A Dissertation for The Degree of Doctor of Engineering

Modern Wireless Relaying Cooperative Network Design: Transmission Performance, Physical Layer Security, and Wireless Power Transfer

無線協調リレーネットワークの設計に関する研究：通信特性、物理層セキュリティと無線電力伝送

Tianji Shen

Graduate School of Engineering, Yokohama National University

Advisor: Prof. Hideki Ochiai

Graduate School of Engineering, Yokohama National University

Date of Submission: June 2021

YNU 横浜国立大学
YOKOHAMA National University

Abstract

Relaying technologies have been actively studied in mobile broadband communication systems, and also considered in the recent standard release by the Third Generation Partnership Project (3GPP). However, relaying in the different transmission scenarios is a challenging topic. Specifically, the Internet of things (IoT) bridges the cyber domain to everything and anything within our physical world which enables unprecedented ubiquitous monitoring, connectivity, and smart control. The utilization of unmanned aerial vehicle (UAV)-enabled relaying network can offer an extra level of flexibility which supports more advanced and efficient connectivity as well as data aggregation for the IoT devices. As a result, however, the higher request of secrecy requirement becomes a critical issue. Although traditional encryption techniques at higher layers require a certain form of information sharing between the transmitter and the legitimate user to achieve security, it may be insufficient or even unsuitable for wireless relaying network systems. Physical layer security has potential in secure wireless communications by leveraging the physical nature of wireless relaying transmission. Furthermore, the replacement of battery is also a critical issue for wireless relaying network. In such scenario, a radio-frequency (RF) wireless transfer technique can be a viable option to prolong the lifetime of such energy-constrained wireless networks, where the transmission node can harvest energy from the access point to assist its information transmission. It is thus important for the system designer to design and analyze the throughput efficient energy harvesting protocols to enhance the lifetime of such energy constrained wireless networks.

In this dissertation, we propose several approaches for the data transmission and the physical layer security in modern wireless relaying networks. We introduce the fundamental principles of cooperative relaying network and physical layer security in Chapter 1. In Chapter 2, the fundamental introductions of fading channel models, decode-and-forward half-duplex relaying, non-orthogonal multiple access (NOMA), and benchmarks of physical layer security are given. In Chapter 3, we introduce the secrecy performance in the adaptive decode-and-forward relaying/jamming cooperative network, without any channel state information (CSI) of the eavesdropper for the system. In Chapter 4, the performance of the unmanned aerial vehicle (UAV)

swarm-based cooperative relaying network is analyzed, which consisting of a pair of source and destination, supported by multiple cooperative UAVs in the presence of a single UAV-aided eavesdropper. For allocation of the UAV swarm, the following four specific approaches are investigated, and the transmission outage probabilities of signals received by destination and eavesdropper for each approach are mathematically formulated. In Chapter 5, the performance of NOMA and cooperative relaying schemes is compared in UAV-enabled wireless powered sensor network. We study several transmission schemes including NOMA as well as cooperative relaying, together with two representative sensor node pairing strategies. In Chapter 6, conclusions and future research directions are given.

Acknowledgments

First, I would like to express my utmost gratitude to my supervisor, Hideki Ochiai for his encouragement, motivation, and the excellent guidance in wireless communications. For a long period in this laboratory, including research student and master student time, he gave me a lot of thoughtful and encouraging comments in my research and the solution for my personal matters. I believe that it was so lucky for me to study under his supervision.

My special thanks should go to Prof. Hamagami, Prof. Ichige, Prof. Shima, and Prof. Ishikawa. I also would like to thank retired Prof. Kohno. They provide me a lot of observant and helpful comments that improve my manuscripts and this dissertation.

I also wish to thank the past and current members of Ochiai laboratory. Especially, I would like to my grateful gratitude to Vikash Singh, Yuki Matsumoto, Yuto Hama, Shuntaro Suzuki, Junya Watanabe, Daiki Yoda, Yoshito Watanabe, Jiajia Song, Khalid Al Shanfari, Kanji Kamada, Yuki Yajima, Ryo Yamamuro, Haruhiko Hasegawa, Junnosuke Hiyama, Daichi Muramatsu, Eito Kurihara, Kosuke Ikeya, Masayuki Kaneko, Yuki Kuraya, Kazuaki Hanazawa, Junpei Hosono, Ying Sun, Ahmad Shahpoor Seraj, ZiaEya Ekolle, Takahiro Goto, former secretary – Naoko Shibukawa, and the secretary – Chiaki Miyauchi, for their sincere help in research as well as in private.

Furthermore, I would also like to extend my gratitude towards my parents and my girlfriend Ji-Cin for their long period of support and encouragement.

感谢在 这长期海外留学期 间帮助以及支持我的父母以及家人，另外 还有在 这期 间一直默默鼓励我的女友 陈季芹。没有 你们的帮助与支持，仅凭我个人很 难完成自己的学业。

另外感谢其他所有海外的中国留学生 对我的帮助。谢谢。

Contents

List of Abbreviations

3GPP Third Generation Partnership Project

3D three-dimensional

5G the fifth-generation

B5G beyond the fifth-generation

6G the sixth-generation

IoT Internet of things

RF radio-frequency

CSI channel state information

NOMA non-orthogonal multiple access

OMA orthogonal multiple access

UAV unmanned aerial vehicle

WPT wireless power transfer

PDF probability density function

CDF cumulative distribution function

RV random variable

AF amplify-and-forward

DF decode-and-forward

BS base station

SIC successive interference cancellation

NAICS network-assisted interference cancellation and suppression

TDMA time division multiple access

OFDMA orthogonal frequency division multiple access

OFDM orthogonal frequency-division multiplexing

PHY physical layer

AN artificial noise

LoS line-of-sight

NLoS non-line-of-sight

A2G air-to-ground

G2A ground-to-air

A2A air-to-air

G2G ground-to-ground

MIMO multiple-input-multiple-output

AWGN additive Gaussian white noise

MRC maximum ratio combining

SC selection combining

BF beamforming

SINR signal-to-interference-plus-noise ratio

i.i.d independent and identically distributed

GS ground station

ACK acknowledgment

WPSN wireless powered sensor network

SWIPT simultaneously wireless information and power transfer

QoS quality of service

CW continuous waveform

List of Figures

List of Tables

Chapter 1

Introduction

Comparing with wired communication, the wireless network has been the practical communication method due to its convenience and flexibility in varies environments. In conjunction with the development of the beyond fifth-generation (5G) and sixth-generation (6G) mobile communications, various kinds of Internet of Things (IoT) devices (e.g., smartphones, smart watches and other IoT sensors) are designed and produced. The number of these devices is predicted to keep increasing in the upcoming years. Therefore, connecting massive number of devices through wireless signals will become more important. The most critical challenge for wireless systems is to find practical solutions in performance and secrecy improvement, i.e., to achieve reliable transmission and keep the information safe while improving data rates as well as confidentiality.

To cope with the above challenge, in this dissertation, a cooperative network technology is focused on, and the modern technologies to the emerging wireless scenarios is applied. In this chapter, we will review these advanced schemes.

1.1 Backgrounds

1.1.1 Cooperative Networks

Cooperative communication is widely considered as a means to make the transmitting signals robust against fading environment, to compensate for the power limitation in the wireless communication devices, and therefore to improve the range of wireless communication [1–5].

A concept of a most widely studied cooperative network is illustrated in Fig. 1.1, where two nodes communicate with the same destination. Since each wireless node is equipped with a single antenna, and thus its spatial diversity cannot be achieved. During the long-distance transmission in a fading environment, or if the building and other obstacles block the direct link, the other nodes help the source nodes as relay. Among many cooperative relaying protocols, the most wildly investigated are the amplify-and-forward (AF) protocol and the decode-and-forward

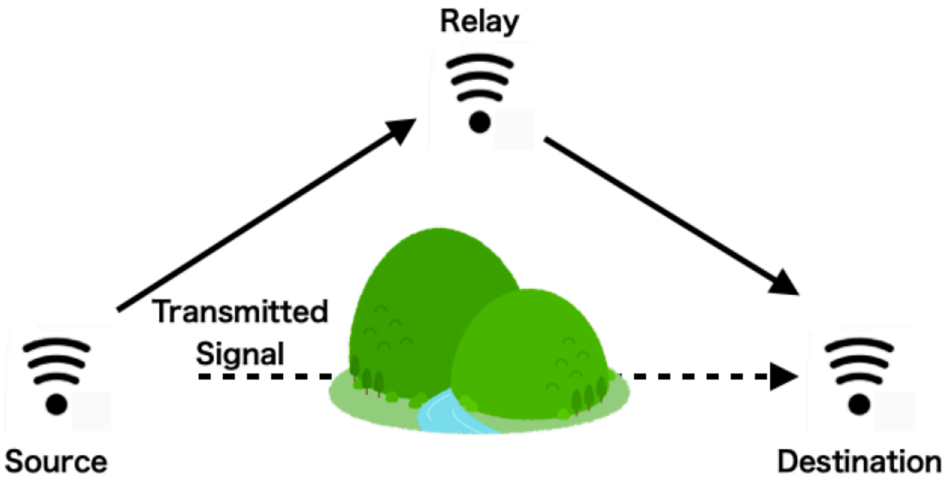


Figure 1.1: Fundamental illustration of cooperative relaying networks

(DF) protocol [6, 7]. In AF protocol, relay amplifies the received data from source without decode and re-encode process, then transmits it to destination [8–15]; In DF protocol, the relay first decodes the received signal before the forwarding process [16–23]. In this dissertation, we are interested in the DF protocol.

1.1.2 Unmanned Aerial Vehicle (UAV) Communication

Unmanned aerial vehicle (UAV) enabled systems and their wireless communication networks are considered for a variety of applications, such as security operations in the military, entertainment, and telecommunications in recent decades [24–30]. The number of UAV applications is increasing in the telecommunication industry, e.g., relay-base stations (BSs), communication gateways, data collection in wireless sensor networks, search and rescue operations in earthquake area, entertainment industry, and power lines maintenance [31]. The potential role of UAVs as a relay BS in hotspots, congested area, makes them an inherent part of the next-generation communication infrastructure [32]. The typical use cases of aerial wireless BSs have been investigated in [33, 34], which is one of the main topics in this dissertation. We list the related scenarios as follows:

- **Ubiquitous Coverage**: UAVs are used in providing seamless wireless network coverage assistance within the serving area. UAV with rapid service recovery after critical disaster situations has been investigated in [33].

- **Relay Nodes**: The UAV can be controlled as a relay node in order to provide a wireless connection between two or more long-distance wireless devices without a reliable direct communication link. In [35], the authors propose a new mobile relaying technique, where the relay node is equipped on a UAV with high moving speed. As a result, the throughput could be maximized by optimizing the relay trajectory and the source-relay power allocation. We will focus on this scenario in Chapter 4.

- **Data Collection**: In [36,37], the UAV data collection scenarios have been discussed, where a large number of distributed wireless devices are sending the delay-tolerant information to the utilized UAV. We investigate this scenario in Chapter 5.

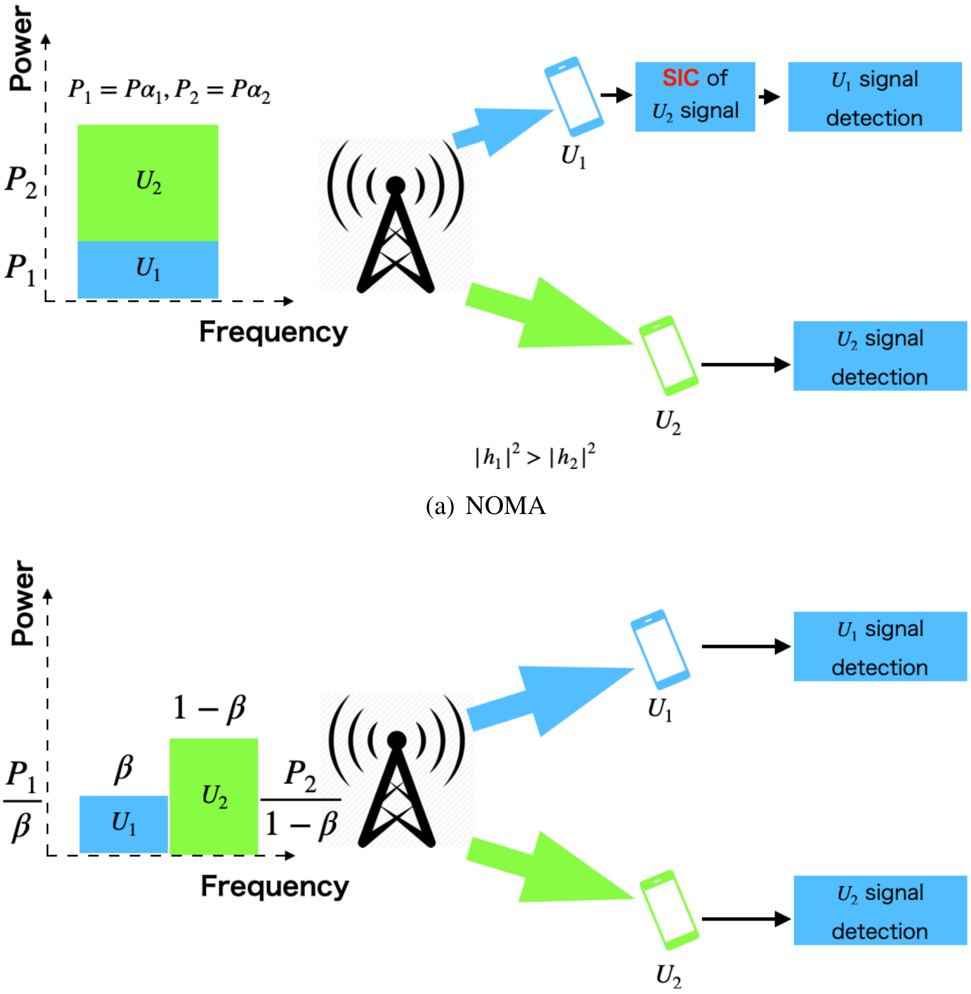
- **Network Gateways**: UAVs can be used as gateway nodes to connect with backbone networks, communication infrastructure, or the Internet in the remote geographic, which has been investigated in [38, 39].

1.1.3 NOMA Technology

In order to achieve enhanced spectrum efficiency of the wireless mobile network, non-orthogonal multiple access (NOMA) has received attention by the researchers focusing on wireless systems [40–42]. Notably, different devices can share the same time and frequency spectrum with cooperative power allocation adjustment. Through the use of successive interference cancellation (SIC), the devices with weak power conditions can decode its own information after removing those strong power condition [43, 44], which has been investigated as an extension of the network-assisted interference cancellation and suppression (NAICS) in 3GPP [45, 46]. This technique significantly improve the spectral efficiency and outperform traditional orthogonal multiple access (OMA) schemes under the limitation of frequency spectrum.

In Fig. 1.2, we illustrate the difference between OMA and NOMA. The OMA technique contains orthogonal frequency division multiple access (OFDMA) or time division multiple access (TDMA). In OFDMA, multiple devices are allocated with orthogonal subcarriers contacted via the orthogonal frequency-division multiplexing (OFDM) technique. In TDMA, the devices divide the signal into different time slots in order to share the same frequency channel.

The downlink scenario with NOMA scheme is demonstrated in Fig. 1.2(a), where two devices (i.e., U_1 and U_2) receive information from a single base station (BS) with the same transmission channel. The BS continuously sends the signal to U_1 and U_2 simultaneously, where the two different signals are non-orthogonally superposed. In the decoding process, U_1 needs to decode the signal of U_2 and run SIC process of U_2 signal before decoding its own signal. In



(a) NOMA

(b) OMA

Figure 1.2: Multiple access scenarios for two devices that form a pair.

this dissertation, we apply the NOMA technology in UAV-aided model in order to improve the transmission performance of the wireless communication system. The details and applications of the NOMA technology are presented as a transmission scheme in Chapter 5.

1.1.4 Physical Layer Security

Exchanging information over wireless channels is vulnerable to eavesdropping attacks and jamming attacks from malicious nodes due to the broadcast nature of wireless communications. In recent years, the critical issue of security against eavesdropper attacks is widely investigated in the different types of wireless networks [47–49]. In order to protect from wireless information leakage, cryptography-based secrecy methods are widely utilized in the upper layer of various wireless transmission protocols. Cryptography-based systems encrypt information with various secret key generation protocols. In most research assumptions, eavesdroppers could not decrypt the wiretapped signal in a limited time through exhaustive search due to the limitation of computing capabilities. Nevertheless, the computing capabilities of eavesdroppers increase significantly in recent years. These traditional cryptography-based solutions are facing a critical risk of being broken via the relentless brute-force attacks of eavesdropper with a short period [50, 51]. Furthermore, in the wireless distributed networks, the decentralized framework of the network design makes the secret keys difficult to be managed and distributed. This requires the introduction of more powerful secrecy methods to increase the security of wireless networks and decrease the method complexity. Therefore, physical layer (PHY) security methods have been proposed in order to provide effective security assurance for wireless networks [52]. Compared to cryptography-based solutions, PHY security has several obvious advantages. It can guarantee information secrecy regardless of the computational capabilities of eavesdroppers. The costly centralized secret key management/distribution methods, which are widely used in cryptography-based security systems, could be eliminated in PHY security techniques, which facilitated the management and improving the efficiency of wireless communication networks.

The PHY security dates back to Wyner's wiretap model [53]. Wyner's results show that without using any secret key protocols between the legitimate transmitter-receiver pairs, the non-zero secrecy rate can be achieved. In the extension researches of Wyner's problem, the secrecy capacity is defined as the difference between Shannon's capacities of the main and eavesdropper channels [54, 55]. In order to improve the secrecy rate, PHY security techniques have been developed based on the inherent randomness of both the main and eavesdropper channels of wireless networks. In this dissertation, we focus on the following schemes:

- **Cooperative Jamming:** Cooperative jamming allows the idle nodes to send artificial noise (AN) to eavesdroppers for the secrecy capacity improvement of a given transmitter-receiver pair [56–59]. AN is usually assumed as a random generated noise with Gaussian distribution independent of the intended information signal, which helps to degrade the information received at the eavesdropper [56]. Particularly, AN used for jamming could be structured by some specific codewords that can be canceled only at legitimate devices [58]. Even though no channel state information (CSI) about the eavesdropper channel is needed in the cooperative jamming scheme, the interference that caused by AN could also degrade the transmission performance of the main channel due to the interference.

- **Relay Selection:** In order to enlarge the secrecy capacity between the main and eavesdropper channels, the relay selection strategy could improve the secrecy performance by choosing a robust main link but a weak eavesdropper link [60–63]. The selected relay should transmit information in a prefixed manner without considering the current channel quality. In order to address this limitation, buffer-aided relay selection strategies have been proposed, where relays select the best link from all available links to transmit buffer stored delay-tolerant information based on the current channel gains [62, 63]. Even though relay selection will not decrease the performance of transmissions in the main channel, the full CSI of the eavesdropper channel is always required due to the optimized relay selection strategy, which may not be practical in the realistic scenario.

- **Beamforming and Precoding:** Beamforming is the technology that transmits one data stream through multiple antennas by adjusting the signal phase [64–67]. The direction of the antennas and the phase alignment of signals are controlled by the controller unit of the transmitter such that the antenna matrix at the transmitter concentrates the signal strength towards the direction of the intended receiver. In contrast, the signal strength is maximized at the eavesdropper should be limited. However, precise synchronization between the transmitter and receiver is required. It also requires the perfect knowledge of eavesdropper CSI for beamforming AN in order to prevent information leakage.

We further discuss relay selection and cooperative jamming in Chapter 3 and Chapter 4. Furthermore, we also investigate the effect of beamforming in Chapter 3.

1.1.5 Wireless Power Transfer (WPT)

In the modern wireless network, the cooperative communication is proposed with the help of intermediate cooperative nodes that forward the information of the source to the destination in a long-distance transmission scenario. The cooperative relay nodes could be subject to severe energy limitation during the long time transmission due to the battery capacity [68, 69]. A radio-frequency (RF) wireless power transfer (WPT) offers an available option to extend the lifetime of low energy-level cost wireless networks with such external power sources. The receiver could extend its lifetime by receiving RF signal for energy recharging. Moreover, transmitting sufficient power to the low-power IoT devices is possible by WPT system. For instance, a distributed WPT system was proposed for wireless charging of low power IoT devices in [70].

We further discuss WPT with UAV-enabled wireless communication in Chapter 5.

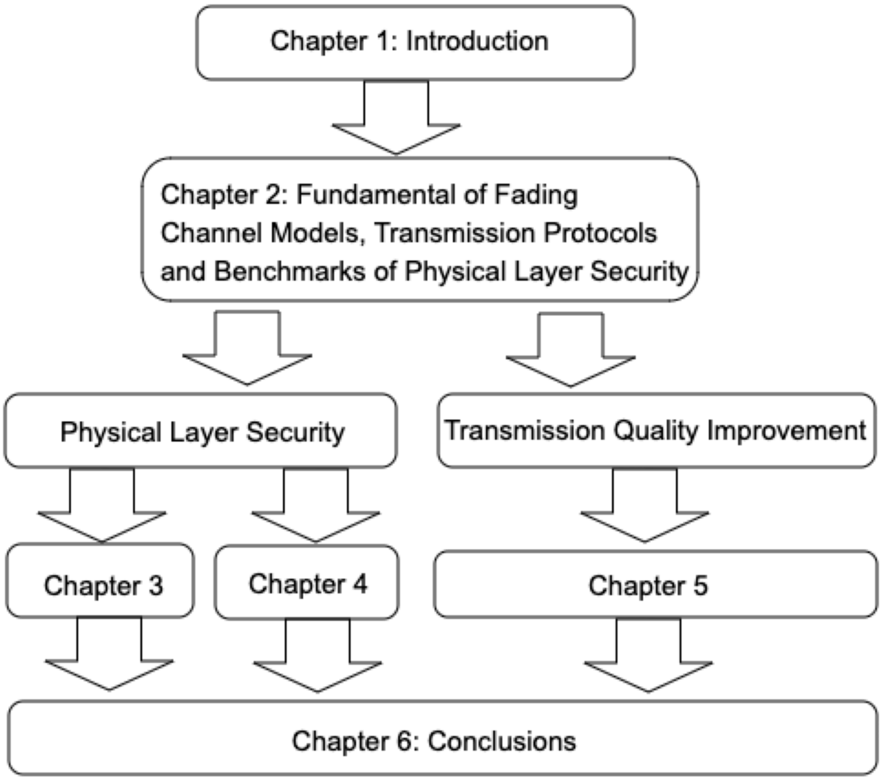

Chapter 1: Introduction
Chapter 2: Fundamental of Fading Channel Models, Transmission Protocols and Benchmarks of Physical Layer Security
Physical Layer Security
Transmission Quality Improvement
Chapter 3
Chapter 4
Chapter 5
Chapter 6: Conclusions

Figure 1.3: Outline of this dissertation

1.2 Outline of the Dissertation

The outline of this dissertation is summarized in Fig. 1.3.

- In Chapter 2, we introduce the fundamental fading channels, transmission protocols, and benchmarks of physical layer security, which are used in this dissertation.

- In Chapter 3 titled as “Secure Transmission Based on Adaptive Multiple-Antenna Cooperative Relays without Eavesdropper CSI,” we consider secure wireless communications between a pair of single-antenna source and destination nodes aided by K-antenna equipped N cooperative devices, subject to individual transmission power constraints on the source node and the cooperative devices. We assume that each transmission device selects its transmission mode in relaying or jamming depending on its signal decoding result from source. Due to line-of-sight channel components, we assume that the channel between source to cooperative devices and the devices to destination are Rician fading. Furthermore, we give the best secrecy scenario and worst secrecy scenario of the eavesdropper as the system cannot access the CSI of eavesdropper. During the best secrecy scenario, the channels between cooperative devices and eavesdropper consist of non-line-of-sight (NLoS) components, i.e., Rayleigh fading channels. On the other hand, during the worst secrecy scenario, the channels between cooperative devices and eavesdropper consist of LoS components, similar to the channels between cooperative devices and destination. The asymptotic closed-form theoretical expressions for its outage probability of destination and eavesdropper, as well as the secrecy outage probability of this system are developed.

- In Chapter 4, titled as "Performance Analysis of Secure Relaying Network Based on Cooperative UAV Swarm Over Rician Fading Channels," the performance of the unmanned aerial vehicle (UAV) swarm-based cooperative relaying network, consisting of a pair of source and destination, supported by multiple cooperative UAVs in the presence of a single UAV-aided eavesdropper is analyzed. The UAV swarm assists source by cooperative relaying, and also prevents interception of eavesdropper through cooperative jamming. Upon cooperation, the UAV swarm is divided into the two different functionalities: relaying and jamming. For allocation of the UAV swarm, the following four specific approaches are investigated: Optimal relay selection (ORS), where a single relay with the highest SNR is selected without jammers; optimal relay selection with single jamming (ORSJ), where one jammer is also selected in addition to ORS; optimal relay selection with multiple jamming (ORSMJ), where multiple UAV jammers are selected and artificial noise is transmitted toward the eavesdropper through cooperative beamforming; and multiple relay combining with multiple jamming (MRCMJ), where the multiple UAV-aided relays also perform cooperative beamforming of information to destination in order to prevent eavesdropper from wiretapping.

- In Chapter 5 titled as "A UAV-Enabled Wireless Powered Sensor Network Based on NOMA and Cooperative Relaying with Altitude Optimization," the uplink of a UAV-enabled wireless network using power-domain NOMA as well as cooperative relaying is studied, where the ground sensor nodes are wireless powered devices. These devices experience air-to-ground (A2G) communication channels, which are characterized by altitude-dependent path loss exponent and fading. A *user pairing* system associated with the wireless networks based on NOMA or cooperative relaying is focused on, where the access devices are divided into two groups and a pair of devices is formed from each group. The available bandwidth is then divided according to the number of the pairs where each pair shares the same sub-channel to send their respective information.

- In Chapter 6, concluding remarks and future research directions are given.

Chapter 2

Fundamental of Fading Channel Models, Transmission Protocols, and Benchmarks of Physical Layer Security

In this chapter, the fundamental frameworks of cooperative networks i.e., fading channel models, decode-and-forward cooperative relaying and NOMA, are presented. Furthermore, the concepts and benchmarks of physical layer security, are also introduced.

2.1 Fading Channel Models

In a wireless system, the signal will interact with highly complex environment before it is received by the receiver, such as Doppler shift, and fading. In this dissertation, the transmission processes consist of discrete-time blocks in short time is assumed. The channel gain is non-frequency selective and constant in each block and independent and identically distributed, i.e., block fading [71, §4.2.1]. As the statistical result based on measurements, if there are only scattered paths between the transmitter and receiver (also called non line-of-sight (NLoS) scenario), the channel gain follows zero-mean circularly symmetric Gaussian distribution. Hence, the signal envelope follows Rayleigh distribution, with its probability density function (PDF) as [71, (3.32)]

$$f_Z^{\mathrm{Rayleigh}}(z) = \frac{z}{\sigma^2} \exp\left(-\frac{z^2}{2\sigma^2}\right), \tag{2.1}$$

where σ^2 is the second moment of random variable Z.

Conversely, if the channel consists of both direct path (also called line-of-sight (LoS) component) and scattered paths, the channel gain follows non zero-mean circularly symmetric Gaussian distribution. Hence, the signal envelope in such case can be shown to have Rician distribution with its PDF as [71, (3.37)]

$$f_Z^{\text{Rician}}(z) = \frac{2(K+1)z}{\Omega} e^{-\left(K + \frac{(K+1)z^2}{\Omega}\right)} I_0 \left(2\sqrt{\frac{K(K+1)}{\Omega}} z \right), \tag{2.2}$$

where K is defined as the ratio between the power in direct path components and scattered multipath components, Ω is defined as the total power received from paths, and $I_0(\cdot)$ is the zero-ordered modified Bessel function of first kind. For special cases, while $K = 0$, Rician distribution will degrade to Rayleigh distribution; while $K = \infty$, the channel will have no fading, i.e., additive white Gaussian noise (AWGN) channel.

Furthermore, in order to simplify the numerical evaluation of Rician fading channel, Nakagami-m fading model is often adopted to approximate the Rician fading, where the PDF is expressed in closed-form as [71, (3.38)]

$$f_Z(z)^{\text{Nakagami}} = \frac{2m^m z^{2m-1}}{\Gamma(m)\Omega^m} z^{2m-1} \exp\left(-\frac{m}{\Omega} z^2\right) \tag{2.3}$$

with parameter $m \triangleq \frac{(K+1)^2}{(2K+1)}$, and Ω follows the same definition as Rician distribution. For special cases, if $m = 1$ the distribution reduces to Rayleigh fading; while $m = \infty$, the channel is approximately equal to AWGN channel.

2.2 Cooperative Networks

In recent advancements of radio techniques, the information systems are requested to have abilities in exchanging information from anywhere, at any time, and with any devices. A key enabling technique for such scenario could be cooperative networks. Whereas in the cooperative networks, neighboring devices assist each other in sharing information. The advantage of such low-complexity networks is that it is feasible even in energy-constrained networks. As a result, there are multiple research directions based on cooperative networks, such as power efficiency, network capacity and coverage.

2.2.1 Decode-and-Forward Half-Duplex Relaying Network

The illustration of a classic half-duplex cooperative relaying network is shown in Fig. 2.2.1, which consists of three devices: the source, the relay and the destination. There are two phases during the cooperative relaying transmission. In phase 1, the source transmits its signal to the

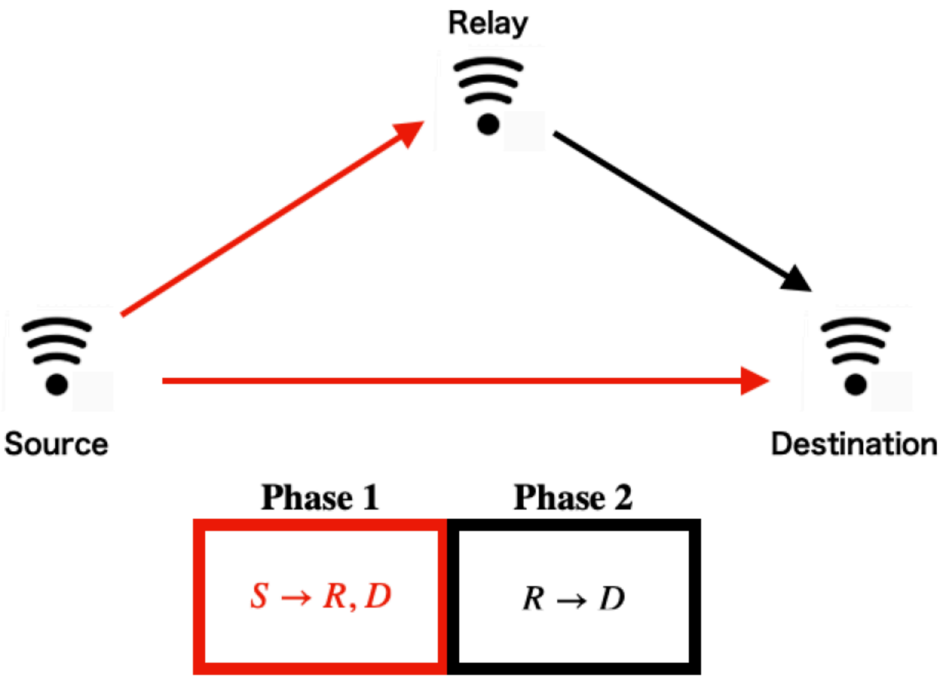


Figure 2.1: Illustration of a classic three devices cooperative relaying network

relay and destination and in phase 2 the relay forwards the signal received in phase 1 to the destination after the decoding and re-encoding processes. The relay needs to successfully decode the received signal before the forwarding, otherwise, it skips the phase 2 transmission [8]. The achievable data rate between each device, i.e., source to relay, source to destination, and relay to destination links in phase 1 and phase 2 can be expressed as

$$C_{i,j} = A_k \log_2 \left(1 + \gamma_{i,j}\right), \tag{2.4}$$

where $A_k \in (0,1),\ k \in \{1,2\}$ is the time ratio of kth phase with $\sum_k A_k = 1$, $\gamma_{i,j}$ is defined as the signal-to-noise ratio (SNR) received at j. In the DF protocol, with the minimum decodable rate R_{th} the system outage can be defined as [72]

$$P_{\text{out}} = P\left[\{(C_{S,R} < R_{\text{th}}) \cap (C_{S,D} < R_{\text{th}})\} \cup \{(C_{S,R} \geq R_{\text{th}}) \cap (C_{R,D} < R_{\text{th}})\}\right]. \tag{2.5}$$

2.2.2 Non-orthogonal Multiple Access (NOMA)

In Chapter 1, Fig. 1.2(a) presents a simple NOMA system, which consists of a single base station and two single-antenna devices. Assuming that the signals transmitted by the base station to devices U_1 and U_2 are x_1 and x_2, the superposed signal transmitted by base station can be expressed as

$$\begin{aligned} s &= \sqrt{P_1}x_1 + \sqrt{P_2}x_2 \\ &= \sqrt{P\alpha_1}x_1 + \sqrt{P\alpha_2}x_2, \end{aligned} \tag{2.6}$$

where P is the transmission power and α_k is the power ratio of signal to the kth device. The channel gains are assumed that from base station to the devices are h_1 and h_2, and variances of additive white Gaussian noise (AWGN) are σ_1^2 and σ_2^2. If transmission power of signal x_1 is less than x_2, i.e., $P_1 < P_2$, U_2 can decode the information x_2 while treating signal x_1 as noise. Therefore, the achievable data rate C_2 received at U_2 can be expressed as

$$C_2 = \log_2\left(1 + \frac{P_2|h_2|^2}{P_1|h_2|^2 + \sigma_2^2}\right). \tag{2.7}$$

Conversely, the device U_1 needs to decode the signal x_2 before receive its own information. If U_1 successfully decodes the signal x_2, it can decode its information by removing signal x_2 with successive interference cancellation (SIC) scheme. The achievable data rate at U_1 with perfect SIC scheme and minimum decodable rate R_{th} can be expressed as

$$C_1 = \begin{cases} \log_2\left(1 + \frac{P_1|h_1|^2}{\sigma_1^2}\right), & \frac{P_2|h_1|^2}{\sigma_1^2} \geq 2^{R_{\text{th}}} - 1 \\ 0, & \text{otherwise} \end{cases} \tag{2.8}$$

2.3 Benchmarks of PHY Security

In Chapter 1, the framework of physical layer (PHY) security is introduced. Furthermore, in this section, the benchmarks of PHY security are introduced: secrecy capacity and secrecy outage probabilities.

As Fig. 2.2 shows, a classic wiretapping model is composed of transmitter (Alice), receiver (Bob) and eavesdropper (Eve). Eve wiretaps the information x_A during Alice transmits its signal. If the channel gain from Alice to Bob and Alice to Eve are defined as $h_{A,B}$ and $h_{A,E}$, the signal received by Bob and Eve can be expressed as

$$y_B = \sqrt{P_A}h_{A,B} + N_B, \tag{2.9}$$

$$y_E = \sqrt{P_A}h_{A,E} + N_E, \tag{2.10}$$

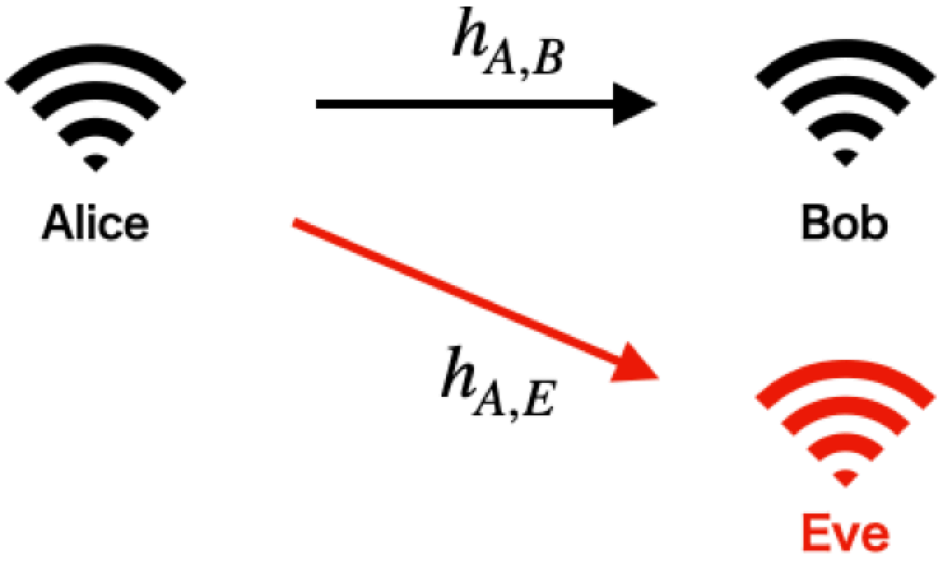


Figure 2.2: Illustration of a classic three devices wiretapping model

where P_A is the transmit power of Alice, N_B and N_E are AWGN variables received by Bob and Eve with expected value $\mathbb{E}(N_B) = \mathbb{E}(N_E) = 1$. Therefore, the achievable data rate of Bob and Eve can be expressed as

$$C_B = \log_2\left(1 + \frac{P_A|h_{A,B}|^2}{\sigma_B^2}\right), \tag{2.11}$$

$$C_E = \log_2\left(1 + \frac{P_A|h_{A,E}|^2}{\sigma_E^2}\right), \tag{2.12}$$

where σ_B^2 and σ_E^2 are variances of AWGN observed by Bob and Eve.

The secrecy capacity is represented by the capacity gap between Bob and Eve [53, 73], i.e.,

$$\begin{aligned} C_s &= [C_B - C_E]^+ \\ &= \left[\log_2\left(\frac{1 + \frac{P_A|h_{A,B}|^2}{\sigma_B^2}}{1 + \frac{P_A|h_{A,E}|^2}{\sigma_E^2}}\right)\right]^+, \end{aligned} \tag{2.13}$$

where $[x]^+ = \max\{x, 0\}$.

Moreover, for given target secrecy rate R_s the secrecy outage probability is defined as the probability that the instantaneous secrecy capacity C_s is less than R_s, which can be expressed as [74, 75]

$$\begin{aligned} P_{\mathrm{out}}^{\mathrm{s}} &= P\left(C_s < R_s\right) \\ &= P\left(\left[\log_2\left(\frac{1+\frac{P_A|h_{A,B}|^2}{\sigma_B^2}}{1+\frac{P_A|h_{A,E}|^2}{\sigma_E^2}}\right)\right]^+ < R_s\right). \end{aligned} \tag{2.14}$$

2.4 Conclusion

In this chapter, the fundamental signal models of transmission protocols are introduced, i.e., fading channels models, DF half-duplex relaying network, and NOMA. Moreover, the definition of secrecy capacity and secrecy outage probability is introduced, which are the benchmarks of PHY security in most of the scenarios. In the subsequent chapters, the system performances and secrecy performances based on the introduced models and the benchmarks will be analyzed.

Chapter 3

Secure Transmission Based on Multiple-Antenna Cooperative Relays without Eavesdropper CSI

In this chapter, the secure wireless communications between a pair of single-antenna and destination nodes aided by K-antenna equipped N cooperative devices is considered, which subject to individual transmission power constraints at the source node and the cooperative devices.

3.1 Introduction

As mentioned in the Section 1.1.4 of Chapter 1, physical layer (PHY) security is a critical issue in modern communication techniques. There are multiple schemes can improve secrecy of PHY: cooperative jamming, relay selection, beamforming, and precoding. The key idea of artificial noise (AN) or interference to impair the channel quality of the eavesdropper, without significantly degrading the main channel, was introduced in [76]. Cooperative jamming is a promising technology for improving information secrecy [77–79]. Moreover, the performance of AN is determined by the accuracy of channel state information (CSI) at the transmitter. Hence, most of the researchers have considered the models where full or partial CSI of the eavesdropper is available upon transmission of information [77, 80–82]. However, in practice, the legitimate parties have no chance to access the full CSI of the eavesdropper as long as it is passive and only receiving information. In order to deal with this issue, the signal hybrid with AN sent from multiple antenna sources has been proposed in [79,83,84]. In [83] and [84], the transmitter sends the AN in the null space of the main channel to maximize the received SNR and avoid interference to the legitimate receiver. More recently, in [79], the secrecy performance under energy-efficient multiple-input-multiple-output (MIMO) decode-and-forward (DF) relaying scheme has been investigated. It is worth noting that in most of the state-of-the-art researches [77,85], the knowledge on the CSI of the eavesdropper's channel is required. However, in practice, the eavesdropper's CSI is difficult to be precisely estimated, and its location that may change over time.

In this chapter, we consider secure wireless communication between a pair of single-antenna source and destination nodes aided by K-antenna equipped N cooperative devices, subject to individual transmission power constraints at the source node and the cooperative devices. We assume that each cooperative device selects its transmission mode in relaying or jamming depending on its signal decoding result from the source. Due to the line-of-sight (LoS) channel components, we assume that the channel between source to cooperative devices and the devices to destination consists of LoS components, i.e., Rician fading. Furthermore, due to the absence of CSI of the eavesdropper in our system assumption, the two estimated secrecy scenarios in our model are derived. During the first case of the secrecy scenario, (i.e., case 1), the channels between cooperative devices and eavesdropper consist of non-line-of-sight (NLoS) components, i.e., Rayleigh fading channels. Conversely, in the second case of the secrecy scenario, (i.e., case 2), the channels between cooperative devices and eavesdropper consist of LoS components, similar to the channels between cooperative devices and destination. The asymptotic closed-form theoretical expressions for the outage probability of the destination and the eavesdropper are developed, as well as the estimated secrecy outage probability of this system.

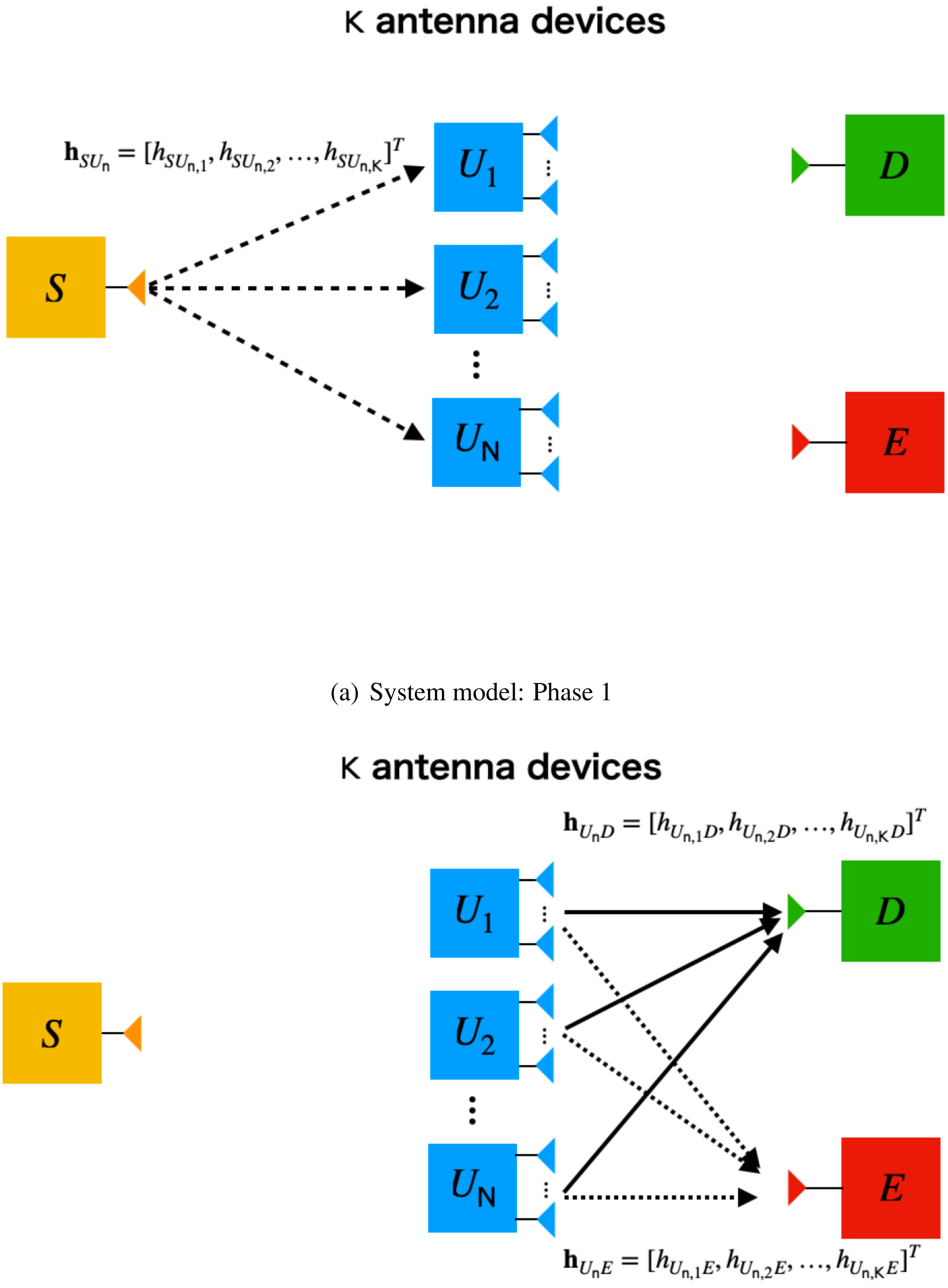
The rest of the chapter is organized as follows. Section 3.2 describes the system model of our proposed adaptive DF secure relaying network with relay mode selection. Our main results on the performance analysis are presented in Section 3.3. Section 3.4 presents several numerical examples obtained from the analytical expressions for the outage probabilities and secrecy outage probabilities. Section 3.5 concludes this chapter.

Notation: Throughout this chapter, $f_\varphi(\cdot)$ and $F_\varphi(\cdot)$ denote the probability density function (PDF) and cumulative distribution function (CDF) of a random variable (RV) φ, respectively; diag$(\cdot)$ denotes the diagonal matrix; $\mathcal{CN}(\mu, \sigma^2)$ denotes the circular-symmetric complex Gaussian distribution with mean μ and variance σ^2; $\mathbb{E}(x)$ is the expected value of a random variable x; $\mathbf{x}^\dagger$ is the Hermitian transpose of $\mathbf{x}$; $\mathbf{x}^T$ is the transpose of $\mathbf{x}$; $[x]^+$ denotes the positive of parameter x, i.e., $\max\{x, 0\}$. Moreover, the following special functions will be used: the nth order Marcum-Q function $Q_n(\alpha, \beta)$ [86]; the modified Bessel function of the first kind $I_\nu(z)$ [87, §8.406].

3.2 System and Channel Models

In this section, the cooperative PHY security system model is considered throughout this chapter. The channel model, signal model, and formulated optimization problem adopted in this chapter are also summarized.

3.2.1 System Model


K antenna devices
$\mathbf{h}_{SU_n} = [h_{SU_{n,1}}, h_{SU_{n,2}}, \ldots, h_{SU_{n,K}}]^T$
S
U_1
U_2
U_N
D
E
K antenna devices
$\mathbf{h}_{U_nD} = [h_{U_{n,1}D}, h_{U_{n,2}D}, \ldots, h_{U_{n,K}D}]^T$
S
U_1
U_2
U_N
D
E
$\mathbf{h}_{U_nE} = [h_{U_{n,1}E}, h_{U_{n,2}E}, \ldots, h_{U_{n,K}E}]^T$

(a) System model: Phase 1

(b) System model: Phase 2

Figure 3.1: Illustration of system model. (Solid arrow: Beamforming transmission; Dash arrow: Unbeamformed transmission)

As shown in Fig. 3.1, a selective relaying secure network is considered, where single-antenna equipped source (S) communicates with single-antenna destination (D) with the help of N intermediate cooperative devices U which are equipped with K antennas (co-devices) $U_1, \ldots, U_{\mathsf{N}}$, in the presence of a single eavesdropper (E).

In what follows, the assumed system operates as follows:

- Let T denote the total transmission time. In the first transmission period with time block length $\zeta T,\ \zeta \in (0,1)$, S broadcasts its information to all cooperative devices. All the devices operate in the decode-and-forward mode, and try to decode the received information from S.

- During the residual block time $(1-\zeta)T$, the devices forward the received information to D. Two transmission strategies are assumed in this chapter: If the devices have the ability to decode the signal from source, it is supposed that all the devices transmit signals depending on the decoding result in the first transmission period, i.e., if the cooperative device decodes the signal from S, then it operates as a relay in the residual period, otherwise, it operates as a jammer to prevent eavesdropper from receiving information[1].

Furthermore, based on the long distance transmission, we assume that the effect of the direct link between $S \to D$ and $S \to E$ are negligible because of the obstacles. It is also assumed that only the phase information between devices and D are available for closed-loop transmit diversity transmission in narrow feedback channel bandwidth [88, 89]. Besides, in most of the state-of-the-art researches, the E location is perfectly or imperfectly known, which is not practical in real scenarios. Hence, in this chapter, it is assumed that the system has no channel state information (CSI) available for E, unless the location of E is clustered at D[2], i.e., E can not receive the beamformed information from cooperative devices.

3.2.2 Channel Assumptions and Problem Formulation

For the devices in the line-of-sight (LoS) scenario, the channel gains typically contain a line-of-sight (LoS) component, but fading effect is often observed. Therefore, we assume that all channels h_{AB} from A to B follow circularly symmetric Gaussian distribution; $h_{AB} \sim \mathcal{CN}(\mu_{\mathcal{AB}}, \sigma^{\in}_{\mathcal{AB}})$, where μ_{AB} are their mean values, whereas σ^2_{AB} are their corresponding varience.

[1] In the residual part of this chapter, the notations of U in phase 2 are changed, which depending on its transmission mode. R_{m} refers to the device working in relay mode with index notation m, as well as J_{l} refers to the device in jamming mode with index notation l.

[2] The E will have same distribution and similarly receive beamforming to D if E clustered at same point position of D. Conversely, the eavesdropper could be physically found in this scenario, which is not practical. Due to these reasons, we assume the E is not clustered at same point of D in this chapter.

Note that $|h_{AB}|$ thus follows Rician distribution (i.e., Rician fading channels). Consequently, the probability density function (PDF) of $X = |h_{AB}|^2$ under the assuption of $\mathbb{E}\left[|h_{AB}|^2\right] = \Omega$, is expressed in the form of

$$f_X(x) = \frac{2(\kappa+1)x}{\Omega} e^{-\kappa - \frac{(\kappa+1)x^2}{\Omega}} I_0\left(2\sqrt{\frac{\kappa(\kappa+1)}{\Omega}x}\right). \tag{3.1}$$

Here, κ is the Rician K-factor defined as the ratio of the powers of the LoS to the scattered components. For simplicity of analysis, it is assumed that all the transmission channels have the identical κ factor, i.e., $\kappa_{SU_\mathsf{n}} = \kappa_{U_\mathsf{n}D} = \kappa$.

In relaying transmission protocol, it is assumed that all the relays operate in DF scheme. We also assume that S transmits signal x_s to destination D through the proposed cooperative network. The $\mathbf{y}_{U_\mathsf{n}}$ signal received by the nth cooperative device can be expressed as

$$\mathbf{y}_{U_\mathsf{n}} = \sqrt{P_S}\mathbf{h}_{SU_\mathsf{n}} x_S + \mathbf{n}_{U_\mathsf{n}}, \tag{3.2}$$

where $\mathbf{h}_{SU_\mathsf{n}} \in \mathbb{C}^\mathsf{K}$ denotes the channel vector from the source to the nth cooperative device with channel coefficients, i.e.,

$$\mathbf{h}_{SU_\mathsf{n}} = [h_{SU_{\mathsf{n},1}}, h_{SU_{\mathsf{n},2}}, \ldots, h_{SU_{\mathsf{n},\mathsf{K}}}]^T,$$

and $\mathbf{n}_{U_\mathsf{n}}$ is the additive Gaussian white noise (AWGN), i.e., $\mathbf{n}_{U_\mathsf{n}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_\mathsf{K}\sigma_U^2)$. The cooperative devices need to decode received signal from source before forwarding it due to the DF relaying approach. The cooperative devices are assumed that operating in the selection combining (SC) scenario while decoding signal, i.e., the devices will choose the received signal with the maximum channel gain coefficient between S and themselves. Hence, the optimal channel gain coefficient $h^*_{SU_\mathsf{n}}$ can be expressed as

$$|h^*_{SU_\mathsf{n}}|^2 = \max_\mathsf{k} |h_{SU_{\mathsf{n},\mathsf{k}}}|^2.$$

We assume the minimum decodable rate R_s for the cooperative device. If there are n cooperative devices which can decode the signal received from S, i.e., $P_S|h^*_{SU_\mathsf{n}}|^2\sigma_U^{-2} \geq \left(2^{\frac{R_s}{\varsigma}} - 1\right)$, they operate in relaying mode with cooperative beamforming (BF); otherwise, they function as a friendly jammer to prevent eavesdropper from wiretapping the signal. The received signal at destination and eavesdropper, which is denoted by y_D and y_E, can be expressed as

$$y_D = \sum_{\mathsf{m}=1}^{\mathsf{n}} \mathbf{h}_{R_\mathsf{m}D}^{\dagger} \mathbf{\Lambda}_{R_\mathsf{m}} \mathbf{x}_{R_\mathsf{m}} + n_D, \tag{3.3}$$

$$y_E = \sum_{\mathsf{m}=1}^{\mathsf{n}} \mathbf{h}_{R_\mathsf{m}E}^{\dagger} \mathbf{\Lambda}_{R_\mathsf{m}} \mathbf{x}_{R_\mathsf{m}} + \sum_{\mathsf{l}=1}^{\mathsf{N-n}} \mathbf{h}_{J_\mathsf{l}E}^{\dagger} \mathbf{\Lambda}_{J_\mathsf{l}} \mathbf{x}_{J_\mathsf{l}} + n_E, \tag{3.4}$$

where $\mathbf{\Lambda}_{R_\mathsf{m}D} = \text{diag}(\sqrt{P_{R_{\mathsf{m},1}}}e^{-j\theta_{\mathsf{m},1}}, \sqrt{P_{R_{\mathsf{m},\mathsf{K}}}}e^{-j\theta_{\mathsf{m},\mathsf{K}}})$ and $\mathbf{\Lambda}_{J_\mathsf{l}D} = \text{diag}(\sqrt{P_{J_{\mathsf{l},1}}}e^{-j\theta_{\mathsf{l},1}}, \ldots, \sqrt{P_{J_{\mathsf{l},\mathsf{K}}}}e^{-j\theta_{\mathsf{l},\mathsf{K}}})$ are the $\mathbb{C}^{\mathsf{K}\times\mathsf{K}}$ diagonal weight matrix for the phase alignment, and x_{R_m} and x_{J_l} are the signals transmitted by the mth cooperative relay and the lth jammer, respectively.

Similarly, given $\mathbf{\Lambda}_{R_\mathsf{m}}$ and $\mathbf{\Lambda}_{J_\mathsf{l}}$, the estimated secrecy outage probability is given by [75]

$$P\left(C_R < C_s\right) = \left(\left[C_D - C_E\right]^{+} < C_s\right) \tag{3.5}$$

where C_s is the target secrecy rate, and C_D and C_E are achievable rates of the destination and the eavesdropper, respectively. They are expressed as

$$C_D = \left(1 - \zeta\right) \log_2\left(1 + \gamma_D\right) \tag{3.6}$$

$$C_E = \left(1 - \zeta\right) \log_2\left(1 + \gamma_E\right), \tag{3.7}$$

where γ_D and γ_E are the signal-to-interference-plus-noise ratio (SINR) at destination and eavesdropper respectively, which can be formulated as

$$\begin{aligned}\gamma_D &= \frac{\sum_{\mathsf{m}=1}^{\mathsf{n}} \mathbf{h}_{R_\mathsf{m}D}^{\dagger} \mathbf{\Lambda}_{R_\mathsf{m}}^{\dagger} \mathbf{\Lambda}_{R_\mathsf{m}} \mathbf{h}_{R_\mathsf{m}D}}{\sigma_D^2 + \sum_{\mathsf{l}=1}^{\mathsf{N-n}} \mathbf{h}_{J_\mathsf{l}D}^{\dagger} \mathbf{\Lambda}_{J_\mathsf{l}}^{\dagger} \mathbf{\Lambda}_{J_\mathsf{l}} \mathbf{h}_{J_\mathsf{l}D}} \\ &= \frac{\sum_{\mathsf{m}=1}^{\mathsf{n}} \sum_{\mathsf{k}=1}^{\mathsf{K}} P_{R_{\mathsf{m},\mathsf{k}}} |h_{R_{\mathsf{m},\mathsf{k}}D}|^2}{\sigma_D^2}\end{aligned} \tag{3.8}$$

$$\gamma_E = \frac{\sum_{\mathsf{m}=1}^{\mathsf{n}} \mathbf{h}_{R_\mathsf{m}E}^{\dagger} \mathbf{\Lambda}_{R_\mathsf{m}}^{\dagger} \mathbf{\Lambda}_{R_\mathsf{m}} \mathbf{h}_{R_\mathsf{m}E}}{\sigma_E^2 + \sum_{\mathsf{l}=1}^{\mathsf{N-n}} \mathbf{h}_{J_\mathsf{l}E}^{\dagger} \mathbf{\Lambda}_{J_\mathsf{l}}^{\dagger} \mathbf{\Lambda}_{J_\mathsf{l}} \mathbf{h}_{J_\mathsf{l}E}}. \tag{3.9}$$

3.3 Performance Analysis

In this section, the analytical expressions are derived for the outage probabilities of destination and eavesdropper for the system model defined in the previous section.

3.3.1 Outage Probability of Main Channel

For the channel to the destination, the outage probability follows binomial distribution, which can be formulated as

$$\begin{aligned}P_{\text{out}}^{D} &= P(C_D < R_s)\\ &= \sum_{\mathsf{n}=0}^{\mathsf{N}} \binom{\mathsf{N}}{\mathsf{n}} P_{U_{\mathsf{n}}}^{\mathsf{N}-\mathsf{n}} \left(1 - P_{U_{\mathsf{n}}}\right)^{\mathsf{n}} P_D^{(\mathsf{n})},\end{aligned} \tag{3.10}$$

where $P_D^{(\mathsf{n})}$ is the outage probability at D in the scenario with n cooperative relaying devices, and residual $\mathsf{N} - \mathsf{n}$ cooperative jamming devices, the superscript (n) refers to the scenario that the transmission contains n relaying devices and $\mathsf{N} - \mathsf{n}$ jamming devices during the second period, $P_{U_{\mathsf{n}}}$ is the transmission outage probability with maximum decodable rate R_s from S to U_{n}, which can be calculated as

$$\begin{aligned}P_{U_{\mathsf{n}}} &= P\left(\zeta \log_2\left(1 + P_S |h_{SU_{\mathsf{n}}}^{*}|^2 \sigma_U^{-2}\right) < R_s\right)\\ &= P\left(|h_{SU_{\mathsf{n}}}^{*}|^2 < \frac{\left(2^{\frac{R_s}{\zeta}} - 1\right)\sigma_U^2}{P_S}\right)\\ &= \left[1 - Q_1\left(\sqrt{2\kappa}, \sqrt{\frac{2(1+\kappa_{U_{\mathsf{n}}})}{\Omega}} \sqrt{\frac{\left(2^{\frac{R_s}{\zeta}} - 1\right)\sigma_U^2}{P_S}}\right)\right]^{\mathsf{K}}.\end{aligned} \tag{3.11}$$

Because cooperative BF is used between cooperative devices and the destination, the outage probability $P_D^{(\mathsf{n})}$ can be expressed as

$$\begin{aligned}P_D^{(\mathsf{n})} &= P\left(\gamma_D < \gamma_{\text{th}}\right)\\ &= P\left(\sum_{\mathsf{m}=1}^{\mathsf{n}} \sum_{\mathsf{k}=1}^{\mathsf{K}} P_{R_{\mathsf{m},\mathsf{k}}} |h_{R_{\mathsf{m},\mathsf{D}}}|^2 \sigma_D^{-2} < \gamma_{\text{th}}\right)\end{aligned} \tag{3.12}$$

where $\gamma_{\rm th}$ is the threshold SNR associated with a given achievable rate R_s, i.e., $\gamma_{\rm th} = 2^{\frac{R_s}{1-\zeta}} - 1$. If the transmission power of each antenna is equally allocated, i.e., $P_{R_{\mathsf{m,k}}} = \frac{P_R}{\mathsf{K}}$, the equation (3.12) can be derived as [90]

$$P_D^{(\mathsf{n})} = \begin{cases} 1 - Q_{\mathsf{nK}}\left(\sqrt{2\kappa}, \sqrt{\frac{2(1+\kappa)}{\Omega}}\sqrt{\frac{\mathsf{K}\sigma_D^2\gamma_{\rm th}}{P_R}}\right), & \mathsf{n} \neq 0, \\ 1, & \text{otherwise.} \end{cases} \tag{3.13}$$

3.3.2 Outage Probability of Eavesdropper Channel

By assumption, the estimated outage probability of the eavesdropper channel can be expressed as

$$\begin{aligned} P_{\rm out}^E &= P(C_D < R_s) \\ &= \sum_{\mathsf{n}=0}^{\mathsf{N}} \binom{\mathsf{N}}{\mathsf{n}} P_{U_\mathsf{n}}^{\mathsf{N}-\mathsf{n}} \left(1 - P_{U_\mathsf{n}}\right)^{\mathsf{n}} P_E^{(\mathsf{n})} \end{aligned} \tag{3.14}$$

where $P_E^{(\mathsf{n})}$ is the outage probability at eavesdropper in the scenario with n cooperative relaying devices and residual $\mathsf{N} - \mathsf{n}$ cooperative jamming devices. For the BF scheme used between the cooperative devices and the destination, the outage probability can be expressed as

$$\begin{aligned} P_E^{(\mathsf{n})} &= P(\gamma_E < \gamma_{\rm th}) \\ &= P\left(\frac{\sum_{\mathsf{m}=1}^{\mathsf{n}} \mathbf{h}_{R_\mathsf{m}E}^\dagger \mathbf{\Lambda}_{R_\mathsf{m}}^\dagger \mathbf{\Lambda}_{R_\mathsf{m}} \mathbf{h}_{R_\mathsf{m}E}}{\sigma_E^2 + \sum_{\mathsf{l}=1}^{\mathsf{N}-\mathsf{n}} \mathbf{h}_{J_\mathsf{l}E}^\dagger \mathbf{\Lambda}_{J_\mathsf{l}}^\dagger \mathbf{\Lambda}_{J_\mathsf{l}} \mathbf{h}_{J_\mathsf{l}E}} < \gamma_{\rm th}\right). \end{aligned} \tag{3.15}$$

Specifically, while $P_{J_\mathsf{k}} = \frac{P_J}{\mathsf{K}}$, $P_{R_\mathsf{k}} = \frac{P_R}{\mathsf{K}}$, and $0 < \mathsf{n} < \mathsf{N}$, (3.15) can reach the asymptotic lower bound with ignoring noise parameter, which can be expressed as

$$\begin{aligned} P_E^{(\mathsf{n})} &\geq P\left(\frac{\sum_{\mathsf{m}=1}^{\mathsf{n}} \mathbf{h}_{R_\mathsf{m}E}^\dagger \mathbf{\Lambda}_{R_\mathsf{m}}^\dagger \mathbf{\Lambda}_{R_\mathsf{m}} \mathbf{h}_{R_\mathsf{m}E}}{\sum_{\mathsf{l}=1}^{\mathsf{N}-\mathsf{n}} \mathbf{h}_{J_\mathsf{l}E}^\dagger \mathbf{\Lambda}_{J_\mathsf{l}}^\dagger \mathbf{\Lambda}_{J_\mathsf{l}} \mathbf{h}_{J_\mathsf{l}E}} < \gamma_{\rm th}\right) \\ &= \int_0^\infty F_\mathsf{R}\left(\frac{(\mathsf{N}-\mathsf{n})P_J\gamma_{\rm th}z}{\mathsf{n}P_R}\right) f_\mathsf{J}(z)\, dz, \end{aligned} \tag{3.16}$$

where $\mathsf{R} = |h_{RE}|^2 = |\sum_{\mathsf{m}=1}^{\mathsf{n}} \sum_{\mathsf{k}=1}^{\mathsf{K}} h_{R_{\mathsf{m,k}}E}|^2$, and $\mathsf{J} = |h_{JE}|^2 = |\sum_{\mathsf{l}=1}^{\mathsf{N}-\mathsf{n}} \sum_{\mathsf{k}=1}^{\mathsf{K}} h_{J_{\mathsf{l,k}}E}|^2$. Note that $h_{R_{\mathsf{m,k}E}}$ and $h_{J_{\mathsf{l,k}E}}$ follow circularly symmetric Gaussian distribution, i.e., $h_{R_{\mathsf{m,k}E}} \sim \mathcal{CN}(\mu_{RE}, \sigma_{RE}^2)$ and $h_{J_{\mathsf{l,k}}E} \sim \mathcal{CN}(\mu_{JE}, \sigma_{JE}^2)$. Due to the fact that all $h_{R_{\mathsf{m,k}}E}$ and $h_{J_{\mathsf{l,k}}E}$ are independent and identically distributed (i.i.d), we can obtain that h_{RE} and h_{JE} follow circularly symmetric Gaussian distribution, i.e., $h_{RE} \sim \mathcal{CN}(\mu_R, \sigma_R^2)$ and $h_{JE} \sim \mathcal{CN}(\mu_J, \sigma_J^2)$ with $\mu_R = \mathsf{nK}\mu_{RE}$, $\sigma_R^2 = \mathsf{nK}\sigma_{RE}^2$, $\mu_J = (\mathsf{N}-\mathsf{n})\mathsf{K}\mu_{JE}$, and $\sigma_J^2 = (\mathsf{N}-\mathsf{n})\mathsf{K}\sigma_{JE}^2$. Due to this scenario, we obtain that R and J follow non-central chi-squared distribution, where their PDF and CDF are defined as [71]

$$
\begin{aligned}
f_X(x) &= \frac{1}{2\sigma^2}\left(\frac{x}{s^2}\right)^{\frac{n-2}{4}} e^{-\frac{s^2+x}{2\sigma^2}} I_{\frac{n}{2}-1}\left(\frac{s}{\sigma^2}\sqrt{x}\right), \\
F_X(x) &= 1 - Q_{\frac{n}{2}}\left(\frac{s}{\sigma}, \frac{\sqrt{x}}{\sigma}\right),
\end{aligned} \tag{3.17}
$$

where n is the degrees of freedom, s is noncentrality parameter, and σ^2 is the variance. Hence, the CDF of random variable R and PDF of random variable J can be formulated as

$$
F_{\mathsf{R}}(x) = 1 - Q_1\left(2\sqrt{\mathsf{Kn}}\sqrt{\frac{\kappa(1+\kappa)}{\Omega}}, \sqrt{\frac{2(\kappa+1)x}{\mathsf{nK}\Omega}}\right), \tag{3.18}
$$

$$
\begin{aligned}
f_{\mathsf{J}}(x) &= e^{-\left[\frac{(1+\kappa)x}{(\mathsf{N}-\mathsf{n})\mathsf{K}\Omega} + \frac{2\mathsf{K}(\mathsf{N}-\mathsf{n})\kappa}{\Omega}\right]}\left(\frac{\kappa+1}{(\mathsf{N}-\mathsf{n})\mathsf{K}\Omega}\right) \\
&\quad \times I_0\left(\frac{2(\kappa+1)\sqrt{2\kappa x}}{\Omega}\right).
\end{aligned} \tag{3.19}
$$

The integral in (3.16) can be carried out using the expression (3.18), (3.19), and [91, eq. (22)-(25)], leading to

$$
P_E^{(\mathsf{n})} \geq 1 - \left(\frac{\kappa+1}{(\mathsf{N}-\mathsf{n})\mathsf{K}\Omega}\right) e^{-\frac{2\mathsf{K}(\mathsf{N}-\mathsf{n})\kappa}{\Omega}}\tau, \tag{3.20}
$$

where

$$
\tau = \left[1 - Q_1\left(\frac{\beta c}{\sqrt{2p\tilde{p}}}, \alpha\sqrt{\frac{2p}{\tilde{p}}}\right)\right]\frac{e^{\frac{c^2}{4p}}}{p} + \frac{2e^{\frac{c^2/2-\alpha^2 p}{\tilde{p}}}}{\tilde{p}} I_0\left(\frac{\alpha\beta c}{\tilde{p}}\right)
$$

with $\alpha = 2\sqrt{\mathsf{Kn}}\sqrt{\frac{\kappa(1+\kappa)}{\Omega}}$, $\beta = \sqrt{\frac{2(\kappa+1)}{\mathsf{nK}\Omega}}$, $c = \frac{2(\kappa+1)\sqrt{2\kappa}}{\Omega}$, $p = \frac{(1+\kappa)}{(\mathsf{N}-\mathsf{n})\mathsf{K}\Omega}$, and $\tilde{p} = 2p + \alpha^2$.

It can obtain obviously $P_E^{(\mathsf{n})} = 1$ while $\mathsf{n} = 0$, and $P_E^{(\mathsf{n})} = F_{\mathsf{R}}\left(\frac{\gamma_{\mathrm{th}}\sigma_E^2}{\mathsf{n}P_R}\right)$ via (3.18) while $\mathsf{n} = \mathsf{N}$.

Consequently, $P_E^{(\mathsf{n})}$ can be expressed as

$$P_E^{(\mathsf{n})} \begin{cases} = 1, & \mathsf{n} = 0 \\ \geq 1 - \left(\frac{\kappa+1}{(\mathsf{N}-\mathsf{n})\mathsf{K}\Omega}\right) e^{-\frac{2\mathsf{K}(\mathsf{N}-\mathsf{n})\kappa}{\Omega}} \tau, & 0 < \mathsf{n} < \mathsf{N} \\ \triangleq 1- & \\ \quad Q_1 \left(2\sqrt{\frac{\mathsf{K}\mathsf{n}\kappa(1+\kappa)}{\Omega}}, \sqrt{\frac{2(\kappa+1)\gamma_{\mathrm{th}}\sigma_E^2}{\mathsf{n}^2\mathsf{K}\Omega P_R}}\right), & \mathsf{n} = \mathsf{N} \end{cases} \tag{3.21}$$

where τ is defined below (3.20).

3.3.3 Estimated Secrecy Outage Probability

In this section, the secrecy outage probabilities which described in the previous session are analyzed. In the subsequent analysis part, the transmitter sends signal from Gaussian codebook and the corresponding mutual information is considered as its achievable rate in our assumptions.

For the different transmission states, the total secure outage probability follows binomial distribution, which can be formulated as

$$\begin{aligned} P(C_R < C_s) &= P([C_D - C_E]^+ < C_s) \\ &= \sum_{\mathsf{n}=0}^{\mathsf{N}} \binom{\mathsf{N}}{\mathsf{n}} P_{U_\mathsf{n}}^{\mathsf{N}-\mathsf{n}} (1 - P_{U_\mathsf{n}})^{\mathsf{n}} P_E^{(\mathsf{n})} \\ &= \sum_{\mathsf{n}=0}^{\mathsf{N}} \frac{\mathsf{N}!}{\mathsf{n}!(\mathsf{N}-\mathsf{n})!} P_{U_\mathsf{n}}^{\mathsf{N}-\mathsf{n}} (1 - P_{U_\mathsf{n}})^{\mathsf{n}} P_E^{(\mathsf{n})} \end{aligned} \tag{3.22}$$

where n is the number of the decoding cooperative devices, and P_{U_n} is the transmission outage probability with maximum decodable rate R_s from S to U_n, which can be calculated as

$$\begin{aligned} P_{U_\mathsf{n}} &= P\left(\max_{\mathsf{k}=1}^{\mathsf{K}} \zeta \log_2\left(1 + P_S|h_{SU_{\mathsf{n},\mathsf{k}}}|^2\sigma_U^{-2}\right) < R_s\right) \\ &= P\left(\max_{\mathsf{k}=1}^{\mathsf{K}} |h_{SU_{\mathsf{n},\mathsf{k}}}|^2 < \frac{2^{\frac{R_s}{\zeta}-1}\sigma_U^2}{P_S}\right) \\ &= \left[1 - Q_1\left(\sqrt{2\kappa}, \sqrt{\frac{2^{\frac{R_s}{\zeta}-1}(1+\kappa_{U_\mathsf{n}})\sigma_U^2}{P_S\Omega}}\right)\right]^{\mathsf{K}}. \end{aligned} \tag{3.23}$$

Next, the estimated secrecy outage probability in the case of n relays and $(\mathsf{N}-\mathsf{n})$ jammers can be calculated as

$$\begin{aligned} P_E^{(\mathsf{n})} &= P\left(C_D^{(\mathsf{n})} - C_E^{(\mathsf{n})} < C_s\right) \\ &= P\left((1-\zeta)\log_2\left(\frac{1+\gamma_D^{(\mathsf{n})}}{1+\gamma_E^{(\mathsf{n})}}\right) < C_s\right) \\ &= P\left(\left[(1-\zeta)\log_2\left(1+\gamma_D^{(\mathsf{n})}\right)\right.\right. \\ &\quad \left.\left. -\ (1-\zeta)\log_2\left(1+\gamma_E^{(\mathsf{n})}\right)\right] < C_s\right). \end{aligned} \tag{3.24}$$

In practice, it is difficult to achieve the exact closed-form expression in such scenario. Hence, it is obtained that the approximate value to calculate the average SINR $\tilde{\gamma}_E^{(\mathsf{n})}$ instead, i.e., $\tilde{\gamma}_E^{(\mathsf{n})} = \mathbb{E}\left[\gamma_E^{(\mathsf{n})}\right]$. Substituting (3.8) and (3.9) into (3.24), $P_E^{(\mathsf{n})}$ can be approximately formulated as

$$\begin{aligned} &P_E^{(\mathsf{n})} \triangleq P\left(\{(1-\zeta)\right. \\ &\times \left[\log_2\left(1+\frac{\sum_{\mathsf{m}=1}^{\mathsf{n}}\sum_{\mathsf{k}=1}^{\mathsf{K}} P_{R_\mathsf{m}}|h_{R_{\mathsf{m},\mathsf{k}}D}|^2}{\sigma_D^2}\right)\right. \\ &\left.\left. -\log_2\left(1+\frac{\sum_{\mathsf{m}=1}^{\mathsf{n}} P_{R_\mathsf{m}}\mathbb{E}\left[\mathbf{h}_{R_\mathsf{m}E}^{\dagger}\boldsymbol{\Lambda}_{R_\mathsf{m}}^{\dagger}\boldsymbol{\Lambda}_{R_\mathsf{m}}\mathbf{h}_{R_\mathsf{m}E}\right]}{\sigma_E^2+\sum_{\mathsf{l}=1}^{\mathsf{N}-\mathsf{n}} P_{J_\mathsf{l}}\mathbb{E}\left[\mathbf{h}_{J_\mathsf{l}E}^{\dagger}\boldsymbol{\Lambda}_{J_\mathsf{l}}^{\dagger}\boldsymbol{\Lambda}_{J_\mathsf{l}}\mathbf{h}_{J_\mathsf{l}E}\right]}\right)\right]\right\} \\ &\left. < C_s\right). \end{aligned} \tag{3.25}$$

The expected value of L-sum Rician fading random variable h_l, i.e., non-central chi-squared fading channel scheme, can be formulated as

$$\mathbb{E}\left[\left(\sum_{l=1}^{L} h_l\right)^2\right] = 2L^2\kappa + \frac{L\Omega}{1+\kappa}. \tag{3.26}$$

Hence, by substituting (3.25) and (3.26) into (3.24), the approximation of estimated secrecy outage probability $P_E^{(\mathsf{n})}$ can be expressed as [90]

$$
\begin{aligned}
P_E^{(\mathsf{n})} &= P\left(C_D^{(\mathsf{n})} < C_s + C_E^{(\mathsf{n})}\right) \\
&\triangleq \begin{cases} 1 - Q_{\mathsf{nK}}\left(\sqrt{2\kappa_R}, \sqrt{\frac{2(\kappa_R+1)}{\Omega}}\sqrt{\frac{\sigma_D^2 2^{\frac{C_s+C_E^{(\mathsf{n})}}{1-\zeta}}-1}{P_R}}\right) & \mathsf{n} \neq 0 \\ 1 & \text{others} \end{cases}
\end{aligned} \tag{3.27}
$$

with

$$
C_E^{(\mathsf{n})} \triangleq (1-\zeta)\log_2\left(1 + \frac{\sum_{\mathsf{m}=1}^{\mathsf{n}} P_{R_{\mathsf{m}}}\left(2\mathsf{K}^2\kappa + \frac{\mathsf{K}\Omega}{1+\kappa}\right)}{\sigma_E^2 + \sum_{\mathsf{l}=1}^{\mathsf{N}-\mathsf{n}} P_{J_{\mathsf{l}}}\left(2\mathsf{K}^2\kappa + \frac{\mathsf{K}\Omega}{1+\kappa}\right)}\right).
$$

3.4 Numerical Results and Discussion

In this section, several Monte-Carlo simulation results are presented along with the analytical calculations for the considered adaptive DF secure communication system. Two scenarios are given in the following results due to the absence of eavesdropper's CSI, i.e., two estimated secrecy scenarios. In case 1 of the secrecy scenario, the channel is set in Rayleigh fading, i.e., $\kappa_E^{\mathsf{JK}} = 0$. The transmission power of S, and cooperative devices are the same, i.e., $P_s = P_r = P_j$; In case 2 of the secrecy scenario, the channel between devices and eavesdropper is set with the same distribution and variance as the the channel between devices and destination, i.e., $\kappa_E^{\mathsf{JK}} = \kappa_D$. Unless otherwise stated, the parameters are set as follows: The channel between the devices and destination $\kappa_D = 5$ dB with the second moment $\Omega = 1$, the power of AWGN $\sigma_U^2 = \sigma_D^2 = \sigma_E^2 = -175$ dBm, the maximum achievable rate $R_s = 15$ dB, the minimum secrecy capacity $C_s = 5$ dB, and time ratio $\zeta = 0.5$.

In Fig. 3.2, the destination outage probability versus transmission power, both analytical results and corresponding simulations are plotted. From the figure, it can observe that as the number of devices and the number of antennas increase, the outage probability decreases. This is because by increasing the number of devices, the received average rate at destination will also linearly increase.

In Fig. 3.3, we plot the outage probability of the eavesdropper with respect to the transmission power in both analytical results and simulations with $\mathsf{N}, \mathsf{K} \in \{2, 6, 10\}$. From this figure, it can observe that the gap between case 1 and case 2 of the estimated secrecy scenario is related to the number of cooperative devices. With the increase of the cooperative devices and total antennas,

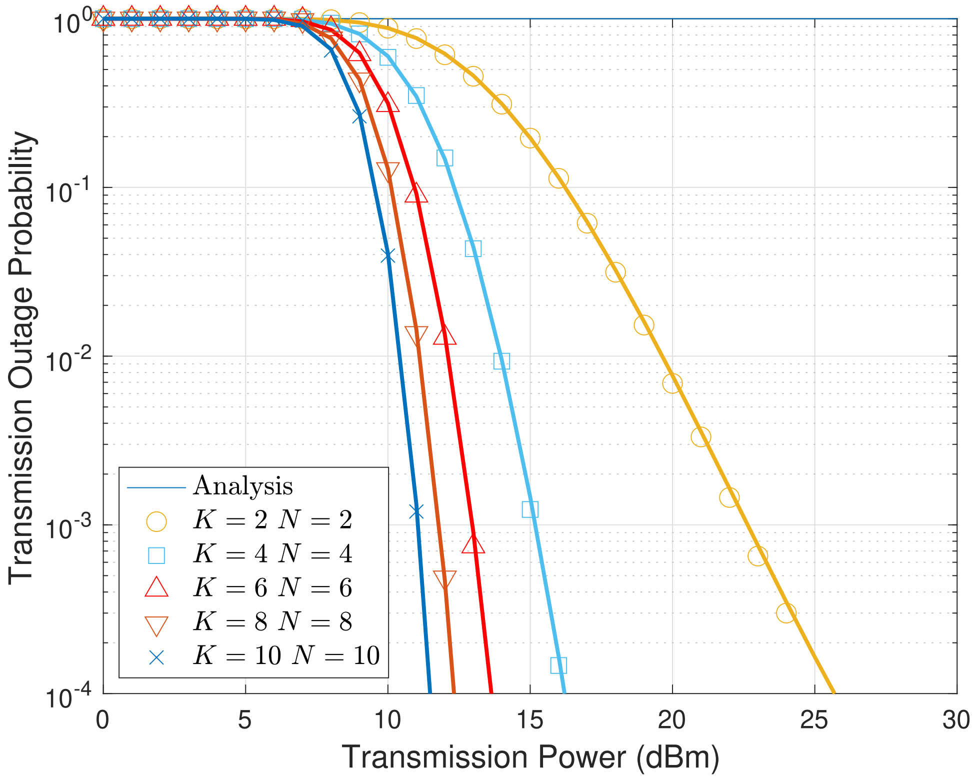


Figure 3.2: The outage probability of destination versus transmission power.(Solid line: analysis; markers:simulation. Parameters: the number of cooperative devices $\mathsf{N} \in \{2,4,6,8,10\}$, the antenna number of eace device $\mathsf{K} \in \{2,4,6,8,10\}$).

the transmission channels are more significantly affected by the channel fading coefficients.

Finally, in Fig. 3.4, we investigate the relationship between the estimated secrecy outage probability with respect to the transmission power. It can easily observe from the figure that there is an optimal transmission power for all the estimated secrecy scenarios in case 2 and in case 1 of the estimated secrecy scenario of $\{\mathsf{K}=2,\mathsf{N}=2\}$ and $\{\mathsf{K}=6,\mathsf{N}=6\}$. However, while $\{\mathsf{K}=10,\mathsf{N}=10\}$, the probabilities of secrecy outage are different between the two estimated scenarios. This is because in the case of the first estimated secrecy scenario of $\{\mathsf{K}=10,\mathsf{N}=10\}$, the average secrecy capacity is more significant than the minimum secrecy capacity, and in the scenario of all the cooperative devices operating as a relay, which leads to the decrease in the estimated secrecy outage probability.

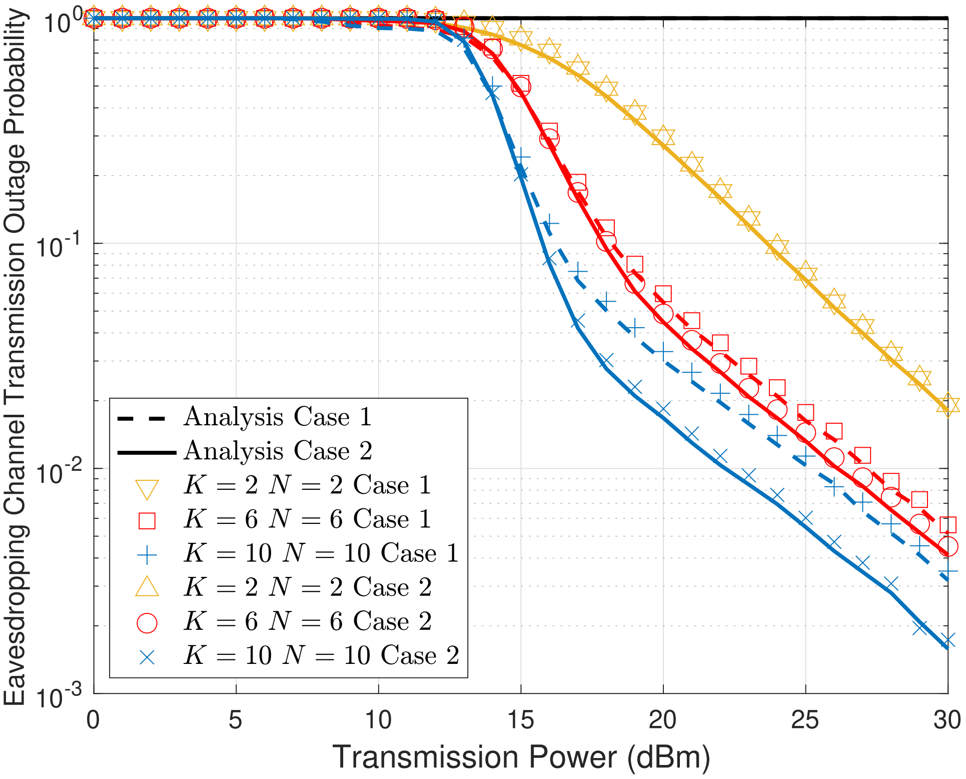


Figure 3.3: The outage probability of eavesdropper versus transmission power. (Dash line: Analysis results of estimated secrecy scenario in case 1; Solid line: Analysis results of estimated secrecy scenario in case 2; Markers: Simulation results. Parameters: the number of cooperative devices N $\in \{2, 6, 10\}$, the antenna number of each device K $\in \{2, 6, 10\}$.)

3.5 Conclusion

In this chapter, the outage probabilities of a multiple-antenna equipped cooperative relaying network with a single eavesdropper without CSI information has been analyzed. The cooperative devices that have successfully decoded the information from source serve as relaying and otherwise they serve as jammers. The multiple-antenna equipped devices form the beam to destination via accessing the full CSI to destination. The closed-form expression of the main channel, the asymptotic lower bound of the eavesdropper channel, and the approximated closed-form expression of the secrecy outage probability have been derived. The numerical comparisons have shown that the analytical expressions and simulation results using Monte-Carlo method match well, suggesting the accuracy of our analytical approach. The results also suggest that there is an optimal power for the worst case of secrecy scenario. Optimizing the power allocation at relay

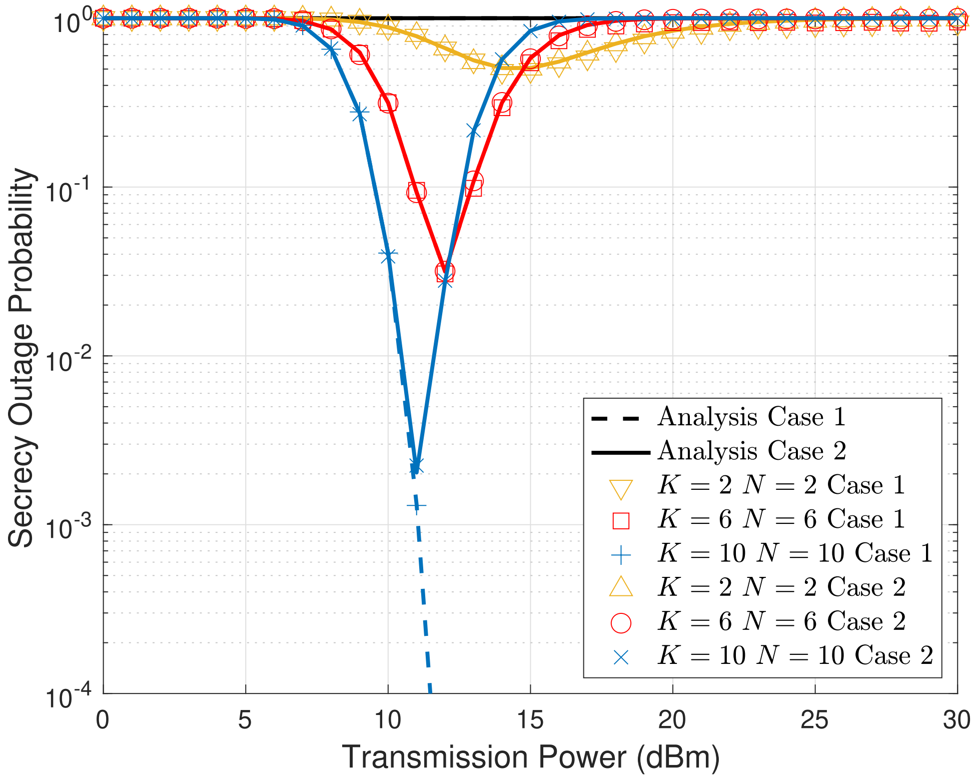


Figure 3.4: The estimated secrecy outage probability versus transmission power ratio. (Dash line: Analysis results of the estimated secrecy scenario in case 1; Solid line: Analysis results of the estimated secrecy scenario in case 2; Markers: Simulation results. Parameters: the number of cooperative devices N $\in \{2, 6, 10\}$, the antenna number of each device K $\in \{2, 6, 10\}$.)

via water-filling algorithm will be left for future work.

Chapter 4

Performance Analysis of Secure Relaying Network Based on Cooperative UAV Swarm Over Rician Fading Channels

In this chapter, a UAV-aided cooperative relaying network is analyzed, which consists of one source representing GS, one destination, and M UAV-aided relays along with a single UAV-aided eavesdropper. Part of this chapter was presented in [92].

4.1 Introduction

The use of small unmanned aerial vehicles (UAVs) has recently gained much attention for wireless communications due to their on-demand mobility and deployment flexibility (e.g., [35, 93, 94]). In UAV networks, wireless channels between ground control unit or ground station (GS) and UAVs generally experience near line-of-sight (LoS) propagation and thus often modeled as Rician fading [95]. On the other hand, as the channel is close to ideal, its security against eavesdropping becomes another concern in wireless networks, and physical layer security approaches have received significant recent interest. For example, in [96], the secrecy performance of a multi-hop selective UAV-aided relaying system with M transmitters has been investigated. In [97], the optimum power allocation and trajectory in view of physical layer security for a UAV-aided relaying network has been studied.

In this chapter, we investigate the performance of UAV-aided selective relaying network with jammer selection over Rician fading channel, where multiple UAV relays serve for a GS over unreliable wireless channels, and the selected UAV will relay information to a destination. In particular, considering the fact that the eavesdropper also needs to deliver its information to the backhaul through wireless channels even after its successful interception, the impact of the backhaul reliability on the resulting performance is considered, which similar to [98, 99]. The main contributions of this work are summarized as follows:

- Depending on the functionality of UAV relays, four different UAV-based collaborative relaying and jamming approaches are introduced and compared that may require different computational complexity, synchronizability, as well as channel knowledge.

- Based on widely accepted Rician fading models for the air-to-air (A2A) and air-to-ground (A2G) links in conjunction with a low-altitude UAV swarm scenario, the four approaches are theoretically analyzed in terms of transmission outage probabilities of the main channel and eavesdropping channel and develop their mathematical expressions that are readily calculated. For the eavesdropping channel, the effect of its backhaul reliability is also taken into account in our analysis.

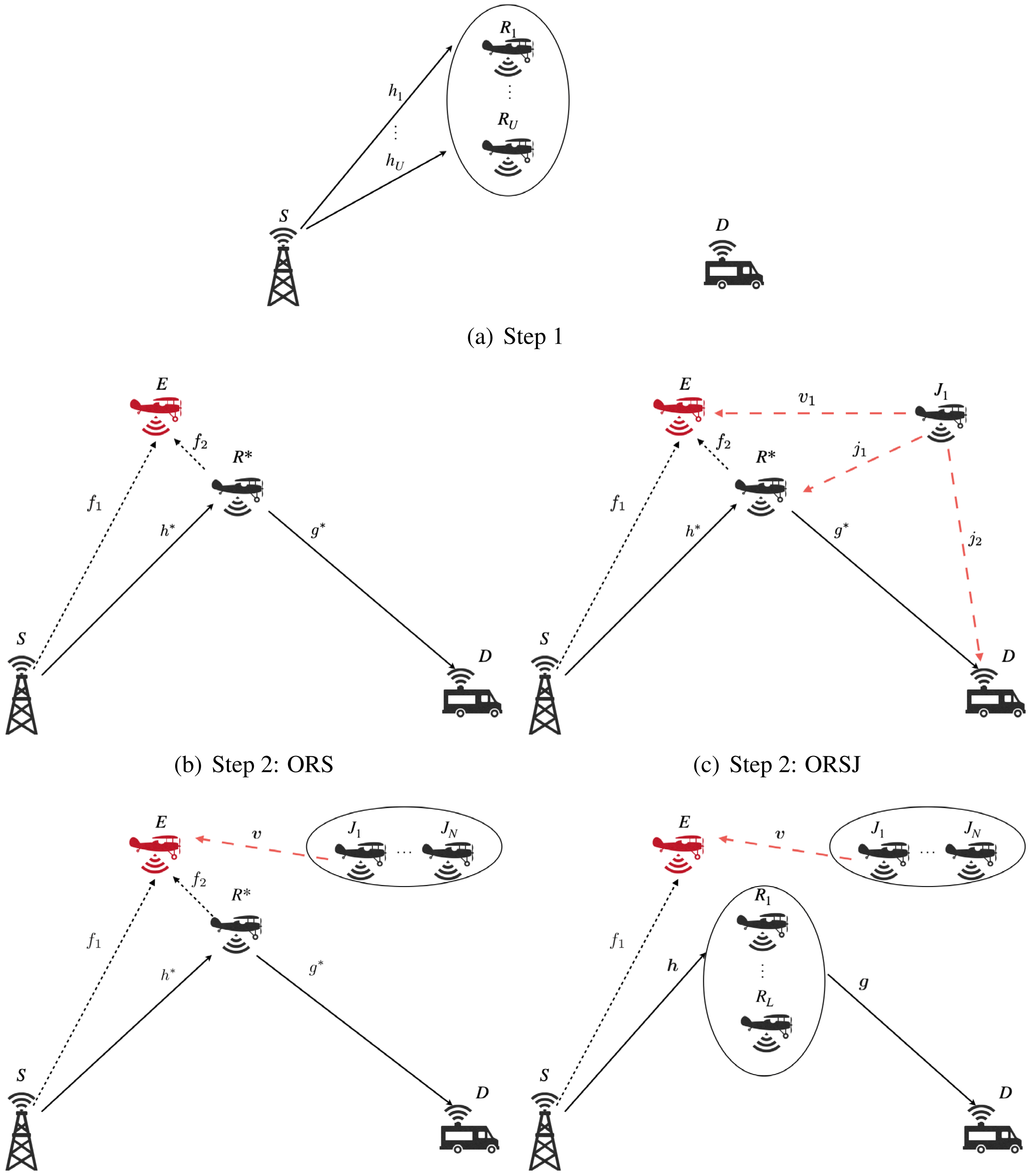
- Using the developed theoretical results, we demonstrate the trade-off relationship between the transmission outage probabilities of the main channel and eavesdropping channel.

The rest of this chapter is organized as follows. Section 4.2 presents the system and channel model of UAV-aided relaying network with jammer selection considered throughout this chapter, and their performances are theoretically analyzed in Section 4.3. Some numerical examples of the transmission outage probability of both main channel and eavesdropping channel based on the developed analytical expressions as well as simulations are presented in Section 4.4. Finally, Section 4.5 concludes this work.

Notation: Throughout this chapter, the following notations are adopted. $f_\varphi(\cdot)$, $F_\varphi(\cdot)$, and $\mathcal{M}_\varphi(\cdot)$ denote the probability density function (PDF), cumulative distribution function (CDF), and moment generating function (MGF) of the random variable (RV) φ, respectively. $\mathcal{L}^{-1}\left(F(s)\right)$ is the inverse Laplace transform (ILT) of the function $F(s)$ [100, §2.4.3]. The following special functions will be used: the Gamma function $\Gamma(\cdot)$ [87, §8.310], the ν-th order modified Bessel function of the first kind $I_\nu(\cdot)$ [87, §8.406], the Kummer confluent hypergeometric function of the first kind ${}_1F_1(\alpha,\gamma;z)$ [87, §9.210], the Whittaker function $M_{\lambda,\mu}(z)$ [87, §9.220], the ν-th order Marcum-Q function $Q_\nu(\cdot)$ [86], the Dirac Delta function $\delta(x)$ [100, §1.17], and the Pochhammer index $(a)_n$ [100, §5.2(iii)].

4.2 System Model and Channel Assumption

Fig. 4.1 illustrates the UAV-aided selective relaying network, where a source (S) GS communicates with a destination (D) via U intermediate UAV-aided relays ($R_1, ..., R_U$) that provide G2A and A2G links, in the presence of a single UAV-aided eavesdropper (E). All the communicating devices are assumed to be equipped with a single antenna, and operate in a half-duplex



(a) Step 1

(b) Step 2: ORS

(c) Step 2: ORSJ

(d) Step 2: ORSMJ

(e) Step 2: MRCMJ

Figure 4.1: An illustration of the UAV-aided selective relaying network.

mode, i.e., it cannot transmit and receive the signal simultaneously. Due to the large path-loss and obstacles, the direct link between S and D does not exist in our assumption.

4.2.1 Compared Models

In what follows, the UAV swarm operates as follows in our assumption:

1. S broadcasts the guidance signal to all the relays, and they estimate their channel gain from S (Step 1 of Fig. 4.1), where the complex channel coefficient from S to the uth relay R_u is given by h_u, with $u \in \{1, 2, \cdots, U\}$. Among U relays, L relays, denoted by $R_\ell,\ \ell \in \{1, 2, ..., L\}$ $(L \leq U)$ in what follows, will be selected by the source based on the predetermined rule.

2. L selected UAV nodes will then serve as relay nodes, and among the residual $(U - L)$ relays, N relays will act as cooperative jammers, denoted by $J_1, J_2, ..., J_N$ $(L + N \leq U)$.

3. In step 2, the two-phase relaying based on the decode-and-forward (DF) protocol will be performed. During this step (over the two successive phases), each jammer broadcasts its artificial noise (AN) with identical power P_j to protect the information signal from E.

In step 2, the following four approaches for relay and jammer selection shown in Fig. 4.1 (b)-(e) are investigated:

Optimal Relay Selection (ORS)

This model does not employ artificial noise generation, and it selects only one relay, denoted by R^*, that has the best performance between all $S \rightarrow R_\ell$ channels among the available relays (i.e., $L = 1$ and $N = 0$). This corresponds to the case in Fig. 4.1(b).

Optimal Relay Selection and Jamming (ORSJ)

This model is an extension of ORS model, and selects two relays ($L = 1$ and $N = 1$) among the multiple available relays such that one relay R^* that has the best performance among $S \rightarrow R_\ell$ channels is employed for signal forwarding in the second phase, whereas the other randomly selected relay, denoted by J_1, serves as a jammer over the two successive phases in step 2. This corresponds to the case in Fig. 4.1(c). Since only one jammer transmits AN without beamforming, both destination and eavesdropper are affected.

Optimal Relay Selection with Multiple Jamming (ORSMJ)

This model is an extension of ORSJ, and it selects one relay R^* among the available relays such that the instantaneous received signal-to-noise ratio (SNR) at the relay is maximized, whereas the remaining UAV transmitters, which act as jammers, collaboratively form a beam in a distributed manner [101] to prevent eavesdropper from receiving information. (Here, it is assumed that the relays have the knowledge of the direction of E and the selected jammers have synchronizability to perform beamforming.) This corresponds to the case in Fig. 4.1(d).

Multiple Relay Combining with Multiple Jamming (MRCMJ)

In this model, S randomly picks up L UAV relays and N UAV jammers upon forwarding information in step 2. The UAV relays use collaborative beamforming strategy to forward information to D [101] in the second phase. More specifically, in addition to the same beamforming capability of jammers as ORSMJ model, the perfect beamforming of information signal in $R_\ell \to D$ links is also assumed such that E can only receive information from S in the first phase. This corresponds to the case in Fig. 4.1(e).

Let $\gamma_{A\to B}$ denote the signal-to-interference-plus-noise ratio (SINR) of the link from node A to B. In order to simplify our subsequent analysis, in ORS, ORSJ, and ORSMJ scenarios, R^* has the highest SINR (more precisely, SNR in this case) upon relaying the received information from the source in our assumption, i.e.,

$$\gamma_{S\to R^*} \triangleq \max_{u\in\{1,2,\cdots,U\}} \{\gamma_{S\to R_u}\} \tag{4.1}$$

and the overhead required for selection of the best relay will be assumed to be negligible.

4.2.2 Channel Assumptions

The notations used for channel coefficients throughout this work are introduced in Fig. 4.1: h_u corresponds to that of S to the relay R_u (with h^* representing that of R^*) and g_ℓ corresponds to that of R_ℓ to D (with g^* representing that of R^*). Furthermore, f_1 corresponds to that of S to E in the first phase and f_2 corresponds to that of R^* to E in the second phase. In the case of ORSJ, the link of the selected jammer J_1 to the selected relay R^* and that of J_1 to D are given by j_1 and j_2, respectively. Finally, v_n is also used to denote the link from the jammer J_n to E. Note that due to the spatial separation, all the channel coefficients are assumed to be statistically independent in what follows.

Due to the UAV-aided scenario, G2A (or A2G) and A2A channels contain a line-of-sight (LoS) component and thus the channel coefficients are modeled by Rician fading [95]. More specifically, h_u with $u \in \{1,2,...,U\}$, g_ℓ with $\ell \in \{1,2,...,L\}$, v_n with $n \in \{1,2,...,N\}$, and f_1 and f_2 are all assumed to be complex Gaussian random variables with their second moments (e.g. $\mathbb{E}\left[|h_u|^2\right]$) given by Ω. In this case, the PDF of its squared envelope, i.e., $z = |h_u|^2$, follows the non-central chi-square distribution with two degrees of freedom [102]:

$$f_Z(z) = \frac{K+1}{\Omega} e^{-\left(K+\frac{(K+1)z}{\Omega}\right)} I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega}}\right) \tag{4.2}$$

where K is a Rician factor. In what follows, it is assumed that the Rician factors of G2A (or A2G) and A2A channels are characterized by K_G and K_A, respectively. Also, the case with $K_A \to \infty$ is separately considered, i.e., the A2A channel is characterized by an AWGN channel without fading, whereas K_G is always bounded. Likewise, κ_G and κ_A are also used to denote the path-loss factors associated with G2A (or A2G) and A2A channels, respectively. In general, the path-loss of G2A (or A2G) is more severe than that of A2A, and thus $\kappa_G \ll \kappa_A$ is derived in general.

4.2.3 Backhaul Reliability of E

In practice, the eavesdropper E should also send the received information to its own destination. It is assumed that even if E can successfully decode the information, it may fail in delivering it to its own destination due to fading and other imperfections in its backhaul. When a backhaul transmission fails, in order to focus on the impact of backhaul reliability in terms of the secrecy performance, additional coding, automatic repeat request (ARQ), and power control are not considered. The backhaul reliability of E is defined as a random variable, and assume that it follows a Bernoulli distribution independent of source message as in [98, 99]. Let $\mathbb{B}_1$ and $\mathbb{B}_2$ denote reliability indicators of communications during the first and second phases in step 2, respectively. In this work, both $\mathbb{B}_1$ and $\mathbb{B}_2$ are assumed to be Bernoulli random variables chosen from $\{0, 1\}$ with probabilities $1-q$ and q, respectively, where 0 and 1 indicate loss of backhaul connection and successful backhaul connection. In other words, q is the probability of successful backhaul connection of E.

4.2.4 SINR of Main Channel

Let γ_D denote the instantaneous SINR observed at the destination. In the cases of ORS,ORSJ, and ORSMJ, it is assumed that S transmits guidance signal to the relays such that the optimal relay R^* is selected according to (4.1) in step 1. After that, the remaining relays will be divided into the two parts: N relays will act as the UAV jammers, which will broadcast AN with the power P_j during the the first and second phases of step 2. The other $(U-N-1)$ relays will keep silence to save energy for the next transmission. With respect to the DF relaying protocol, the end-to-end SINR associated with the overall link $S \rightarrow R^* \rightarrow D$ of step 2 can be expressed as

$$\gamma_D = \min(\gamma_{S \rightarrow R^*}, \gamma_{R^* \rightarrow D}). \tag{4.3}$$

In the case of MRCMJ, on the other hand, the UAV-aided relays forward its information with ideal beamforming scheme in the second phase. Therefore, the received SINR at D can be expressed as [71]

$$\gamma_D^{\mathrm{MRCMJ}} = \sum_{\ell=1}^{L} \min\left(\gamma_{S \rightarrow R_\ell}, \gamma_{R_\ell \rightarrow D}\right). \tag{4.4}$$

4.2.5 SINR of Eavesdropper Channel

It is assumed that the eavesdropper operates in a greedy mode, i.e., it attempts to intercept the signals transmitted from both S and R^* over the two phases. In order to maximize the total received SINR, the eavesdropper intelligently proceeds detection using maximum ratio combining (MRC) across all the received signals from S and R^*. Hence, the instantaneous received SINR with MRC by E can be expressed as [103]

$$\gamma_E = \gamma_{S \rightarrow E} + \gamma_{R^* \rightarrow E} \tag{4.5}$$

where $\gamma_{S \rightarrow E}$ and $\gamma_{R^* \rightarrow E}$ are the received SINRs of the first and second phases, respectively.

4.2.6 SINR Expressions

In what follows, SINR expressions γ_D and γ_E are developed for each of the four models, which described in Section 4.2.1.

ORS

In this model, there is no interference observed by the relay and destination. Hence, the corresponding instantaneous SINR of the main channel in the first phase can be expressed as

$$\gamma_{S \rightarrow R^*}^{\mathrm{ORS}} = \frac{\kappa_G P_0 |h^*|^2}{P_n} \tag{4.6}$$

where h^* is the channel coefficient of the link from S to the selected relay R^* (as described in Section 4.2.2), P_0 is the transmission power of S, and P_n is the power of the additive white Gaussian noise (AWGN) observed at the receiver. Similarly, in the second phase for the communication between R^* and D, we have

$$\gamma_{R^*\to D}^{\text{ORS}} = \frac{\kappa_G P_0 |g^*|^2}{P_n} \tag{4.7}$$

where g^* is the channel coefficient of the link from R^* to D. It is also assumed that the selected relay transmits its signal with the same power P_0 as that of S for simplicity. Since both communications take place over ground and air, the path-loss is modeled by the same parameter κ_G for simplicity as discussed in Section 4.2.2. The end-to-end instantaneous SINR over the two phases can be expressed by (4.3) with (4.6) and (4.7).

For the eavesdropping channel, the SNR of the eavesdropper received from S in the first phase can be expressed as

$$\gamma_{S\to E}^{\text{ORS}} = \frac{\kappa_G \mathbb{B}_1 P_0 |f_1|^2}{P_n} \tag{4.8}$$

where $\mathbb{B}_1$ denotes the reliability of backhaul in the first phase defined in Section 4.2.3. Similarly, the SNR of the eavesdropper received from R^* in the second phase can be expressed as

$$\gamma_{R^*\to E}^{\text{ORS}} = \frac{\kappa_A \mathbb{B}_2 P_0 |f_2|^2}{P_n}. \tag{4.9}$$

The resulting end-to-end SNR of E is given by (4.5) with (4.8) and (4.9), i.e.,

$$\gamma_E^{\text{ORS}} = \frac{\kappa_G \mathbb{B}_1 P_0 |f_1|^2 + \kappa_A \mathbb{B}_2 P_0 |f_2|^2}{P_n}. \tag{4.10}$$

ORSJ

This model differs from ORS in that it has a single jammer during the two phases. Therefore, the instantaneous SINR observed by R^* can be expressed as

$$\gamma_{S\to R^*}^{\text{ORSJ}} = \frac{\kappa_G P_0 |h^*|^2}{P_n + \kappa_A P_j |j_1|^2} \tag{4.11}$$

where P_j is the transmit power of the jammer. Similarly, the SINR observed by D in the second phase can be expressed as

$$\gamma_{R^* \to D}^{\text{ORSJ}} = \frac{\kappa_G P_0 |g^*|^2}{P_n + \kappa_G P_j |j_2|^2}. \tag{4.12}$$

The end-to-end instantaneous SINR over the two phases can be expressed by (4.3) with (4.11) and (4.12).

For the eavesdropper channel, we have

$$\gamma_{S \to E}^{\text{ORSJ}} = \frac{\kappa_G P_0 \mathbb{B}_1 |f_1|^2}{P_n + \kappa_A P_j |v_1|^2} \tag{4.13}$$

and

$$\gamma_{R^* \to E}^{\text{ORSJ}} = \frac{\kappa_A P_0 \mathbb{B}_2 |f_2|^2}{P_n + \kappa_A P_j |v_1|^2}. \tag{4.14}$$

Therefore, the end-to-end instantaneous SINR is given by

$$\gamma_{E}^{\text{ORSJ}} = \frac{\kappa_G P_0 \mathbb{B}_1 |f_1|^2 + \kappa_A P_0 \mathbb{B}_2 |f_2|^2}{P_n + \kappa_A P_j |v_1|^2}. \tag{4.15}$$

ORSMJ

This model differs from ORSJ in that multiple jammers are randomly selected, and they form an ideal beam of AN to the eavesdropper. By assumption, the effect of jammers can be ignored for the selected relay R^*. Therefore, as is apparent by comparing Fig. 4.1 (b) and (d), in this model, the end-to-end SINR expression of the main channel is the same as that of ORS.

For the eavesdropping channel, similar to (4.15), the end-to-end instantaneous SINR over two phases can be expressed as

$$\gamma_{E}^{\text{ORSMJ}} = \frac{\kappa_G P_0 \mathbb{B}_1 |f_1|^2 + \kappa_A P_0 \mathbb{B}_2 |f_2|^2}{P_n + \kappa_A P_j \sum_{n=1}^{N} |v_n|^2}. \tag{4.16}$$

MRCMJ

In this case, the end-to-end instantaneous SNR over two phases can be expressed by (4.4), where

$$\gamma_{S\to R_\ell}^{\mathrm{MRCMJ}} = \frac{\kappa_G P_0 |h_\ell|^2}{P_n} \tag{4.17}$$

and

$$\gamma_{R_\ell\to D}^{\mathrm{MRCMJ}} = \frac{\kappa_G P_0 |g_\ell|^2}{P_n}. \tag{4.18}$$

For the eavesdropping channel, by assumption the eavesdropper cannot receive any information in the second phase due to the ideal beamforming by multiple relays. Hence, the instantaneous received SINR by E is degraded from (4.16) and expressed as

$$\gamma_{E}^{\mathrm{MRCMJ}} = \frac{\kappa_G P_0 \mathbb{B}_1 |f_1|^2}{P_n + \kappa_A P_j \sum_{n=1}^{N} |v_n|^2}. \tag{4.19}$$

4.3 Performance Analysis

In this section, the analytical expressions of the transmission outage probabilities for the four UAV-based relaying and jamming approaches defined in the previous section are derived. Throughout the rest of this chapter, the outage event is defined such that a given instantaneous SINR is less than the required threshold level γ_{th}, and the transmission outage probability is defined as

$$P_{\mathrm{out}}\left(\gamma_{\mathrm{th}}\right) = \Pr\left(\gamma < \gamma_{\mathrm{th}}\right) \tag{4.20}$$

where $\gamma = \gamma_D$ and γ_E for the main channel and eavesdropping channel, respectively.

Due to the difficulty in the derivation of simple mathematical expressions, in several models our derivations are restricted to the following two cases: 1) K_A and K_G are assumed to be identical, i.e., $K_A = K_G = K$; 2) the fading effect of A2A is negligible ($K_A \to \infty$) and thus K_G is the only parameter that should be taken into account. It is noted that even though the former case may not necessarily reflect practical environment, it may still serve as a useful theoretical bound (or approximation) when the fading effect of A2A link is as severe as that of G2A.

4.3.1 Outage Probabilities for Main Channel

ORS

In ORS, the transmission outage probability for the main channel link, (i.e., $S \to R^* \to D$), can be expressed as

$$\begin{aligned} P_{\text{out}}^{\text{ORS}-\text{M}}(\gamma_{\text{th}}) &= 1 - \Pr\left(\gamma_{S\to R^*}^{\text{ORS}} > \gamma_{\text{th}}\right) \Pr\left(\gamma_{R^*\to D}^{\text{ORS}} > \gamma_{\text{th}}\right) \\ &= 1 - \left(1 - \prod_{u=1}^{U} \Pr(\gamma_{S\to R_u}^{\text{ORS}} < \gamma_{\text{th}})\right) \left(1 - \Pr\left(\gamma_{R^*\to D}^{\text{ORS}} < \gamma_{\text{th}}\right)\right), \end{aligned} \tag{4.21}$$

where

$$\begin{aligned} \Pr(\gamma_{S\to R_u}^{\text{ORS}} < \gamma_{\text{th}}) &= \Pr\left(\gamma_{R^*\to D}^{\text{ORS}} < \gamma_{\text{th}}\right) \\ &= 1 - Q_1\left(\sqrt{2K_G}, \sqrt{\frac{2(K_G+1)}{\Omega}}\sqrt{\frac{P_n\gamma_{\text{th}}}{\kappa_G P_0}}\right). \end{aligned} \tag{4.22}$$

It is noted that this model does not involve A2A link for the main channel.

ORSJ

Similar to (4.21), the transmission outage probabilities for the main channel link can be expressed as

$$P_{\text{out}}^{\text{ORSJ}-\text{M}}(\gamma_{\text{th}}) = 1 - \left(1 - \prod_{u=1}^{U} \Pr(\gamma_{S\to R_u}^{\text{ORSJ}} < \gamma_{\text{th}})\right) \left(1 - \Pr\left(\gamma_{R^*\to D}^{\text{ORSJ}} < \gamma_{\text{th}}\right)\right), \tag{4.23}$$

where

$$\Pr\left(\gamma_{S\to R_u}^{\text{ORSJ}} < \gamma_{\text{th}}\right) = \Pr\left(\frac{\kappa_G P_0 |h|^2}{P_n + \kappa_A P_j |j_1|^2} < \gamma_{\text{th}}\right) \tag{4.24}$$

$$\geq \Pr\left(\frac{\kappa_G P_0 |h|^2}{\kappa_A P_j |j_1|^2} < \gamma_{\text{th}}\right) \triangleq \Pr_{L,1}^{\text{ORSJ}}(\gamma_{\text{th}}) \tag{4.25}$$

$$\mathrm{Pr}_{L,1}^{\mathrm{ORSJ}}(\gamma_{\mathrm{th}}) = Q_1\left(\sqrt{\frac{2K\kappa_A P_j\gamma_{\mathrm{th}}}{\kappa_A P_j\gamma_{\mathrm{th}}+\kappa_G P_0}}, \sqrt{\frac{2K\kappa_G P_0}{\kappa_A P_j\gamma_{\mathrm{th}}+\kappa_G P_0}}\right) - \frac{e^{-K}\kappa_G P_0}{\kappa_A P_j\gamma_{\mathrm{th}}+\kappa_G P_0} I_0\left(\frac{2K\sqrt{\kappa_G P_0\kappa_A P_j\gamma_{\mathrm{th}}}}{\kappa_A P_j\gamma_{\mathrm{th}}+\kappa_G P_0}\right) \tag{4.28}$$

$$\mathrm{Pr}_{L,2}^{\mathrm{ORSJ}}(\gamma_{\mathrm{th}}) = Q_1\left(\sqrt{\frac{2KP_j\gamma_{\mathrm{th}}}{P_0+P_j\gamma_{\mathrm{th}}}}, \sqrt{\frac{2KP_0}{P_0+P_j\gamma_{\mathrm{th}}}}\right) - \frac{e^{-K}P_0}{P_0+P_j\gamma_{\mathrm{th}}} I_0\left(\frac{2K\sqrt{P_0P_j\gamma_{\mathrm{th}}}}{P_0+P_j\gamma_{\mathrm{th}}}\right) \tag{4.29}$$

and

$$\Pr\left(\gamma_{R^*\to D}^{\mathrm{ORSJ}} < \gamma_{\mathrm{th}}\right) = \Pr\left(\frac{\kappa_G P_0|g|^2}{P_n+\kappa_G P_j|j_2|^2} < \gamma_{\mathrm{th}}\right) \tag{4.26}$$

$$\geq \Pr\left(\frac{P_0|g|^2}{P_j|j_2|^2} < \gamma_{\mathrm{th}}\right) \triangleq \mathrm{Pr}_{L,2}^{\mathrm{ORSJ}}(\gamma_{\mathrm{th}}). \tag{4.27}$$

Since the exact probabilities of (4.24) and (4.26) are mathematically intractable, the lower bounds defined in (4.25) and (4.27) will be considered, which is a consequence of eliminating the noise power term P_n (i.e., high SNR and thus interference-limited regime) in what follows.

Theorem 1. *Under the assumption of $K_G = K_A = K$, the lower bounds for one-hop outage probabilities of ORSJ model defined in* (4.25) *and* (4.27) *can be expressed by* (4.28) *and* (4.29) *shown at the top of the next page.*

Proof. See Appendix A.1. □

In the case that A2A link is modeled by AWGN (i.e., $K_A \to \infty$), the exact probabilities corresponding to (4.24) and (4.26) are replaced by

$$\Pr\left(\gamma_{S\to R_u}^{\mathrm{ORSJ}} < \gamma_{\mathrm{th}}\right) = 1 - Q_1\left(\sqrt{2K_G}, \sqrt{\frac{2(K_G+1)}{\Omega}}\sqrt{\frac{(P_n+\kappa_A P_j)\gamma_{\mathrm{th}}}{\kappa_G P_0}}\right), \tag{4.30}$$

$$\Pr\left(\gamma_{R^*\to D}^{\mathrm{ORSJ}} < \gamma_{\mathrm{th}}\right) = 1 - Q_1\left(\sqrt{2K_G}, \sqrt{\frac{2(K_G+1)}{\Omega}}\sqrt{\frac{(P_n+\kappa_G P_j)\gamma_{\mathrm{th}}}{\kappa_G P_0}}\right). \tag{4.31}$$

ORSMJ

As mentioned in Section 4.2.6, the SINR expression of ORSMJ model in the case of the main channel is the same as that of ORS. Therefore, its outage probability is equal to (4.22).

MRCMJ

In this case, the outage probability is expressed from (4.4) as

$$\begin{aligned} P_{\text{out}}^{\text{MRCMJ}}(\gamma_{\text{th}}) &= \Pr\left(\gamma_D^{\text{MRCMJ}} < \gamma_{\text{th}}\right) \\ &= \Pr\left(\sum_{\ell=1}^{L} Z_\ell < \frac{P_n \gamma_{\text{th}}}{\kappa_G P_0}\right) \end{aligned} \tag{4.32}$$

where

$$Z_\ell = \min\left(|h_\ell|^2, |g_\ell|^2\right) \tag{4.33}$$

and thus its CDF is given by

$$F_{Z_\ell}(\gamma) = \Pr\left(Z_\ell < \gamma\right) = 1 - \Pr\left(|h_\ell|^2 > \gamma\right)\Pr\left(|g_\ell|^2 > \gamma\right). \tag{4.34}$$

As observed in (4.32), the exact analysis requires the probability distribution of the sum of squared Rician random variables, which involves Marcum-Q functions and thus hinders further mathematical manipulation. Therefore, an alternative approach based on the approximation of Rician fading by Nakagami-m fading is often adopted. Specifically, the PDF of $X_\ell = |h_\ell|^2$ (or equivalently $X_\ell = |g_\ell|^2$) is replaced by

$$f_{X_\ell}(x) = \frac{e^{-\frac{mx}{\Omega}}\left(\frac{m}{\Omega}\right)^m x^{m-1}}{\Gamma(m)} \tag{4.35}$$

where the parameter m can be related to the Rician factor K by [104]

$$m = \frac{(K+1)^2}{2K+1}. \tag{4.36}$$

In the case of Nakagami-m fading, (4.34) can be expressed as

$$F_{Z_\ell}(\gamma) = 1 - \Gamma^2\left(m, \frac{m\gamma}{\Omega}\right) \tag{4.37}$$

and its PDF is

$$f_{Z_\ell}(\gamma) = 2\frac{e^{-\frac{mx}{\Omega}}\left(\frac{m}{\Omega}\right)^m \gamma^{m-1}\Gamma(m, \frac{m\gamma}{\Omega})}{\Gamma(m)}. \tag{4.38}$$

The MGF of Z_ℓ can be expressed by the Laplace transform of the corresponding PDF [87, §6.455.1], i.e.,

$$\begin{aligned}\mathcal{M}_{Z_\ell}(s) &= \mathcal{L}\left(f_{Z_\ell}(\gamma)\right)(s)\\ &= \frac{2\left(\frac{m}{\Omega}\right)^m}{\Gamma(m)}\int_0^\infty e^{-\left(s+\frac{m}{\Omega}\right)\gamma}\gamma^{m-1}\Gamma\left(m, \frac{m\gamma}{\Omega}\right)d\gamma\\ &= \frac{2\Gamma(2m)_2F_1\left(1, 2m; 1+m; \frac{m+s\Omega}{2m+s\Omega}\right)}{m\Gamma(m)}\left(\frac{m}{2m+s\Omega}\right)^{2m}.\end{aligned} \tag{4.39}$$

Finally, the outage probability of the main channel can be numerically calculated through the inverse Laplace transform (ILT) as

$$P_{\text{out}}^{\text{MRCMJ}-\text{M}}(\gamma_{\text{th}}) = \mathcal{L}^{-1}\left(\frac{\mathcal{M}_{Z_\ell}^L(s)}{s}\right)\Bigg|_{s=\frac{P_n\gamma_{\text{th}}}{\kappa_G P_0}}. \tag{4.40}$$

This model does not involve A2A link for the main channel.

4.3.2 Outage Probabilities for Eavesdropping Channel

ORS

In this case, a UAV does not serve as a jammer. Similar to the main channel, the outage probability of eavesdropper channel based on SNR in (4.10) can be calculated as

$$\begin{aligned}P_{\text{out}}^{\text{ORS}-\text{E}}(\gamma_{\text{th}}) &= \Pr(\gamma_E < \gamma_{\text{th}})\\ &= \Pr\left(\frac{P_0(\kappa_G\mathbb{B}_1|f_1|^2 + \kappa_A\mathbb{B}_2|f_2|^2)}{P_n} < \gamma_{\text{th}}\right).\end{aligned} \tag{4.41}$$

For convenience, we assume that $\mathbb{B}_1$ and $\mathbb{B}_2$ are statistically independent. In the case of Rician fading the PDF of $X_1 = \mathbb{B}_1|f_1|^2$ can be expressed as [105]

$$f_{X_1}(\gamma) = (1-q)\delta(\gamma) + qe^{-\left(\frac{\gamma(1+K_G)}{\Omega}+K_G\right)}\left(\frac{1+K_G}{\Omega}\right)I_0\left(2\sqrt{\frac{K_G(1+K_G)\gamma}{\Omega}}\right) \tag{4.42}$$

where q is the probability of successful backhaul connection for E as defined in Section 4.2.3.

The MGF of (4.42) can be expressed as

$$\begin{aligned}\mathcal{M}_{X_1}(s) &= \mathcal{L}\left(f_{X_1}(\gamma)\right)\\ &= 1-q+q\int_0^\infty e^{-\left(\frac{\gamma(1+K_G)}{\Omega}+K_G+\gamma s\right)}\left(\frac{1+K_G}{\Omega}\right)I_0\left(2\sqrt{\frac{K_G(1+K_G)\gamma}{\Omega}}\right)d\gamma\\ &= 1-q+\frac{e^{-K_G+\frac{K_G(1+K_G)}{1+K_G+s\Omega}}q(1+K_G)}{1+K_G+s\Omega}. \end{aligned} \tag{4.43}$$

Hence, the MGF of $Z=\kappa_A\mathbb{B}_1|f_1|^2+\kappa_G\mathbb{B}_2|f_2|^2$ that appears in (4.41) can be expressed as

$$\mathcal{M}_Z(s)=\left(1-q+\frac{e^{-K_G+\frac{K_G(1+K_G)}{1+K_G+s\Omega\kappa_G}}q(1+K_G)}{1+K_G+s\Omega\kappa_G}\right)\left(1-q+\frac{e^{-K_A+\frac{K_A(1+K_A)}{1+K_A+s\Omega\kappa_A}}q(1+K_A)}{1+K_A+s\Omega\kappa_A}\right). \tag{4.44}$$

Thus, the outage probability from MGF by using inverse Laplace transform can be calculated, which can be expressed as

$$\mathrm{P}_{\text{out}}^{\text{ORS-E}}(\gamma_{\text{th}})=\mathcal{L}^{-1}\left(\frac{\mathcal{M}_Z(s)}{s}\right)\Bigg|_{s=\frac{P_n\gamma_{\text{th}}}{P_0}}. \tag{4.45}$$

In the case that A2A channel is modeled as AWGN, it follows from (4.41) that

$$\begin{aligned}P_{\text{out}}^{\text{ORS-E}}(\gamma_{\text{th}}) &= \Pr\left(\frac{P_0\left(\kappa_G\mathbb{B}_1|f_1|^2+\kappa_A\mathbb{B}_2\right)}{P_n}<\gamma_{\text{th}}\right)=\Pr\left(\kappa_G\mathbb{B}_1|f_1|^2+\kappa_A\mathbb{B}_2<\frac{P_n}{P_0}\gamma_{\text{th}}\right)\\ &= q^2\Pr\left(|f_1|^2<\frac{P_n\gamma_{\text{th}}-\kappa_AP_0}{\kappa_GP_0}\right)+(1-q)^2\\ &\quad+(1-q)q\left\{\Pr\left(|f_1|^2<\frac{P_n\gamma_{\text{th}}}{\kappa_GP_0}\right)+\mathbb{I}\left(\kappa_A<\frac{P_n\gamma_{\text{th}}}{P_0}\right)\right\}\\ &= 1-q+q^2-q^2Q_1\left(\sqrt{2K_G},\sqrt{\frac{2(K_G+1)}{\Omega}\left(\frac{P_n\gamma_{\text{th}}-\kappa_AP_0}{\kappa_GP_0}\right)}\right)\\ &\quad-(1-q)q\left\{Q_1\left(\sqrt{2K_G},\sqrt{\frac{2(K_G+1)}{\Omega}\frac{P_n\gamma_{\text{th}}}{\kappa_GP_0}}\right)-\mathbb{I}\left(\kappa_A<\frac{P_n\gamma_{\text{th}}}{P_0}\right)\right\}, \end{aligned} \tag{4.46}$$

where $\mathbb{I}(C)$ is the indicator function that takes 1 if the condition C holds and 0 otherwise.

$$\begin{aligned}\mathcal{T}_{\mathrm{ORSJ}} = 2(1-q)q&\left[\frac{e^{-\frac{K[P_0+NP_j\gamma_{\mathrm{th}}]}{P_0+P_j\gamma_{\mathrm{th}}}}P_j\gamma_{\mathrm{th}}(1+K)}{P_0+P_j\gamma_{\mathrm{th}}}I_0\left(\frac{2K\sqrt{P_0P_j\gamma_{\mathrm{th}}}}{P_0+P_j\gamma_{\mathrm{th}}}\right)-Q_1\left(\sqrt{\frac{2P_0K}{P_0+P_j\gamma_{\mathrm{th}}}},\sqrt{\frac{2KP_j\gamma_{\mathrm{th}}}{P_0+P_j\gamma_{\mathrm{th}}}}\right)\right]\\ +q^2&\left\{\frac{2^{\frac{N-1}{2}}e^{-\frac{K[2P_0+NP_j\gamma_{\mathrm{th}}]}{P_0+P_j\gamma_{\mathrm{th}}}}NP_j^2\gamma_{\mathrm{th}}^2}{(P_0+P_j\gamma_{\mathrm{th}})^2}\sum_{k=0}^{1}\sum_{n=0}^{1-k}\frac{(-1)^n(k-1)_n}{n!}\left(\frac{P_0}{2P_j\gamma_{\mathrm{th}}}\right)^{\frac{n+k}{2}}\right.\\ &\left.\times\left(\frac{P_0+P_j\gamma_{\mathrm{th}}}{P_0}\right)^kI_{n+k}\left(\frac{2K\sqrt{2P_0P_j\gamma_{\mathrm{th}}}}{P_0+P_j\gamma_{\mathrm{th}}}\right)-Q_2\left(2\sqrt{\frac{P_0K}{P_0+P_j\gamma_{\mathrm{th}}}},\sqrt{\frac{2KP_j\gamma_{\mathrm{th}}}{P_0+P_j\gamma_{\mathrm{th}}}}\right)\right\}\end{aligned}\tag{4.49}$$

ORSJ

In ORSJ, the eavesdropper can receive signal from S in the first phase and that from the selected relay R^* in the second phase. Similar to the main channel case, the exact analysis of the outage probability may be intractable, and thus it attempts to derive a simple lower bound (i.e., high SNR case). From (4.13) and (4.14), we have

$$\begin{aligned}\mathrm{P}_{\mathrm{out}}^{\mathrm{ORSJ-E}}(\gamma_{\mathrm{th}}) &\geq \Pr\left(\frac{P_0\left(\kappa_G\mathbb{B}_1|f_1|^2+\kappa_A\mathbb{B}_2|f_2|^2\right)}{\kappa_AP_j|v_1|^2}<\gamma_{\mathrm{th}}\right)\\ &\geq \Pr\left(\frac{P_0\sum_{l=1}^{2}\mathbb{B}_l|f_l|^2}{P_j|v_1|^2}<\gamma_{\mathrm{th}}\right)\triangleq \mathrm{Pr}_L^{\mathrm{ORSJ-E}}(\gamma_{\mathrm{th}}),\end{aligned}\tag{4.47}$$

where the first inequality stems from $P_n\to 0$ and the second inequality is due to the fact that $\kappa_G/\kappa_A \ll 1$ in general.

Theorem 2. *Under the assumption of $K_G = K_A = K$, the lower bound of outage probability of the eavesdropping channel in the ORSJ model defined in* (4.47) *can be expressed by*

$$\mathrm{Pr}_L^{\mathrm{ORSJ-E}}(\gamma_{\mathrm{th}}) = 1+\mathcal{T}_{\mathrm{ORSJ}},\tag{4.48}$$

where $\mathcal{T}_{\mathrm{ORSJ}}$ is expressed by (4.49) *shown at top of this page.*

Proof. See Appendix A.2. □

In the case that A2A channel is modeled as AWGN, similar to the case of ORS, it could be written as

$$\begin{aligned}P_{\text{out}}^{\text{ORSJ-E}}(\gamma_{\text{th}}) &= \Pr\left(\frac{P_0\left(\kappa_G \mathbb{B}_1|f_1|^2+\kappa_A\mathbb{B}_2\right)}{P_n+\kappa_A P_j}<\gamma_{\text{th}}\right)\\ &=1-q+q^2-q^2Q_1\left(\sqrt{2K_G},\sqrt{\frac{2(K_G+1)}{\Omega}\left(\frac{P_n\gamma_{\text{th}}+\kappa_A P_j\gamma_{\text{th}}-\kappa_A P_0}{\kappa_G P_0}\right)}\right)\\ &\quad-(1-q)q\left\{Q_1\left(\sqrt{2K_G},\sqrt{\frac{2(K_G+1)}{\Omega}\frac{P_n+\kappa_A P_j}{\kappa_G P_0}\gamma_{\text{th}}}\right)-\mathbb{I}\left(\kappa_A<\frac{P_n\gamma_{\text{th}}}{P_0-P_j\gamma_{\text{th}}}\right)\right\}.\end{aligned} \tag{4.50}$$

ORSMJ

By assumption, since the eavesdropper can only receive information from source in the first phase, the transmission outage probability of eavesdropper can be lower bounded similar to the case of ORSJ as

$$\begin{aligned}P_{\text{out}}^{\text{ORSMJ-E}}(\gamma_{\text{th}}) &= \Pr\left(\frac{P_0(\kappa_G\mathbb{B}_1|f_1|^2+\kappa_A\mathbb{B}_2|f_2|^2)}{P_n+\kappa_A\sum_{n=1}^N P_j|v_n|^2}<\gamma_{\text{th}}\right)\\ &\geq \Pr\left(\frac{P_0\sum_{l=1}^2\mathbb{B}_l|f_l|^2}{\sum_{n=1}^N P_j|v_n|^2}<\gamma_{\text{th}}\right)\triangleq \Pr_L^{\text{ORSMJ-E}}(\gamma_{\text{th}}).\end{aligned} \tag{4.51}$$

The above lower bound can be explicitly derived as follows:

Theorem 3. *Under the assumption of $K_G = K_A = K$, the outage probability lower bound of the eavesdropping channel in ORSMJ given in* (4.51) *can be expressed as*

$$\Pr_L^{\text{ORSMJ-E}}(\gamma_{\text{th}}) = 1-q+\mathcal{T}_{\text{ORSMJ}} \tag{4.52}$$

where $\mathcal{T}_{\text{ORSMJ}}$ is given by (4.53) *shown at top of the next page.*

Proof. See Appendix A.3. □

In the case that the A2A channel does not suffer from Rician fading, from (4.51) it has

$$P_{\text{out}}^{\text{ORSMJ-E}}(\gamma_{\text{th}}) = \Pr\left(\frac{P_0(\kappa_G\mathbb{B}_1|f_1|^2+\kappa_A\mathbb{B}_2)}{P_n+\kappa_A NP_j}<\gamma_{\text{th}}\right). \tag{4.54}$$

Therefore, the expression is the same as (4.50) with P_j replaced by NP_j.

$$
\begin{aligned}
\mathcal{T}_{\mathrm{ORSMJ}} &= \frac{2(1-q)q(1+K)}{\sqrt{NK}} e^{-\left[K+\frac{(N-1)P_j K\gamma_{\mathrm{th}}}{P_0+P_j\gamma_{\mathrm{th}}}\right]} \left(\frac{P_0(1+K)}{P_j\Omega NK\gamma_{\mathrm{th}}}\right)^{\frac{N-1}{2}} \left(\frac{P_j\gamma_{\mathrm{th}}}{P_0+P_j\gamma_{\mathrm{th}}}\right)^{N} \left(\frac{K\Omega}{1+K}\right)^{\frac{N}{2}} \\
&\times \sum_{k_1=0}^{N-1}\sum_{j_1=0}^{N-k_1-1} \frac{(-1)^{j_1}(1+k-N)_{j_1}}{j_1!} \left(\frac{P_0(K+1)}{P_j\gamma_{\mathrm{th}}\Omega}\right)^{\frac{j_1+k_1}{2}} \left(\frac{P_0+P_j\gamma_{\mathrm{th}}}{P_0}\right)^{k_1} \left(\frac{N\Omega}{K+1}\right)^{\frac{j_1+k_1+1}{2}} \\
&\times I_{1+j_1+k_1-N}\left(\frac{2K\sqrt{P_0P_jN\gamma_{\mathrm{th}}}}{P_0+P_j\gamma_{\mathrm{th}}}\right) - 2(1-q)q\cdot Q_1\left(\sqrt{\frac{2P_0K}{P_0+P_j\gamma_{\mathrm{th}}}}, \sqrt{\frac{2KNP_j\gamma_{\mathrm{th}}}{P_0+P_j\gamma_{\mathrm{th}}}}\right) \\
&+ \frac{q^2 e^{-\left[2K+\frac{(N-2)P_jK\gamma_{\mathrm{th}}}{P_0+P_j\gamma_{\mathrm{th}}}\right]} P_j\gamma_{\mathrm{th}}}{P_0+P_j\gamma_{\mathrm{th}}} \sqrt{\frac{N}{K}} \left[\frac{P_0(K+1)}{P_j\gamma_{\mathrm{th}}\Omega NK}\right]^{\frac{N-1}{2}} \left(\frac{P_0\gamma_{\mathrm{th}}}{P_0+P_j\gamma_{\mathrm{th}}}\right)^{N} \left(\frac{K\Omega}{1+K}\right)^{\frac{N}{2}} \\
&\times \sum_{k_2=0}^{N}\sum_{j_2=0}^{N-k_2} \frac{(-1)^{j_2}2^{\frac{N-j_2-k_2-1}{2}}(k_2-N)_{j_2}}{j_2!} \left(\frac{P_0(1+K)}{P_j\gamma_{\mathrm{th}}\Omega}\right)^{\frac{j_2+k_2}{2}} \left(\frac{P_0+P_j\gamma_{\mathrm{th}}}{P_0}\right)^{k_2} \left(\frac{N\Omega}{1+K}\right)^{\frac{j_2+k_2-1}{2}} \\
&\times I_{1+j_2+k_2-N}\left(\frac{2K\sqrt{2P_0P_jN\gamma_{\mathrm{th}}}}{P_0+P_j\gamma_{\mathrm{th}}}\right) - q^2\cdot Q_2\left(2\sqrt{\frac{P_0K}{P_0+P_j\gamma_{\mathrm{th}}}}, \sqrt{\frac{2KNP_j\gamma_{\mathrm{th}}}{P_0+P_j\gamma_{\mathrm{th}}}}\right) \quad (4.53)
\end{aligned}
$$

MRCMJ

Since the eavesdropper can only receive information from source in the first phase, the transmission outage probability of eavesdropper can be expressed as

$$
\begin{aligned}
P_{\mathrm{out}}^{\mathrm{MRCMJ-E}}(\gamma_{\mathrm{th}}) &= \Pr\left(\frac{\kappa_G P_0 \mathbb{B}_1 |f_1|^2}{P_n + \kappa_A P_j \sum_{n=1}^{N} |v_n|^2} < \gamma_{\mathrm{th}}\right) \\
&\geq \Pr\left(\frac{\kappa_G P_0 \mathbb{B}_1 |f_1|^2}{\kappa_A P_j \sum_{n=1}^{N} |v_n|^2} < \gamma_{\mathrm{th}}\right) \triangleq \Pr_L^{\mathrm{MRCMJ-E}}(\gamma_{\mathrm{th}}). \qquad (4.55)
\end{aligned}
$$

The lower bound can be evaluated as follows:

Theorem 4. *Under the assumption of $K_G = K_A = K$, the outage probability lower bound of the eavesdropping channel for MRCMJ, given in* (4.55)*, can be expressed as*

$$
\Pr_L^{\mathrm{MRCMJ-E}}(\gamma_{\mathrm{th}}) = 1 + \mathcal{T}_{\mathrm{MRCMJ}} \qquad (4.56)
$$

where $\mathcal{T}_{\mathrm{MRCMJ}}$ is given by (4.57) *shown at top of this page.*

Proof. See Appendix A.4. □

$$\begin{aligned}\mathcal{T}_{\text{MRCMJ}} = {} & \frac{q(1+K)e^{-\left[K+\frac{(N-1)\kappa_A P_j K\gamma_{\text{th}}}{\kappa_G P_0+\kappa_A P_j\gamma_{\text{th}}}\right]}}{\Omega\sqrt{NK}} \left(\frac{\kappa_G P_0(1+K)}{\kappa_A P_j\gamma_{\text{th}}\Omega NK}\right)^{\frac{N-1}{2}} \left(\frac{\kappa_A P_j K\gamma_{\text{th}}}{\kappa_G P_0+\kappa_A P_j\gamma_{\text{th}}}\right)^{N} \left(\frac{\Omega}{K(1+K)}\right)^{\frac{N}{2}} \\ & \times \sum_{k=0}^{N-1}\sum_{n=0}^{N-k-1} \frac{(-1)^n(1+k-N)_n}{n!} \left(\frac{\kappa_G P_0(1+K)}{\kappa_A P_j\gamma_{\text{th}}\Omega}\right)^{\frac{n+k}{2}} \left(\frac{\kappa_G P_0+\kappa_A P_j\gamma_{\text{th}}}{\kappa_G P_0}\right)^{k} \left(\frac{N\Omega}{1+K}\right)^{\frac{n+k+1}{2}} \\ & \times I_{1+n+k-N}\left(\frac{2K\sqrt{P_0 P_j\kappa_G\kappa_A N\gamma_{\text{th}}}}{\kappa_G P_0+\kappa_A P_j\gamma_{\text{th}}}\right) - q\cdot Q_1\left(\sqrt{\frac{2K\kappa_G P_0}{\kappa_G P_0+\kappa_A P_j\gamma_{\text{th}}}}, \sqrt{\frac{2NK\kappa_A P_j\gamma_{\text{th}}}{\kappa_G P_0+\kappa_A P_j\gamma_{\text{th}}}}\right)\end{aligned} \tag{4.57}$$

In the case that A2A channel is modeled by AWGN, (4.55) can be expressed as

$$\begin{aligned} P_{\text{out}}^{\text{MRCMJ}-\text{E}}(\gamma_{\text{th}}) &= \Pr\left(\frac{\kappa_G P_0 \mathbb{B}_1 |f_1|^2}{P_n+\kappa_A N P_j} < \gamma_{\text{th}}\right) \\ &= 1-q+q\Pr\left(|f_1|^2 < \frac{P_n+\kappa_A N P_j}{\kappa_G P_0}\gamma_{\text{th}}\right) \\ &= 1-qQ_1\left(\sqrt{2K_G}, \sqrt{\frac{2(K_G+1)}{\Omega}\frac{P_n+\kappa_A N P_j}{\kappa_G P_0}\gamma_{\text{th}}}\right). \end{aligned} \tag{4.58}$$

As a final remark, it can be easily observed that as $P_0 \to \infty$ with P_j and P_n being constant, the transmission outage probabilities of eavesdropping channel for ORS, ORSJ, and ORSMJ models become

$$P_{\text{out}}^{E} \to (1-q)^2, \tag{4.59}$$

whereas in the case of MRCMJ it has

$$P_{\text{out}}^{\text{MRCMJ}-\text{E}} \to 1-q. \tag{4.60}$$

In other words, the eavesdropping channel for high SINR regime is only affected by the backhaul reliability, similar to the observation made in [106].

4.4 Numerical Results and Discussion

In this section, some numerical results are demonstrated for the considered UAV relay/jammer secure communication system based on analytical expressions developed in the previous section as well as the corresponding Monte-Carlo simulations for verification. In the simulations, the outage probability is evaluated by generating over $100\,000$ realizations of channel coefficients. In the numerical results, unless otherwise stated, the parameters are set as follows: Rician factor of G2A/A2G is $K_G = 10$ with the second moment $\Omega = 1$, jammer-to-noise ratio $P_j/P_n = 10$ dB, wireless backhaul reliability parameter $q = \{0.3, 0.7\}$, and the threshold SINR $\gamma_{\text{th}} = 10$ dB. For simplicity, two cases for the A2A channel are investigated: $K_A = K_G = 10$ or $K_A \to \infty$ (AWGN). It also defined the path-loss ratio of G2A/A2G to A2A channels as $\beta = \kappa_G/\kappa_A \in (0, 1)$, and we set $\beta = 0.5$, which corresponds to the scenario where the distance between the source and the relay is around 50 m in UAV-based urban area network [107]. Furthermore, without loss of generality, the path-loss of κ_G is normalized in 1 such that the transmit SNR P_0/P_n also corresponds to the received SNR. The total number of UAV relays is set as $U = 10$. In the case of MRCMJ, for the purpose of investigating the balance between the numbers of UAV relays L and jammers N to be deployed, the following two cases are considered: $L = 7$, $N = 3$ (Case 1), $L = 5$, $N = 5$ (Case 2). In the case of ORSMJ, the number of selected UAV jammers is equal to that of MRCMJ model in our parameter settings.

4.4.1 Transmission Outage Probability of Main Channel

Fig. 4.2 shows the transmission outage probability versus signal-to-noise ratio P_0/P_n of the main channel achieved by the four different models with $K_A = K_G = 10$. In the case of ORSJ, the result with $K_A \to \infty$ is also shown. For the analytical expression of ORS and ORSMJ, (4.21) with (4.22) is employed, whereas (4.40) with (4.39) is used for MRCMJ. In the case of ORSJ, (4.23) with (4.28) and (4.29) is plotted for $K_A = 10$, which serves as a lower bound, whereas the exact expression, i.e., (4.23) with (4.30) and (4.31), is plotted in the case of $K_A \to \infty$. From Fig. 4.2, it can observe that theoretical results well agree with simulation results, which verifies the correctness of the theoretical expressions.

Among the four models compared, ORSJ achieves the worst transmission performance, which is due to the fact that both the selected relay and destination suffer from AN transmitted by a single jammer, whereas in the other three approaches they do not receive any AN by assumption. The best performance is achieved by MRCMJ as D employs MRC scheme to enhance SINR. Moreover, when comparing Case 1 ($L = 7$, $N = 3$) and Case 2 ($L = 5$, $N = 5$), it

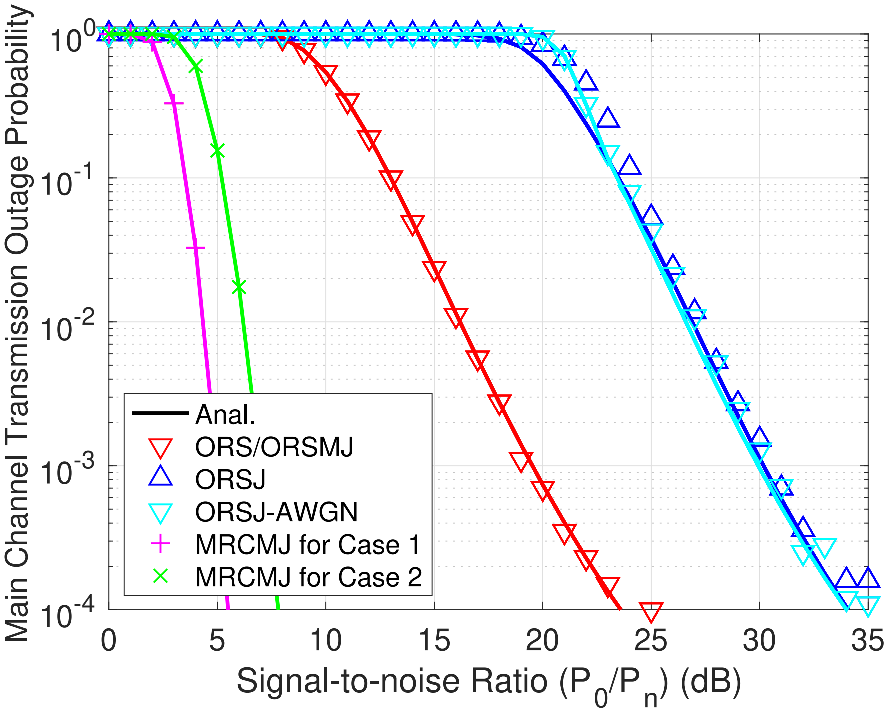


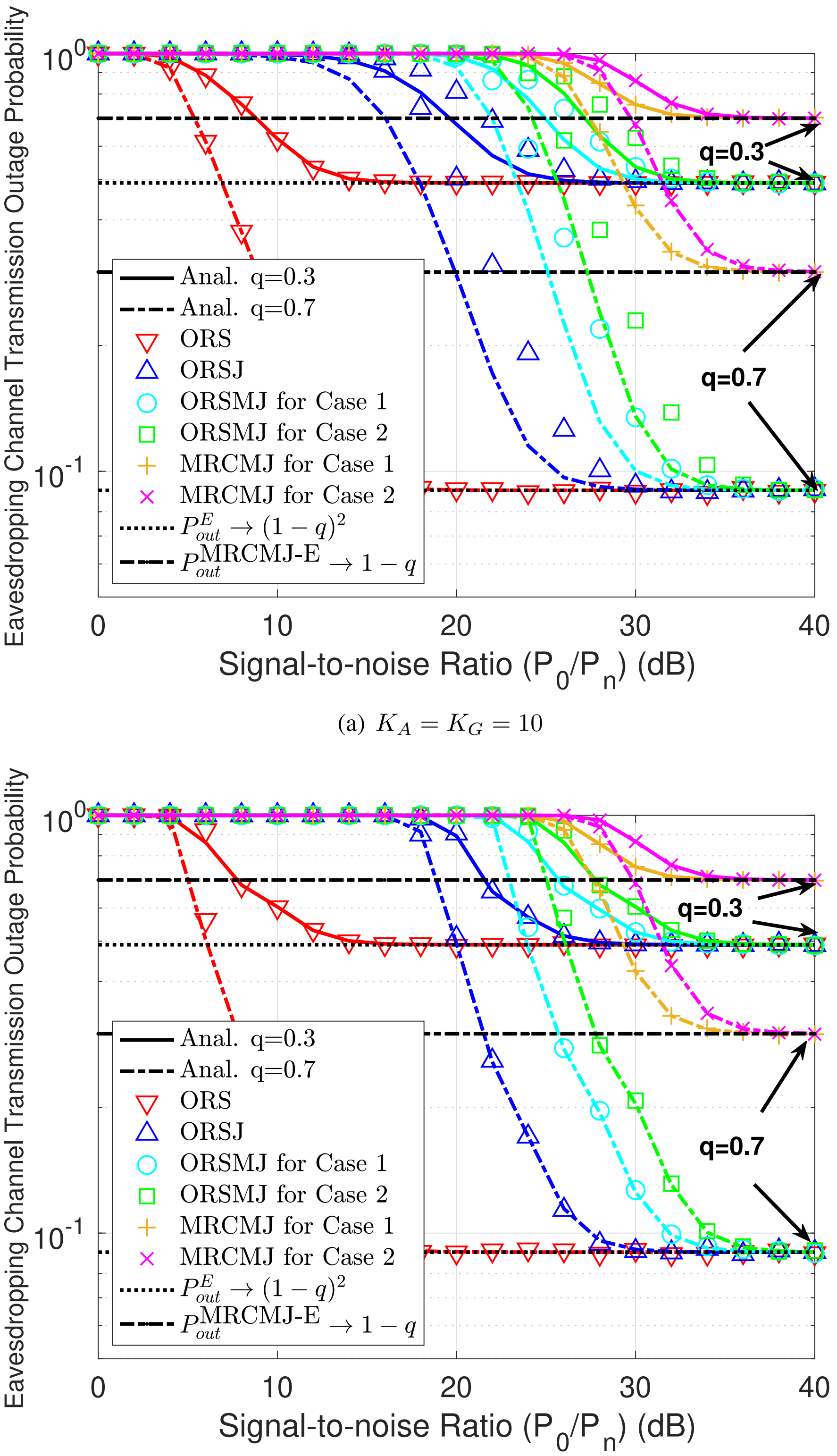
Figure 4.2: Transmission outage probabilities of main channel versus signal-to-noise ratio P_0/P_n. For MRCMJ: $L = 7$, $N = 3$ (Case 1) and $L = 5$, $N = 5$ (Case 2). (Solid lines: analytical results; Marks: corresponding simulation results.)

can observed that the former outperforms the latter. This stems from the fact that Case 1 employs more relays for information transmission and thus the achievable diversity effect by MRC can be enhanced.

4.4.2 Transmission Outage Probability of Eavesdropping Channel

Fig. 4.3 shows the transmission outage probability versus signal-to-noise ratio P_0/P_n of the eavesdropping channel achieved by the four different models with $q \in \{0.3, 0.7\}$. Fig. 4.3(a) and (b) correspond to the scenarios of $K_A = K_G = 10$ and $K_A \to \infty$, respectively. For MRCMJ (and ORSMJ), the results for both Case 1 ($L = 7$, $N = 3$) and Case 2 ($L = 5$, $N = 5$) are plotted.

For this eavesdropping channel, the analytical expressions of ORSJ, ORSMJ, and MRCMJ with finite K_A, i.e., (4.45) with (4.44), (4.47) with (4.48) and (4.49), and (4.56) with (4.57), are based on the lower bound, whereas that of ORS, i.e., (4.45) with (4.44), is based on the exact analysis. In the case of $K_A \to \infty$, the exact expressions are given by (4.46) for ORS, (4.50)



(a) $K_A = K_G = 10$

(b) $K_A \to \infty$

Figure 4.3: Transmission outage probability of eavesdropping channel versus signal-to-noise ratio P_0/P_n. For ORSMJ: $N = 3$ (Case 1), $N = 5$ (Case 2); For MRCMJ: $L = 7$, $N = 3$ (Case 1), $L = 5$, $N = 5$ (Case 2). (Lines: analytical results; Marks: corresponding simulation results.)

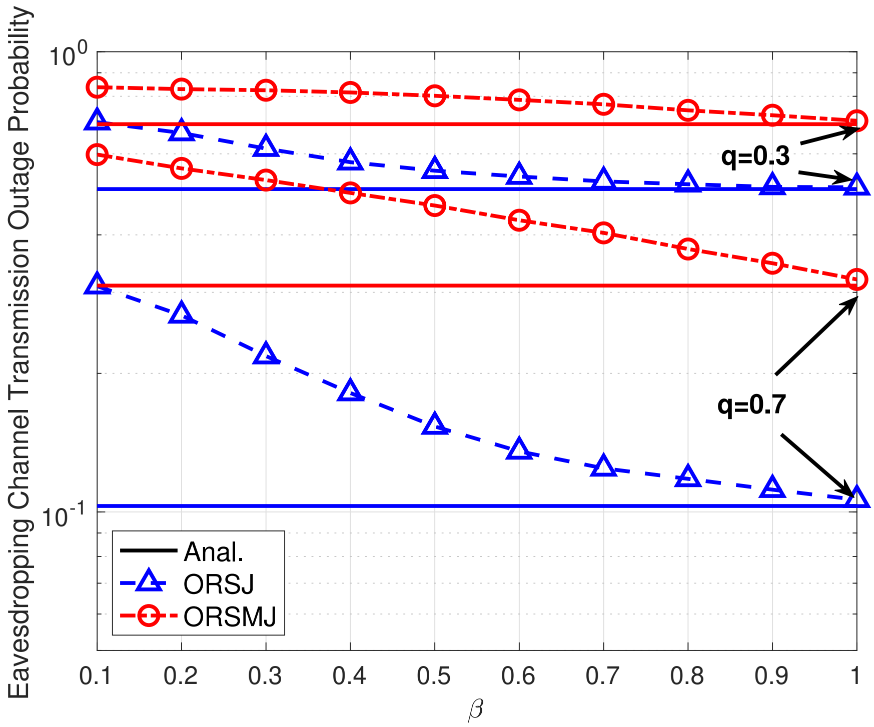


Figure 4.4: $\beta = \kappa_G/\kappa_A$ versus outage probability in ORSJ and ORSMJ models over eavesdropping channels for Case 1. (Solid lines: analytical results; Dash lines with marks: corresponding simulation results. Parameters: signal-to-noise ratio $P_0/P_n = 25$ dB, wireless backhaul reliability parameter $q \in \{0.3, 0.7\}$.)

for ORSJ, (4.54) for ORSMJ, and (4.58) for MRCMJ. It can observe that these expressions show good agreement with simulations. As expected, among the four models compared, the outage probability of MRCMJ is highest (i.e., desirable from a viewpoint of achievable secrecy), whereas that of ORS is lowest. This results from the number of effective jammers; No jammer is assigned for ORS, one jammer for ORSJ, and multiple jammers for ORSMJ and MRCMJ, but in the case of MRCMJ the eavesdropper can receive information only from source, thus improving the security. When comparing the results for Case 1 and Case 2 of ORSMJ and MRCMJ, the outage probability of Case 2 is higher than that of Case 1, indicating that Case 2 which deploys more jammers will enhance security. Furthermore, Fig. 4.3 also elucidates the fact that the asymptotic behavior of outage probability in high SNR is dominated by the backhaul reliability, and the asymptotic expressions (4.59) and (4.60) indicate that the outage probability of eavesdropper will be determined only by q.

Note that the outage lower bound expressions of (4.47) for ORS and (4.51) for ORSMJ are obtained based on the assumption that $\beta = \kappa_G/\kappa_A = 1$. In order to investigate the effect of this assumption, Fig. 4.4 compares these bounds along with the corresponding simulation results with respect to β, where setting $q \in \{0.3, 0.7\}$ and $P_0/P_n = 25$ dB. It can observe that as β approaches 1, the gap between the two results decreases as expected.

As a final remark, comparing the results shown in Fig. 4.2 and Fig. 4.3 for MRCMJ, Case 1 (more relays than jammers) is preferable in terms of the main channel, but in order to enhance security, Case 2 (increasing jammers) may be more beneficial. Therefore, there is clearly a trade-off relationship between the number of UAV relays and jammers to be deployed. In other words, for the MRCMJ approach, it is possible to adaptively allocate the numbers of relays and jammers based on the required level of security and reliability.

4.5 Conclusion and Future Works

This chapter has investigated the performance of the UAV swarm cooperative relaying network over Rician fading channels in the presence of a single UAV eavesdropper. Depending on how the UAV swarm is selected for relay or how it is divided into relays and jammers, the four specific models are introduced, and for each model, the mathematical expressions are developed for the transmission outage probabilities of both main channel and eavesdropping channel. The numerical comparisons with Monte-Carlo simulation results have shown that the analytical expressions match well with simulations, thus suggesting the accuracy of our analytical approach.

Chapter 5

UAV-Enabled WPSN Based on Multiple Cooperative Transmission Schemes

In this chapter, we study the uplink of a UAV-enabled wireless network using power-domain NOMA as well as cooperative relaying, where the ground sensor nodes are wireless powered devices. Part of this chapter was presented in [108, 109].

5.1 Introduction

UAV-enabled communication networks have spawned a variety of new results. For example, the use of UAV for energy-efficient data collection has been investigated in [110, 111]. In [112], an energy-efficient UAV communication with a ground terminal based on trajectory optimization has been proposed. A three-dimensional (3D) downlink coverage model for UAV communication networks has been developed in [113]. In [114, 115], the authors have studied an optimum trajectory for single-UAV broadcasting communication. Beamwidth control of UAV-enabled communication network has been proposed in [116]. In [117, 118], an optimized bandwidth allocation of UAV-enabled communication networks has been proposed. In [119], the altitude optimization of UAV that combines its antenna beamwidth, location, and transmission bandwidth for throughput maximization has been studied for several communications models. The optimal altitude of UAVs in terms of their coverage has been investigated in [120, 121]. In [122], the authors focus on the trajectory and resource allocation design for downlink UAV communications where a communicating UAV that serves multiple ground users in the existence of multiple ground eavesdroppers is assisted by a multi-antenna jamming UAV for the purpose of secrecy improvement.

Meanwhile, wireless powered sensor network (WPSN) is a promising candidate for self-sustainable IoT, where communicating devices are powered over the air by dedicated wireless power transmitters [123, 124]. Compared to conventional battery-powered wireless communications, WPSN eliminates the need of manual battery replacement and recharging, leading to effective reduction of the operation cost. Various approaches for WPSN, such as wireless power transfer (WPT), energy harvesting, and simultaneous wireless information and power transfer (SWIPT), have been considered in the literature. For example, in [35], throughput maximization of WPSN has been investigated based on the optimization of the time resource allocation to users with harvest-then-transmit protocol. The resource allocation with relay selection in a two-hop relay-assisted multi-user orthogonal frequency-division multiple-access (OFDMA) network with SWIPT has been proposed in [125]. In [126], the authors investigate the minimization of energy consumption in a cooperative system with energy harvesting users with quality of service (QoS) constraints of each user in terms of minimum required data rate.

On the other hand, non-orthogonal multiple access (NOMA) is a potential solution to accommodate an ever-increasing data traffic in mobile networks without expansion of spectral resources, and thus has stimulated the upsurge of interest from both academia and industry [40]. NOMA exploits the difference in the channel gain among users for multiplexing [127], [128]. By allowing multiple users to be served in the same resource block with assistance of successive interference cancellation (SIC), NOMA may significantly improve the spectral efficiency and outperform traditional orthogonal multiple access (OMA) schemes under severe limitation of spectral resources. In [129], the impact of user pairing on the performance of fixed power allocation NOMA and cognitive radio inspired NOMA has been investigated. More recently, in [130], the potential gain of NOMA over OMA in a cellular communication system has been investigated where a base station is equipped with massive antenna arrays.

This chapter focuses on an access scheme for WPSN served by a UAV based on the power-domain NOMA protocol as well as cooperative relaying. In [131,132] the applicability of NOMA for UAV-assisted communication systems has been studied. It has been shown in [132] that the performance of the NOMA scheme outperforms the OMA scheme under several different scenarios. In [133], the authors study a UAV-enabled NOMA-based network and suggest that NOMA can be a potential candidate for backscatter communications. Other recent studies on NOMA-based communication through UAV are prolific, which include resource allocation and user clustering for multi-UAV communication [134], an asymptotic interference cancellation based on NOMA for UAV [135], a precoding optimization for NOMA cellular networks with UAV [136], and performance analysis of NOMA-based UAV communication under correlated Rician fading channels [137].

In this chapter, the uplink of a UAV-enabled wireless network using power-domain NOMA as well as cooperative relaying is studied, where the ground sensor nodes are wireless powered devices[1]. These devices experience air-to-ground (A2G) communication channels, which are characterized by altitude-dependent path loss exponent and fading. It is focused on a *user pairing* system associated with the wireless networks based on NOMA or cooperative relaying, where the access devices are divided into two groups and a pair of devices is formed from each group. The available bandwidth is then divided according to the number of the pairs where each pair shares the same sub-channel to send their respective information [132]. The primary issues that addressed in this chapter are as follows: What is the best user-pairing strategy for NOMA and cooperative relaying in our UAV-enabled WPSN model? Which performs better given a specific user pairing strategy? How should the resources be allocated between the energy transmission and information transmission? In response to these fundamental questions, the major contributions in this chapter are summarized as follows:

- The performance improvement of power-domain NOMA and cooperative relaying is analyzed over the conventional OMA scheme in conjunction with two representative sensor node paring strategies. Through the theoretical analysis of outage probabilities, the suitable pairing strategies are revealed for each scheme. More specifically, we show that the preferable pairing strategies are different depending on whether we adopt NOMA or cooperative relaying: For NOMA, the pairing strategy referred to as better-better pairing (BBP) outperforms the other strategy called better-worse pairing (BWP), whereas BWP turns out to be better than BBP in the case of cooperative relaying. To the best of the authors' knowledge, the identification of the performance dependence on pairing strategies should be new.

- The optimal altitude of UAV is identified that minimizes the transmission outage probability for each scheme. Intuitively, in the channel model based on [93], if the UAV operates in lower altitude, the elevation angle between wireless powered sensor nodes and UAV will become smaller, thus leading to the decrease of line-of-sight (LoS) factor; however, in the case of higher altitude, the distance between the wireless powered sensor nodes and UAV increases, which also decreases the received power associated with increasing free-space path loss. Therefore, there exists an optimal altitude, which will be identified through numerical analysis.

Throughout this chapter, for simplicity of analysis, it is assumed that a UAV that performs data collection is equipped with a single antenna. If the UAV were equipped with multiple antennas,

[1] More advanced UAV models include solar-powered UAVs that can provide self-sustainable communications (e.g., [138]).

one could enhance the performance through beamforming (see e.g., [139]). However, in this case the UAV should acquire the channel state information (CSI) before energy transmission, which would make the initial process of power supply more complex for our system model. The extension to multiple antenna cases is thus left as future work.

The rest of this chapter is organized as follows: In Section 5.2, the system and channel models considered throughout this chapter are presented. The transmission schemes and pairing strategies evaluated in this chapter are described in Section 5.3. The outage probabilities of all the considered transmission schemes are theoretically analyzed in Section 5.4. The numerical results are provided and discussed in Section 5.5. Finally, Section 5.6 presents conclusion.

Notations Throughout the chapter, $f_{\varphi}(\cdot)$ and $F_{\varphi}(\cdot)$ denote the probability density function (PDF) and cumulative distribution function (CDF) of a random variable (RV) φ, respectively; $\mathcal{CN}(\mu, \sigma^2)$ denotes the circular-symmetric complex Gaussian distribution with mean μ and variance σ^2; $\mathbb{E}(x)$ is the expected value of a random variable x. Moreover, the following special functions will be used: the Gamma function $\Gamma(\cdot)$ [87, §8.31], the modified Bessel function of the second kind $K_n(\cdot)$ [87, §8.407], and the Meijer G-function $G_{p,q}^{m,n}\left(\begin{smallmatrix} a_1,\ldots,a_p \\ b_1,\ldots,b_q \end{smallmatrix} \middle| z\right)$ [87, §9.301].

5.2 System and Channel Models

In this section, we describe the UAV-enabled WPSN system model considered throughout this chapter. The channel model and energy transmission model adopted in this chapter are also summarized.

5.2.1 System Model

A network model illustrated in Fig. 5.1 is considered, where a certain outdoor location is served by a single-antenna data-collecting UAV. The UAV is placed in an adjustable altitude H, aiming to collect the information from wireless powered sensor nodes located within the disk area with radius r_C on the ground (e.g., [133, 140]). As shown in Fig. 5.1, by sending RF signals the UAV supplies energy to all the sensor nodes in the first phase, and the sensor nodes send back their information by using the supplied energy in the second phase. It is assumed that there are N ground sensor nodes in the coverage disk area. It is further focused on the case where N is an even number with $N = 2\mathsf{P}$ for simplicity. Its extension to the case with odd sensor nodes is straightforward. Among N total sensor nodes, the P nodes located in closer vicinity of the UAV in terms of the Euclidean distance are called *center area sensors* and belong to the group $\mathbb{G}_1$, whereas the remaining P sensor nodes located farther from the center are called *cell-edge*

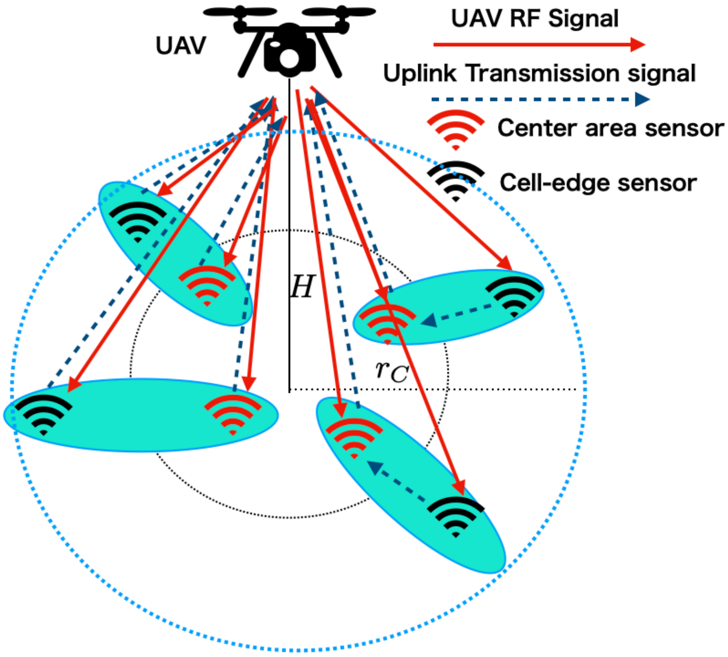


Figure 5.1: Illustration of the system model.

sensors and belong to the group $\mathbb{G}_2$. It is denoted that the kth node of the ith group as $S_{i,k}$, where $k \in \{1, 2, \ldots, \mathsf{P}\}$ and $i \in \{1, 2\}$, and the nodes $S_{1,k}$ and $S_{2,k}$ form the kth pair which shares the same resource block. In order to successfully decode all of the collected signals, the UAV requests that the instantaneous capacity of the channel associated with all sensor nodes should be higher than the target information rate R^*.

It is denoted that the location of the sensor node $S_{i,k}$ by $(r_{i,k}, \varphi_{i,k})$ in the polar coordinates on the ground plane with the projection of UAV located at its origin. Hence, the Euclidean distance between the sensor node $S_{i,k}$ and UAV is given by

$$d_{i,k} = \sqrt{H^2 + r_{i,k}^2}. \tag{5.1}$$

The elevation angle between the sensor node $S_{i,k}$ and UAV can be expressed as

$$\theta_{i,k} = \arcsin\left(\frac{H}{d_{i,k}}\right), \qquad 0 \le \theta_{i,k} \le \frac{\pi}{2}. \tag{5.2}$$

In Section 5.3, it will be described that how to pair the two nodes from each group and how they transmit their information for each given pair.

5.2.2 Channel Models

For the sensor node $S_{i,k}$, let $h_{i,k}$ and $g_{i,k}$ denote the complex channel coefficients of downlink (UAV to $S_{i,k}$) and uplink ($S_{i,k}$ to UAV) for energy and information transmission, respectively. Due to the flight altitude of the UAV, the air-to-ground (A2G) and ground-to-air (G2A) channels are typically characterized by the line-of-sight (LoS) link and thus commonly modeled by Rice fading [95]. However, Rice distribution often causes difficulty in mathematical manipulation as its probability density function (PDF) involves the modified Bessel function. As an alternative approach, the channel coefficients are modeled as statistically independent Nakagami-m random variables, i.e., the PDF of $X = |h_{i,k}|^2$ (or $X = |g_{i,k}|^2$), under the assumption of $\Omega \triangleq \mathbb{E}\left[X\right]$, can be expressed with the parameter m as [102]

$$f_X(x) = e^{-\frac{m}{x}}\Omega\left(\frac{m}{\Omega}\right)^m \frac{x^{m-1}}{\Gamma(m)}. \tag{5.3}$$

Note that Rice distribution can be approximated by Nakagami-m distribution by selecting the Nakagami parameter m as [141, eq.(5.37)]

$$m \approx \frac{\left(K+1\right)^2}{2K+1}, \tag{5.4}$$

where K is a reference Rician factor.

The Nakagami parameter m is modeled as a function of the elevation angle θ by introducing the non-decreasing function $m(\theta)$ with $0 \leq \theta \leq \frac{\pi}{2}$. Since larger θ implies higher LoS contribution and less multipath scatters at the receiver, it should result in larger m. Specifically, we define

$$m(\theta) \triangleq \frac{\left[\kappa_0\left(\frac{\kappa_{\frac{\pi}{2}}}{\kappa_0}\right)^{\frac{2\theta}{\pi}}+1\right]^2}{2\kappa_0\left(\frac{\kappa_{\frac{\pi}{2}}}{\kappa_0}\right)^{\frac{2\theta}{\pi}}+1}, \tag{5.5}$$

where κ_0 is the Rician factor of ground-to-ground (G2G) communication, and $\kappa_{\frac{\pi}{2}}$ is the maximum Rician factor of G2A communication [121, 142]. The parameter m experienced by the sensor node $S_{i,k}$ is denoted as $m_{i,k} \triangleq m(\theta_{i,k})$.

The path loss is also influenced by the elevation angle such that the path loss exponent α may decrease as the elevation angle θ increases. Based on [93], G2G links with $\theta = 0$ may experience the largest α (denoted by α_0 in what follows), whereas the value of α at $\theta = \pi/2$ (denoted by $\alpha_{\frac{\pi}{2}}$)

would be the smallest. More specifically, $\alpha(\theta)$ is characterized by the following model based on the concept of *probability* of LoS [93]:

$$\alpha(\theta) = a_1 \mathcal{P}_{\mathrm{LoS}}(\theta) + b_1 \tag{5.6}$$

with

$$\mathcal{P}_{\mathrm{LoS}}(\theta) = \frac{1}{1 + a_2 e^{-b_2 \theta}}, \tag{5.7}$$

$$a_1 = \frac{\alpha_{\frac{\pi}{2}} - \alpha_0}{\mathcal{P}_{\mathrm{LoS}}\left(\frac{\pi}{2}\right) - \mathcal{P}_{\mathrm{LoS}}\left(0\right)} \cong \alpha_{\frac{\pi}{2}} - \alpha_0, \tag{5.8}$$

and

$$b_1 = \alpha_0 - a_1 \cdot \mathcal{P}_{\mathrm{LoS}}(0) \cong \alpha_0, \tag{5.9}$$

where the approximations are due to the fact that $\mathcal{P}_{\mathrm{LoS}}(\theta)$ should decrease as $\theta \rightarrow 0$ and should increase as $\theta \rightarrow \frac{\pi}{2}$, and the coefficients a_2 and b_2 are determined by the environmental characteristics and the carrier frequency of RF signal.

5.2.3 Wireless Powered Sensor Network Model

Upon receiving RF energy signal from the UAV, the sensor nodes are equipped with a wireless power transfer circuit that stores energy from the UAV in the first phase, and using all the harvested energy they transmit their information signal in the second phase. Specifically, all the sensor nodes are assumed to operate in a harvest-then-transmit mode. As soon as the transmission completes, the sensor nodes switch to the sleep mode. The power received by the sensor node in the first phase can be expressed as

$$P_{i,k}^{r} = P_0 |h_{i.k}|^2 d_{i,k}^{-\alpha_{i,k}}, \tag{5.10}$$

where $\alpha_{i,k}$ is the path-loss exponent parameter experienced by $S_{i,k}$, and P_0 is the transmission power by the UAV. Let $\zeta_{i,k}$ denote the power conversion efficiency of the sensor node $S_{i,k}$. Then the transmit power $P_{i,k}^{t}$ of the sensor node $S_{i,k}$ in the second phase is expressed as

$$P_{i,k}^{t} = \zeta_{i,k} P_{i,k}^{r}. \tag{5.11}$$

Remark

Throughout this chapter, it is assumed that the channel state information (CSI) is available only at the receiver side of modulated signals. In the first phase, the unmodulated signal, i.e., continuous waveform (CW) is transmitted by UAV for the purpose of energy transfer and thus sensor nodes need not have the CSI of the link from the UAV. On the other hand, in the second phase, the UAV should estimate the CSI of all the links from the ground sensor nodes. Furthermore, in the case of cooperative relaying (discussed in Section 5.3.2), the sensor nodes in the center area should also estimate the CSI of the link from their own pairing node. Since our main focus is on comparison of the achievable performances by various transmission schemes, it is assumed that the ideal CSI is available when the channel estimation is necessary.

5.3 Transmission Schemes and Pairing Strategies

In this section, the node pairing strategies are firstly described. Four specific transmission schemes are introduced, which followed by the UAV altitude optimization.

5.3.1 Sensor Node Pairing

A network in practical scenario is considered where a fixed bandwidth of $\mathcal{B}_0$ is allocated to each sensor node. Therefore, when the two sensor nodes form a pair and share the same spectral resources, each pair can use the bandwidth of $\mathcal{B} = 2\mathcal{B}_0$. It is assumed that the two sensor nodes $S_{1,k}$ and $S_{2,k}$ with the same index k from each group form the kth pair as described in Section 5.2.1 and they share the kth bandwidth of size $\mathcal{B}$ in order to transmit their respective information.

The sensor node pairing strategies have a significant impact on the performance of NOMA-based network. It has been demonstrated in [129] that pairing the two devices with most different channel conditions should yield best performance gain over the conventional OMA approach. Considering that the path loss between the sensor node $S_{i,k}$ and UAV increases with radius $r_{i,k}$, the following two sensor node pairing strategies are investigated[2] illustrated in Fig. 5.2:

- The better-better pairing (BBP) strategy : The sensor node with better condition in $\mathbb{G}_1$ forms a pair with the sensor node with better condition in $\mathbb{G}_2$. In other words, the sensor

[2] The two representative pairing strategies introduced here are for the purpose of our fundamental study. One may also consider an optimal pairing strategy at the cost of additional complexity (e.g., through exhaustive search), which will be left as future work.

nodes are located with their radii given by

$$r_{1,1} < r_{1,2} < \cdots < r_{1,\mathsf{P}} < r_{2,1} < r_{2,2} < \cdots < r_{2,\mathsf{P}}.$$

- The better-worse pairing (BWP) strategy: The sensor node with better condition in $\mathbb{G}_1$ forms a pair with the sensor node with worse condition in $\mathbb{G}_2$. In other words, the sensor nodes are located with their radii given by

$$r_{1,1} < r_{1,2} < \cdots < r_{1,\mathsf{P}} < r_{2,\mathsf{P}} < r_{2,\mathsf{P}-1} < \cdots < r_{2,1}.$$

In this chapter, d_k denotes the Euclidean distance between the two sensor nodes in the kth pair, which can be expressed as

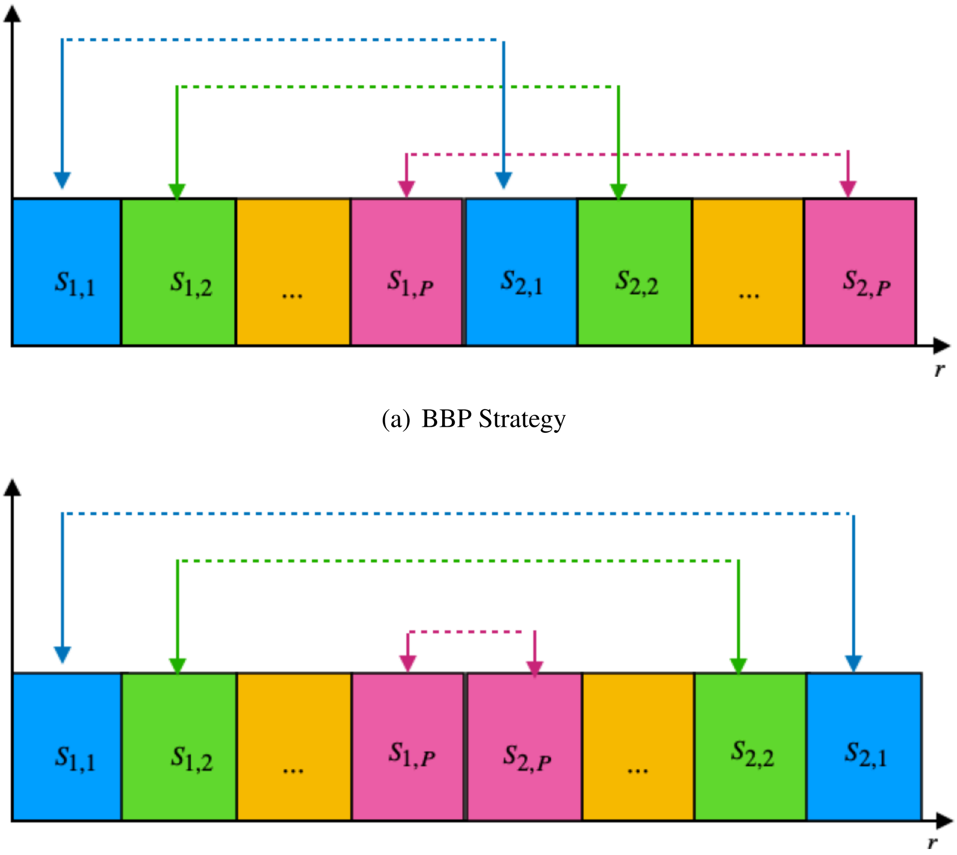
$$d_k = \left| r_{2,k} e^{j\varphi_{2,k}} - r_{1,k} e^{j\varphi_{1,k}} \right|. \tag{5.12}$$

5.3.2 Transmission Schemes

In the uplink transmission process, the data collection takes place after the UAV reaches the center of the service area, and all the sensor nodes are assumed to transmit their own data with information rate R^*. It is defined that the outage event as the case where at least a single node fails to transmit its own information. Let T denote the entire time period spent for this process. The following harvest-then-transmit protocol is considered: In the first phase, the UAV will broadcast the power supply signal for wireless power transfer (WPT) spending the time duration ξT with $\xi \in (0, 1)$. In the second phase, all the wireless powered sensor nodes send back their data during the period of $(1 - \xi)T$. Because of the independence assumption of fading channels among the sensor nodes in our system model, the total outage probability of the network can be expressed as

$$P_{\text{out}}^{Y} = 1 - \prod_{k=1}^{\mathsf{P}} \left(1 - P_{\text{out},k}^{Y}\right), \tag{5.13}$$

where $P_{\text{out},k}^{Y}$ is the outage probability of the kth pair with Y indicating a specific transmission scheme to be discussed shortly. All the wireless powered sensor nodes are assumed to be equipped with a rechargeable battery to store the energy harvested in the first phase, and all the energy is used when they attempt to transmit their information in the second phase by one of



(a) BBP Strategy

(b) BWP Strategy

Figure 5.2: Illustration of the two sensor node pairing strategies: The two sensor nodes with the same color form a pair. (The horizontal axis represents the distance from the origin.)

the following four specific transmission schemes:

- *NOMA-based transmission (NOMA)*: All the sensor nodes send their information to the UAV in the second phase simultaneously, regardless of their location. Then, the SIC-based detection is performed by the UAV: For the kth sub-channel, the UAV first decodes the signal of the sensor node $S_{1,k}$ in the group $\mathbb{G}_1$, treating that of $S_{2,k}$ as noise, and then decodes the signal of $S_{2,k}$ after subtracting that of $S_{1,k}$ from the received signal. For a given information rate R^*, the outage probability for the kth pair under this transmission scheme can be expressed as

$$P^{\text{NOMA}}_{\text{out},k} = P\left(\mathcal{C}^{\text{NOMA}}_{1,k} < R^* \cup \mathcal{C}^{\text{NOMA}}_{2,k} < R^*\right), \tag{5.14}$$

Table 5.1: The success events of RELAY scheme

	Transmission links of the kth pair in RELAY scheme		
	$S_{2,k} \rightarrow$ UAV	$S_{2,k} \rightarrow S_{1,k}$	$S_{1,k} \rightarrow$ UAV
Signal decodable?	Yes	Yes	Yes
	Yes	No	Yes
	No	Yes	Yes

where $\mathcal{C}_{i,k}^{\mathrm{NOMA}}$ is the corresponding maximum information rate of $S_{i,k}$ to UAV achieved by NOMA.

- *Cooperative relaying-based transmission (RELAY)*: The sensor nodes cooperatively transmit their information in the second phase using the variable-rate strategy [143]. In the first period of the second phase with time ratio β (i.e., the first $(1-\xi)\beta T$ period), the cell-edge sensor node $S_{2,k}$ broadcasts its signal to UAV as well as its center area pair $S_{1,k}$. In the second period (i.e., the remaining $(1-\xi)(1-\beta)T$ period), the center area sensor node $S_{1,k}$ attempts to decode the signal from the cell-edge sensor node $S_{2,k}$ via decode-and-forward (DF) scheme. If decoding is successful, the center area sensor node will encode the information of its pair along with its own information and send to the UAV with the resulting information rate doubled. Otherwise, the center area sensor node will send its own information only. In this strategy, there are three possible cases that lead to the success event in the kth pair, which are listed in Tab. 5.1. The outage probability of the kth pair under this transmission scheme can be thus expressed as

$$\begin{aligned}
&P_{\mathrm{out},k}^{\mathrm{RELAY}} = \\
&1 - \left[P\left(\mathcal{C}_{2,k}^{\mathrm{RELAY}} \geq R^* \cap \mathcal{C}_{k}^{\mathrm{RELAY}} < R^* \cap \mathcal{C}_{1,k}^{\mathrm{RELAY}} \geq R^*\right)\right. \\
&\left. + \, P\left(\mathcal{C}_{k}^{\mathrm{RELAY}} \geq R^* \cap \mathcal{C}_{1,k}^{\mathrm{RELAY}} \geq 2R^*\right)\right], \qquad (5.15)
\end{aligned}$$

where $\mathcal{C}_{i,k}^{\mathrm{RELAY}}$ is the corresponding maximum information rate of $S_{i.k}$ to UAV achieved by RELAY, $\mathcal{C}_{k}^{\mathrm{RELAY}}$ is the maximum achievable transmission rate of the corresponding G2G links $(S_{2,k} \rightarrow S_{1,k})$, and $2R^*$ stems from the fact that if the center area sensor node $S_{2,k}$ successfully decoded the signal received from $S_{1,k}$, it should transmit the information of two sensor nodes by doubling the information rate.

- *OMA-based transmission (OMA)*: The sensor nodes in each pair transmit their information in the conventional OMA using half of the second phase period, i.e., in a time-division multiple access (TDMA) manner. For example, the cell-edge sensor node $S_{2,k}$ sends its signal to the UAV in the first half of the second phase, followed by the information transmission of the center area sensor node $S_{1,k}$ in its second half. In this scheme, the outage probability of the kth pair can be expressed as

$$P^{\mathrm{OMA}}_{\mathrm{out},k} = P\left(\mathcal{C}^{\mathrm{OMA}}_{1,k} < R^* \cup \mathcal{C}^{\mathrm{OMA}}_{2,k} < R^*\right), \tag{5.16}$$

where $\mathcal{C}^{\mathrm{OMA}}_{i,k}$ is the corresponding maximum transmission rate of $S_{i,k}$ to UAV achieved by OMA.

- *Optimal selection-based transmission (OPT)*: For each pair, the sensor nodes autonomously select the best scheme among NOMA, RELAY, and OMA for their data transmission. The achievable outage probability of the kth pair under this ideal scheme can be expressed as

$$P^{\mathrm{OPT}}_{\mathrm{out},k} = \min_{Y \in \{\mathrm{NOMA,RELAY,OMA}\}} P^{Y}_{\mathrm{out},k}. \tag{5.17}$$

In this chapter, this research is interested in the probability that the UAV can collect data of all the wireless powered sensor nodes in the coverage area by one shot. Therefore, if the achievable rate of channel associated with any sensor node is less than the target information rate R^*, it is considered as outage. The resulting outage probability is thus expressed by (5.13) with (5.14) – (5.17) depending on the transmission schemes employed.

5.3.3 UAV Altitude Optimization

In our channel model, the G2A channel benefits from a lower path loss *exponent* α and larger LoS component (Nakagami parameter m) compared to a G2G link. However, when the UAV altitude H increases, the link distance also increases and thus may eventually decrease the received SNR of UAV as it reduces the energy deliverable to the ground sensor nodes. Therefore, there is an optimal altitude that minimizes the outage probability for each given scheme.

More specifically, since the received SNR at UAV depends on the relative position of the UAV and the location of the sensor nodes, the outage probability of (5.13) can be explicitly indicated as $P_{\mathrm{out}} = P_{\mathrm{out}}(\mathbf{r}, \mathbf{d}, H)$, where $\mathbf{r} = (r_{1,1}, \cdots, r_{1,\mathsf{P}}, r_{2,1}, \cdots, r_{2,\mathsf{P}})$ is the vector representing the distances of the sensor nodes from the center and $\mathbf{d} = (d_1, d_2, \cdots, d_{\mathsf{P}})$ is the vector representing the distances of the two sensor nodes that form each pair. For given sensor node locations $\mathbf{r}$ and

$\mathbf{d}$, the optimal altitude of UAV for maximum reliable link, denoted by H^*, can be defined as

$$H^* \triangleq \arg \min_{H \in [0, H_{\max}]} P_{\text{out}}(\mathbf{r}, \mathbf{d}, H), \tag{5.18}$$

where $H_{\max}$ is the maximum target flight altitude of the UAV. Note that the altitude H implicitly affects the received (and thus transmit) power of the sensor nodes, i.e., $P^r_{i,k}$ in (5.10). In other words, the transmit power of the sensor nodes depends on the UAV-sensor node distance of $d_{i,k}$ in (5.1) as well as the corresponding elevation angle of $\theta_{i,k}$ in (5.2), both of which are nonlinear functions of H. Furthermore, the elevation angle affects the path loss exponent $\alpha(\theta)$ through (5.6) and (5.7), as well as Nakagami parameter $m(\theta)$ by (5.5). Due to these intractable functions associated with H that appear in $P_{\text{out}}(\mathbf{r}, \mathbf{d}, H)$, (5.18) may not be formulated into an accessible closed-form function with respect to H. To cope with this difficulty, Nelder-Mead optimization algorithm will be applied [144] in our subsequent numerical studies shown in Section 5.5, where the impact of the two node pairing strategies are revealed on the performance of different transmission schemes, each evaluated at the optimized UAV altitude.

5.4 Performance Analysis

In this section, the outage probabilities of the four different transmission schemes are analyzed, which described in the previous section. In the subsequent analysis, it is assume that the transmitter sends signals from Gaussian codebook and the corresponding mutual information is considered as its achievable rate.

5.4.1 NOMA-based Transmission (NOMA)

In this scheme, the achievable rate of the center area sensor node in the kth pair, $S_{1,k}$, can be expressed as

$$\begin{aligned} \mathcal{C}^{\text{NOMA}}_{1,k} &= (1-\xi) 2\mathcal{B}_0 \\ &\times \log_2 \left(1 + \frac{\zeta_{1,k} \frac{\xi}{1-\xi} P_0 |h_{1,k}|^2 |g_{1,k}|^2 d_{1,k}^{-2\alpha_{1,k}}}{\sigma_n^2 + \zeta_{2,k} \frac{\xi}{1-\xi} P_0 |h_{2,k}|^2 |g_{2,k}|^2 d_{2,k}^{-2\alpha_{2,k}}} \right), \end{aligned} \tag{5.19}$$

where σ_n^2 is the power of additive white Gaussian noise (AWGN) and $\xi \in (0, 1)$ is the time ratio of energy harvesting and data transmission as described in Section 5.3.2. Provided that the SIC at the UAV for the signal of $S_{1,k}$ is successful, i.e., $\mathcal{C}^{\text{NOMA}}_{1,k} > R^*$, the *conditional* achievable rate of the corresponding pair $S_{2,k}$ may be given by

$$\tilde{\mathcal{C}}_{2,k}^{\mathrm{NOMA}} = (1-\xi)2\mathcal{B}_0 \times \log_2\left(1 + \frac{\zeta_{2,k}\frac{\xi}{1-\xi}P_0|h_{2,k}|^2|g_{2,k}|^2 d_{2,k}^{-2\alpha_{2,k}}}{\sigma_n^2}\right). \tag{5.20}$$

In order to analyze the corresponding outage probability, the following lemma is firstly introduced:

Lemma 5 (Product of Two Independent Squared Nakagami-m RVs). *Let $Z = W_1W_2$ be the product of two independent squared Nakagami-m random variables W_1 and W_2 with different parameters m_1 and m_2 and mean Ω_1 and Ω_2. Then, the corresponding PDF and CDF are given by*

$$f_Z(x) = \frac{2x^{\frac{m_1+m_2}{2}-1}}{\prod_{i=1}^{2}\Gamma(m_i)(\Omega_i/m_i)^{\frac{m_1+m_2}{2}}} \times K_{m_1-m_2}\left(2\prod_{i=1}^{2}\sqrt{\frac{m_i x}{\Omega_i}}\right) \tag{5.21}$$

and

$$F_Z(x) = \left[\prod_{i=1}^{2}\Gamma(m_i)\right]^{-1} G_{1,3}^{2,1}\left(\begin{array}{c}1\\ m_1, m_2, 0\end{array}\middle| x\prod_{i=1}^{2}\left(\frac{m_i}{\Omega_i}\right)\right), \tag{5.22}$$

respectively.

Proof. The PDF follows from the corresponding expression given in [145]. The CDF can be obtained by direct integration of the PDF using [87, §6.592.2]. □

By excluding the effect of AWGN in (5.19), let us define

$$\hat{\mathcal{C}}_{1,k}^{\mathrm{NOMA}} \triangleq (1-\xi)2\mathcal{B}_0\log_2\left(1 + \frac{\zeta_{1,k}|h_{1,k}|^2|g_{1,k}|^2 d_{1,k}^{-2\alpha_{1,k}}}{\zeta_{2,k}|h_{2,k}|^2|g_{2,k}|^2 d_{2,k}^{-2\alpha_{2,k}}}\right). \tag{5.23}$$

Then, the following theorem holds:

Theorem 6. *For a given target information rate R^*, the outage probability of the kth pair with*

NOMA scheme can be bounded as

$$\begin{aligned} P_{\mathrm{out},k}^{\mathrm{NOMA}} \geq 1 &- \left\{1 - P\left(\hat{\mathcal{C}}_{1,k}^{\mathrm{NOMA}} < R^*\right)\right\} \\ &\times \left\{1 - P\left(\tilde{\mathcal{C}}_{2,k}^{\mathrm{NOMA}} < R^*\right)\right\} \\ &\triangleq \hat{P}_{\mathrm{out},k}^{\mathrm{NOMA}}, \end{aligned} \tag{5.24}$$

where

$$\begin{aligned} &P\left(\hat{\mathcal{C}}_{1,k}^{\mathrm{NOMA}} < R^*\right) \\ &= \frac{1}{\Gamma^2\left(m_{1,k}\right)\Gamma^2\left(m_{2,k}\right)} \\ &\quad \times G_{3,3}^{2,3}\left(\begin{matrix} 1, 1 - m_{2,k}, 1 - m_{2,k} \\ m_{1,k}, m_{1,k}, 0 \end{matrix} \middle| \frac{m_{1,k}^2 Z_1}{m_{2,k}^2}\right) \end{aligned} \tag{5.25}$$

and

$$\begin{aligned} &P\left(\tilde{\mathcal{C}}_{2,k}^{\mathrm{NOMA}} < R^*\right) \\ &= \frac{1}{\Gamma^2(m_{2,k})} G_{1,3}^{2,1}\left(\begin{matrix} 1 \\ m_{2,k}, m_{2,k}, 0 \end{matrix} \middle| m_{2,k}^2 Z_2\right), \end{aligned} \tag{5.26}$$

with

$$Z_1 = \left(2^{\frac{R^*}{2\mathcal{B}_0(1-\xi)}} - 1\right) \frac{\zeta_{2,k}}{\zeta_{1,k}} \frac{d_{1,k}^{2\alpha_{1,k}}}{d_{2,k}^{2\alpha_{2,k}}}, \tag{5.27}$$

and

$$Z_2 = \left(2^{\frac{R^*}{2\mathcal{B}_0(1-\xi)}} - 1\right) \frac{\sigma_n^2 d_{2,k}^{2\alpha_{2,k}}}{\zeta_{2,k} \frac{\xi}{1-\xi} P_0}. \tag{5.28}$$

Proof. From Lemma 5, we have

$$\begin{aligned}
&P\left(\hat{\mathcal{C}}_{1,k}^{\mathrm{NOMA}} < R^*\right)\\
&= \int_0^\infty \frac{1}{\Gamma^2(m_{1,k})} G_{1,3}^{2,1}\left(\begin{matrix} 1 \\ m_{1,k}, m_{1,k}, 0 \end{matrix} \middle| Z_1 m_{1,k}^2 x\right)\\
&\quad \times \frac{2x^{m_{2,k}-1} m_{n,2}^{2m_{2,k}}}{\Gamma^2(m_{2,k})} K_0\left(2m_{2,k}\sqrt{x}\right) dx. \qquad (5.29)
\end{aligned}$$

Applying [146, §3.36.5.7] into (5.29), (5.25) is obtained. Equation (5.26) results from (5.20) and (5.22).

From (5.14), we have

$$\begin{aligned}
&P_{\mathrm{out},k}^{\mathrm{NOMA}}\\
&= 1 - P\left(\mathcal{C}_{1,k}^{\mathrm{NOMA}} > R^* \cap \mathcal{C}_{2,k}^{\mathrm{NOMA}} > R^*\right)\\
&= 1 - P\left(\mathcal{C}_{1,k}^{\mathrm{NOMA}} > R^*\right) P\left(\mathcal{C}_{2,k}^{\mathrm{NOMA}} > R^* \,|\, \mathcal{C}_{1,k}^{\mathrm{NOMA}} > R^*\right)\\
&= 1 - \left\{1 - P\left(\mathcal{C}_{1,k}^{\mathrm{NOMA}} < R^*\right)\right\}\\
&\quad \times \left\{1 - P\left(\tilde{\mathcal{C}}_{2,k}^{\mathrm{NOMA}} < R^*\right)\right\}. \qquad (5.30)
\end{aligned}$$

Then, since $\mathcal{C}_{1,k}^{\mathrm{NOMA}} \le \hat{\mathcal{C}}_{1,k}^{\mathrm{NOMA}}$, it follows that $P\left(\mathcal{C}_{1,k}^{\mathrm{NOMA}} < R^*\right) \ge P\left(\hat{\mathcal{C}}_{1,k}^{\mathrm{NOMA}} < R^*\right)$, thus leading to the lower bound (5.24). □

Finally, from (5.13) we have

$$\begin{aligned}
P_{\mathrm{out}}^{\mathrm{NOMA}} &= 1 - \prod_{k=1}^{\mathsf{P}} \left(1 - P_{\mathrm{out},k}^{\mathrm{NOMA}}\right)\\
&\ge 1 - \prod_{k=1}^{\mathsf{P}} \left(1 - \hat{P}_{\mathrm{out},k}^{\mathrm{NOMA}}\right) \triangleq \hat{P}_{\mathrm{out}}^{\mathrm{NOMA}}. \qquad (5.31)
\end{aligned}$$

5.4.2 Cooperative Relaying-based Transmission (RELAY)

In this scheme, the cell-edge sensor node sends its information to the UAV with the cooperation of center area sensors. In the first period of the second phase, the sensor node $S_{2,k}$ broadcasts its information to both $S_{1,k}$ and UAV. Hence, the maximum information rate achieved by UAV via G2A link $S_{2,k} \rightarrow \mathrm{UAV}$ and that achieved by sensor node $S_{1,k}$ via G2G link $S_{2,k} \rightarrow S_{1,k}$ can be expressed as

$$\begin{aligned}\mathcal{C}_{2,k}^{\mathrm{RELAY}} &= 2(1-\xi)\beta\mathcal{B}_0 \\ &\times \log_2\left(1+\frac{\zeta_{2,k}\frac{\xi}{(1-\xi)\beta}P_0|h_{2,k}|^2|g_{2,k}|^2 d_{2,k}^{-2\alpha_{2,k}}}{\sigma_n^2}\right),\end{aligned} \tag{5.32}$$

and

$$\begin{aligned}\mathcal{C}_{k}^{\mathrm{RELAY}} &= 2(1-\xi)\beta\mathcal{B}_0 \\ &\times \log_2\left(1+\frac{\zeta_{2,k}\frac{\xi}{(1-\xi)\beta}P_0|h_{2,k}|^2|g_{k}|^2 d_{2,k}^{-\alpha_{2,k}} d_k^{-\alpha_0}}{\sigma_n^2}\right),\end{aligned} \tag{5.33}$$

respectively, where d_k is the Euclidean distance between the two sensor nodes in the kth pair defined in (5.12), g_k is the corresponding channel coefficient of the G2G link, and α_0 is its path loss exponent, i.e., $\alpha_0 = \alpha(0)$.

In the residual period of the second phase, the sensor node $S_{1,k}$ transmits (re)encoded signal to the UAV. The maximum achievable information rate of the sensor node $S_{1,k}$ can be expressed as

$$\begin{aligned}\mathcal{C}_{1,k}^{\mathrm{RELAY}} &= 2(1-\xi)(1-\beta)\mathcal{B}_0 \\ &\times \log_2\left(1+\frac{\zeta_{1,k}\frac{\xi}{(1-\xi)(1-\beta)}P_0|h_{1,k}|^2|g_{1,k}|^2 d_{1,k}^{-2\alpha_{1,k}}}{\sigma_n^2}\right).\end{aligned} \tag{5.34}$$

The following theorem can be obtained directly from (5.15) and (5.22).

Theorem 7. *For a given target information rate R^*, the outage probability of the kth pair with RELAY can be expressed as*

$$\begin{aligned}P_{\mathrm{out},k}^{\mathrm{RELAY}} &= 1-\Big\{\left[1-P(\mathcal{C}_{1,k}^{\mathrm{RELAY}}<R^*)\right]P\left(\mathcal{C}_{k}^{\mathrm{RELAY}}<R^*\right) \\ &\times\left[1-P(\mathcal{C}_{2,k}^{\mathrm{RELAY}}<R^*)\right] \\ &+\left[1-P\left(\mathcal{C}_{k}^{\mathrm{RELAY}}<R^*\right)\right] \\ &\times\left[1-P\left(\mathcal{C}_{1,k}^{\mathrm{RELAY}}<2R^*\right)\right]\Big\},\end{aligned} \tag{5.35}$$

where

$$P(\mathcal{C}_{1,k}^{\mathrm{RELAY}} < R) = \frac{1}{\Gamma^2(m_{1,k})} \times G_{1,3}^{2,1}\left(\begin{matrix} 1 \\ m_{1,k}, m_{1,k}, 0 \end{matrix} \middle| m_{1,k}^2 A_1(R) \right), \tag{5.36}$$

$$P\left(\mathcal{C}_{2,k}^{\mathrm{RELAY}} < R^*\right) = \frac{1}{\Gamma^2(m_{2,k})} \times G_{1,3}^{2,1}\left(\begin{matrix} 1 \\ m_{2,k}, m_{2,k}, 0 \end{matrix} \middle| m_{2,k}^2 A_2 \right), \tag{5.37}$$

and

$$P\left(\mathcal{C}_{k}^{\mathrm{RELAY}} < R^*\right) = \frac{1}{\Gamma(m_{2,k})\Gamma(m_k)} \times G_{1,3}^{2,1}\left(\begin{matrix} 1 \\ m_{2,k}, m_0, 0 \end{matrix} \middle| m_{2,k} m_0 A_k \right), \tag{5.38}$$

with

$$A_1(R) = \left(2^{\frac{R}{2(1-\xi)(1-\beta)\mathcal{B}_0}} - 1\right) \frac{\sigma_n^2 d_{1,k}^{2\alpha_{1,k}}}{\zeta_{1,k} \frac{\xi}{(1-\xi)(1-\beta)} P_0},$$

$$A_2 = \left(2^{\frac{R^*}{2(1-\xi)\beta\mathcal{B}_0}} - 1\right) \frac{\sigma_n^2 d_{2,k}^{2\alpha_{2,k}}}{\zeta_{2,k} \frac{\xi}{(1-\xi)\beta} P_0},$$

and

$$A_k = \left(2^{\frac{R^*}{2(1-\xi)\beta\mathcal{B}_0}} - 1\right) \frac{\sigma_n^2 d_{2,k}^{\alpha_{2,k}} d_k^{\alpha_0}}{\zeta_{2,k} \frac{\xi}{(1-\xi)\beta} P_0}.$$

Note that from (5.13) we have

$$P_{\mathrm{out}}^{\mathrm{RELAY}} = 1 - \prod_{k=1}^{\mathsf{P}} \left(1 - P_{\mathrm{out},k}^{\mathrm{RELAY}}\right). \tag{5.39}$$

5.4.3 OMA-based Transmission (OMA)

In the conventional OMA, the information rate of the sensor node $S_{i,k}$ to the UAV can be expressed as

$$\mathcal{C}_{i,k}^{\mathrm{OMA}} = (1-\xi)\mathcal{B}_0 \log_2\left(1 + \frac{\zeta_{i,k}\frac{\xi}{1-\xi}P_0|h_{i,k}|^2|g_{i,k}|^2 d_{i,k}^{-2\alpha_{i,k}}}{\sigma_n^2}\right). \tag{5.40}$$

For a given target information rate R^*, the outage probability of the kth pair in OMA can be expressed from (5.16), (5.22), and (5.40), as

$$P_{\mathrm{out},k}^{\mathrm{OMA}} = 1 - \prod_{i=1}^{\mathsf{2}}\left\{1 - P\left(\mathcal{C}_{i,k}^{\mathrm{OMA}} < R^*\right)\right\} \tag{5.41}$$

where

$$P\left(\mathcal{C}_{i,k}^{\mathrm{OMA}} < R^*\right) = \frac{1}{\Gamma^2(m_{i,k})} G_{1,3}^{2,1}\left(\begin{array}{c} 1 \\ m_{i,k}, m_{i,k}, 0 \end{array}\middle| m_{i,k}^2 Z_{i,k}\right), \tag{5.42}$$

with

$$Z_{i,k} = \left(2^{\frac{R^*}{\mathcal{B}_0(1-\xi)}} - 1\right)\frac{\sigma_n^2 d_{i,k}^{2\alpha_{i,k}}}{\zeta_{i,k}\frac{\xi}{1-\xi}P_0}. \tag{5.43}$$

Finally, from (5.13) we have

$$P_{\mathrm{out}}^{\mathrm{OMA}} = 1 - \prod_{k=1}^{\mathsf{P}}\left(1 - P_{\mathrm{out},k}^{\mathrm{OMA}}\right). \tag{5.44}$$

5.4.4 Optimal Selection-based Transmission (OPT)

The optimal performance can be achieved by the OPT scheme whose outage probability can be expressed as

$$\begin{aligned} &P_{\mathrm{out}}^{\mathrm{OPT}} \\ &\geq 1 - \prod_{k=1}^{\mathsf{P}}\left(1 - \min\left\{\hat{P}_{\mathrm{out},k}^{\mathrm{NOMA}}, P_{\mathrm{out},k}^{\mathrm{RELAY}}, P_{\mathrm{out},k}^{\mathrm{OMA}}\right\}\right) \triangleq \hat{P}_{\mathrm{out}}^{\mathrm{OPT}}. \end{aligned} \tag{5.45}$$

Note that the above inequality stems from the fact that our theoretical result developed for NOMA is valid only if the effect of AWGN is negligible and thus it serves as a lower bound in a strict sense.

5.5 Numerical Results and Discussion

In this section, simulations are provided to examine the accuracy of the analytical results developed in the previous section as well as to investigate the performance difference among various transmission schemes with the two representative pairing strategies.

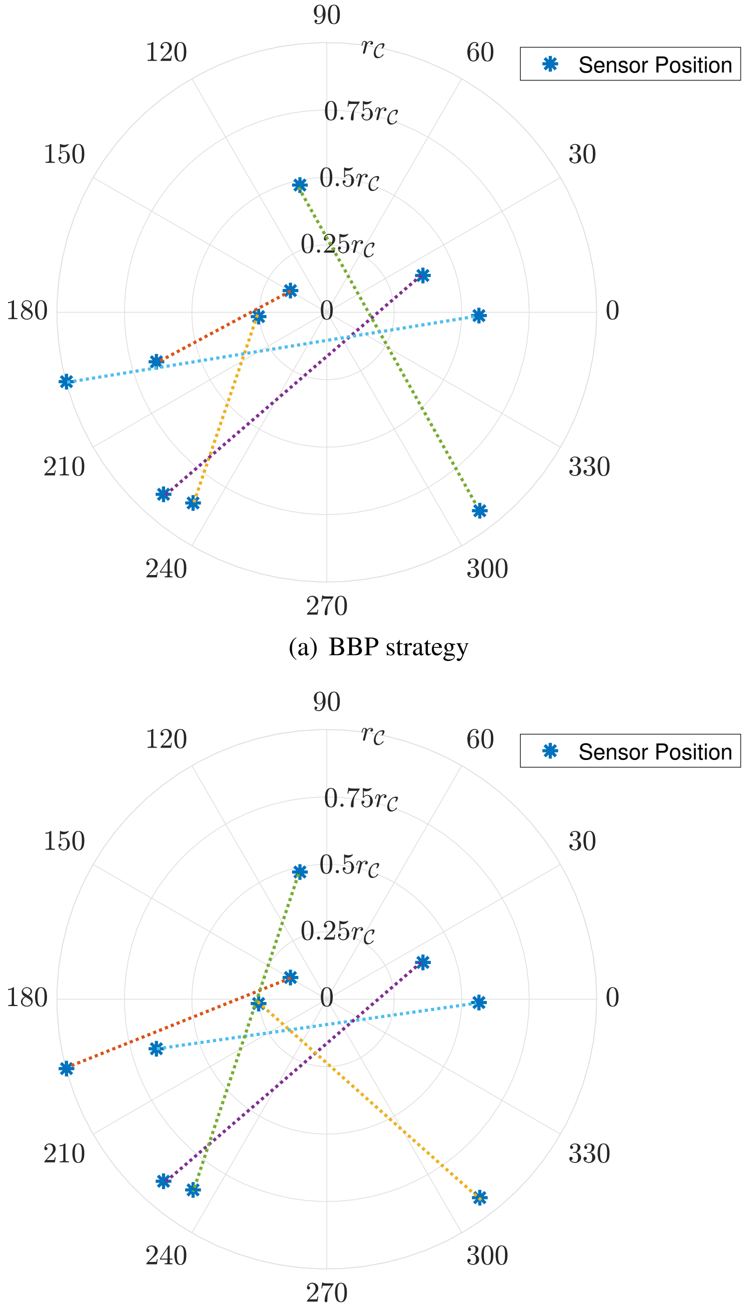
5.5.1 Network Setting

A specific topology consisting of ten sensor nodes is firstly considered, which is shown in Fig. 5.3 (i.e., $N = 10$), which was generated in a *pseudo-random* manner[3]. As a channel model associated with path loss, a suburban area is considered, i.e., the parameters a_2 and b_2 in (5.7) are chosen according to the corresponding values in [93]. The other channel parameters are set as $\alpha_0 = 3.5$, $\alpha_{\frac{\pi}{2}} = 2$, $\kappa_0 = 5$ dB, and $\kappa_{\frac{\pi}{2}} = 15$dB, with reference to [121]. Considering the low rate transmission requirement of typical sensor nodes and based on the measurement results in [147], the remaining parameters used in this section are set as $R^* = 0.63$bit/s/Hz, $\xi = 0.5$, $\beta = 0.5$, $P_0 = 20$ dBm, $\sigma_n^2 = -190$ dBm, $\mathcal{B} = 10$Hz, and $\zeta_{i,k} = 0.35$ for all sensor nodes, unless indicated otherwise. It is also set that the maximum flight altitude as $H_{\max} = 3$ km, considering the link budget.

5.5.2 Outage Probability Versus UAV Transmission Power

The accuracy of our theoretical results is firstly verified, which developed in the previous section by comparing with the corresponding simulation results. The outage probabilities of NOMA, OMA, and RELAY with respect to the UAV transmission power P_0 are compared in Fig. 5.4, where the UAV altitude is fixed at $H = 600$ m and coverage radius is set as $r_{\mathcal{C}} = 800$ m. It can be observed that the analytical results agree well with the corresponding simulation results. In the case of NOMA, the analytical result of (5.31) is based on the lower bound, but it is observed that the gap from the simulation results is negligible. Therefore, these bounds will be adopted for the subsequent numerical evaluations.

[3] Even though it is exclusively focused on this specific topology, it has been confirmed that similar results may be obtained by other realizations generated in a pseudo-random manner.



(a) BBP strategy

(b) BWP strategy

Figure 5.3: Topology of ten sensor nodes based on pseudo-random positioning adopted throughout numerical performance evaluation. The markers represent sensor node positions and dotted lines represent the sensor node pairs based on (a) BBP strategy and (b) BWP strategy.

From this figure, it can be observe that the outage probabilities can be successfully reduced as the transmission power P_0 exceeds 20 dBm in this network and parameter setting. It is interesting to observe that NOMA eventually exhibits an irreducible error floor as P_0 increases. In particular, the NOMA scheme with BWP strategy is significantly worse than that with BBP. This is due to the fact that there always exists a pair that is closely located in terms of their distance from the UAV in the case of BWP strategy, thus substantially reducing the signal-to-interference power ratio (SIR) that determines the detectability of the center area sensors by UAV. This property may be mitigated by BBP strategy, but the error floor will be inevitable since the SIR achieved by UAV cannot be reduced by increasing P_0.

On the other hand, in the case of RELAY, BWP strategy exhibits lower outage probability compared to BBP strategy. The reason for this behavior may be conjectured as follows. In the first period of the second phase, the outage event will be dominated by transmission failure of the worst sensor node in the cell-edge group. In BWP strategy, this node is assisted by the best sensor node in the center area group through cooperative relaying in the second period, which is likely to be successful since its channel condition is best among all the sensor nodes. Due to this balance of good and bad links with UAV, the total outage performance may be improved more effectively in the case of BWP strategy.

5.5.3 Outage Probability Versus UAV Altitude

In Fig. 5.5, the outage probabilities of NOMA, OMA, and RELAY with respect to the UAV altitude H are compared, where the coverage radius is set as $r_C = 800$ m. Again, it is observed that the analytical results well agree with the corresponding simulation results.

From this figure, it can be observed that as the UAV altitude increases, the outage probability approaches 1 eventually. This is because the path loss component between UAV and sensor nodes increases, thus resulting in reduction of the energy supplied to all the sensor nodes. Similar to the previous results in Fig. 5.4, it is observed that BBP strategy outperforms BWP strategy in the case of NOMA, whereas BWP strategy is better than BBP strategy in the case of RELAY.

5.5.4 Outage Probability Versus Coverage

Having observed that the analytical expressions and simulations well agree in the previous results, the subsequent numerical results will be shown based exclusively on the theoretical expressions for simplicity.

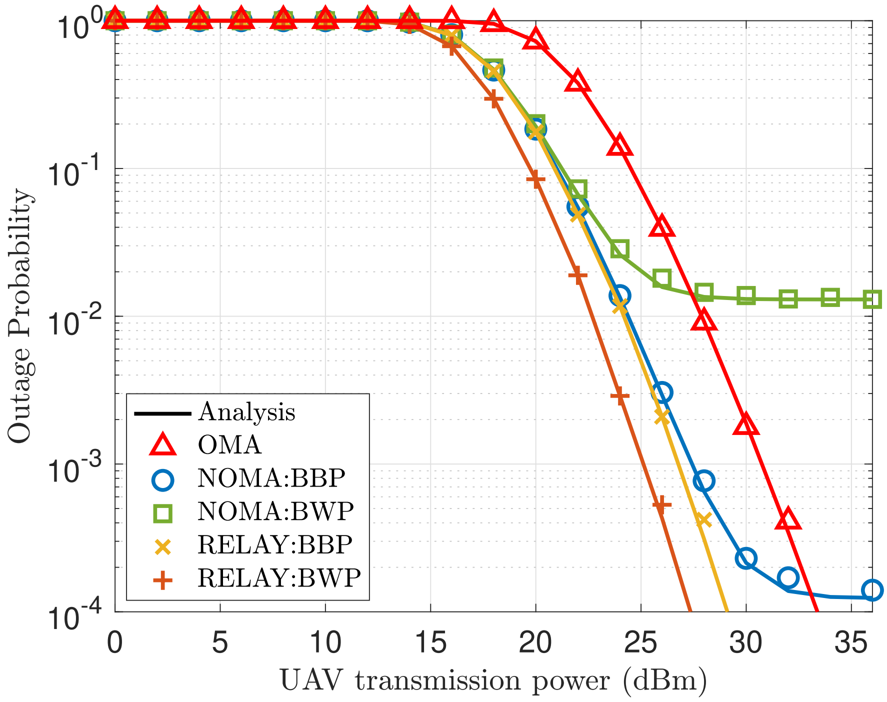


Figure 5.4: Comparison of the outage probabilities of the three different schemes (NOMA, OMA, and RELAY) based on the two node pairing strategies with respect to the UAV transmission power P_0. The solid lines represent analytical results, whereas the markers represent the corresponding simulation results. (The sensor node topology is given in Fig. 5.3, the coverage radius is $r_C = 800$ m, and UAV altitude is $H = 600$ m.)

Fixed UAV Altitude Case

Fig. 5.6 shows the relationship between the outage probability and coverage radius r_C with UAV altitude fixed at $H = 600$ m. It is interesting to observe that in the case of NOMA the performance eventually becomes worse as the coverage area reduces. This can be explained as follows. The average power that can be harvested by the sensor nodes in a small coverage area case is higher than those in a larger coverage area and thus the outage probability decreases as r_C decreases in general. In this case, however, the signal powers of the two sensor nodes that form a pair may not have much difference in the uplink transmission. Since the receiver based on SIC has difficulty in decoding the two different signals with similar power, reduction of the coverage area may eventually lead to increasing outage probability for NOMA scheme that relies on SIC.

From the above observations, it may be concluded that when the coverage area is small, it is better to use cooperative relaying than NOMA. Moreover, the comparison reveals that NOMA becomes even inferior to OMA as the coverage area decreases.

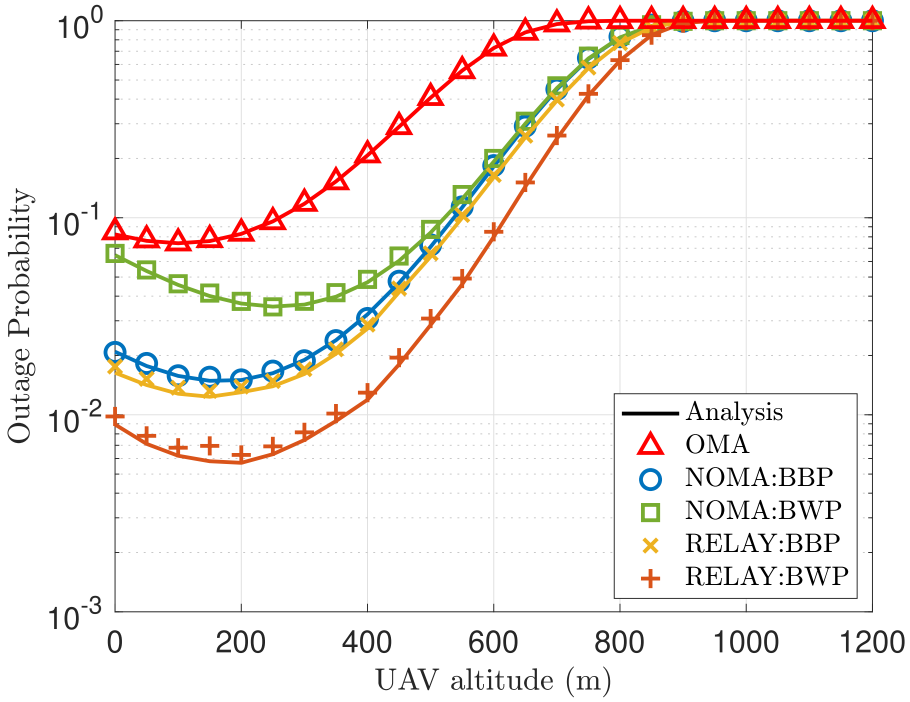


Figure 5.5: Comparison of the outage probabilities of the three different schemes (NOMA, OMA, and RELAY) based on the two node pairing strategies with respect to the UAV altitude H. The solid lines represent analytical results, whereas the markers represent the corresponding simulation results. (The sensor node topology is given in Fig. 5.3, and the coverage radius is $r_{\mathcal{C}} = 800$ m.)

Optimal UAV Altitude Case

In Fig. 5.7, the relationship between the radius of the coverage area and outage probability evaluated is investigated at the optimal altitude H^* defined in (5.18). It can be observed that for NOMA scheme, the error floor exists when the coverage area is small similar to the observation in Fig. 5.6. Comparing Fig. 5.6 and Fig. 5.7, it is clearly observed that the performance of all the schemes can be significantly improved by adjusting the altitude of UAV and thus can enhance the coverage area for a given target outage probability.

5.5.5 Effect of Node Locations

To gain further insight on each scheme, only on a single pair and their outage probabilities will be focused and evaluated for given node locations. Note that in the case of NOMA and OMA schemes, the outage probabilities of each pair $P_{\text{out},k}$ depend on the radii of the two nodes

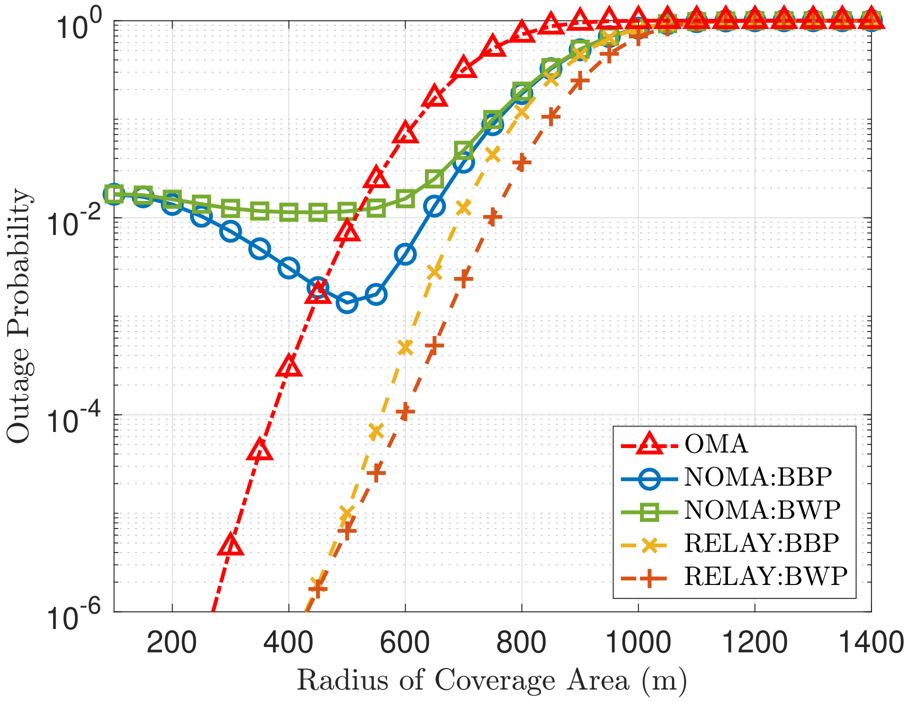


Figure 5.6: Comparison of the outage probabilities of the three different schemes (NOMA, OMA, and RELAY) based on the two node pairing strategies with respect to the coverage radius $r_{\mathcal{C}}$. (The sensor node topology is given in Fig. 5.3 and UAV altitude is $H = 600$ m.)

$(r_{1,k}, r_{2,k})$ (i.e., the distance from the center) but not on the distance between the two nodes, as they only utilize A2G and G2A links. On the other hand, in the case of RELAY, its outage probability depends also on the distance between the two nodes d_k defined in (5.12) as they utilize the associated G2G link. Therefore, the effect of the three parameters $(r_{1,k}, r_{2,k}, d_k)$ on the resulting outage probabilities will be investigated.

Fig. 5.8 shows the comparison of the outage probabilities where $r_{1,k} = 400$ m or 600 m, and $r_{2,k} = r_{1,k} + \epsilon$ with ϵ ranging from 0 to 400 m. In the case of RELAY, the node distances are chosen as either $d_k = r_{2,k} - r_{1,k}$ (closest case) or $d_k = r_{2,k} + r_{1,k}$ (furthest case) for demonstration purpose. From the figure, it can be observed that except for RELAY with two nodes located closely, the performance becomes worse as the radius of the cell-edge node $r_{2,k}$ increases. This results from the fact that A2G and G2A links of $S_{2,k}$ become less reliable as $r_{2,k}$ increases. For NOMA, there exists an optimal node location of $S_{2,k}$ that minimizes the outage probability. This is associated with the NOMA principle that has an optimal power balance of the two pairing sensor nodes for successful SIC. (The SIC with small ϵ is likely to perform worse than that with large ϵ.) On the other hand, in the case of RELAY, the performance starts to degrade as the node

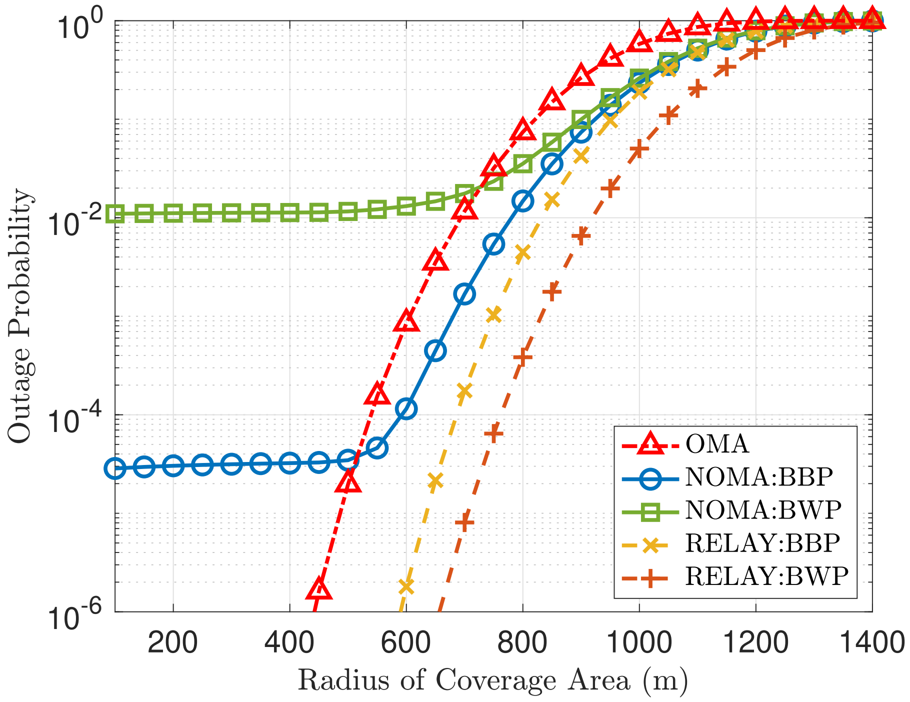


Figure 5.7: Comparison of the outage probabilities of the three different schemes (NOMA, OMA, and RELAY) based on the two node pairing strategies at the optimized UAV altitude H^* with respect to the coverage radius r_C. (The sensor node topology is given in Fig. 5.3.)

distance d_k exceeds some threshold value as the G2G link becomes less reliable.

From these results, our observation can be summarized as follows: When both $S_{1,k}$ and $S_{2,k}$ are located close to the UAV, OMA performs best. On the other hand, RELAY performs well as long as $S_{1,k}$ is close to the UAV and G2G link is reliable. The performance of NOMA strongly depends on the location of the two nodes, and may outperform RELAY as the distance between $S_{1,k}$ and the UAV increases.

5.5.6 Time Ratio Optimization

So far, it has fixed that the energy transmission time ratio ξ as 0.5 and the relaying time ratio β for RELAY as 0.5. In what follows, the optimal values for these parameters are investigated.

Outage Probabilities Versus Time Ratio ξ

The optimum value of ξ is firstly investigated for the four schemes (including OPT). In Fig. 5.9, the outage probabilities with respect to ξ are compared, where the UAV altitude is fixed at $H = 600$ m and the coverage radius is set as $r_{\mathcal{C}} = 800$ m in Fig. 5.3. From this figure, it is observed that the optimal ξ varies depending on the transmission schemes, and OPT can achieve the best performance for a given parameter ξ as expected.

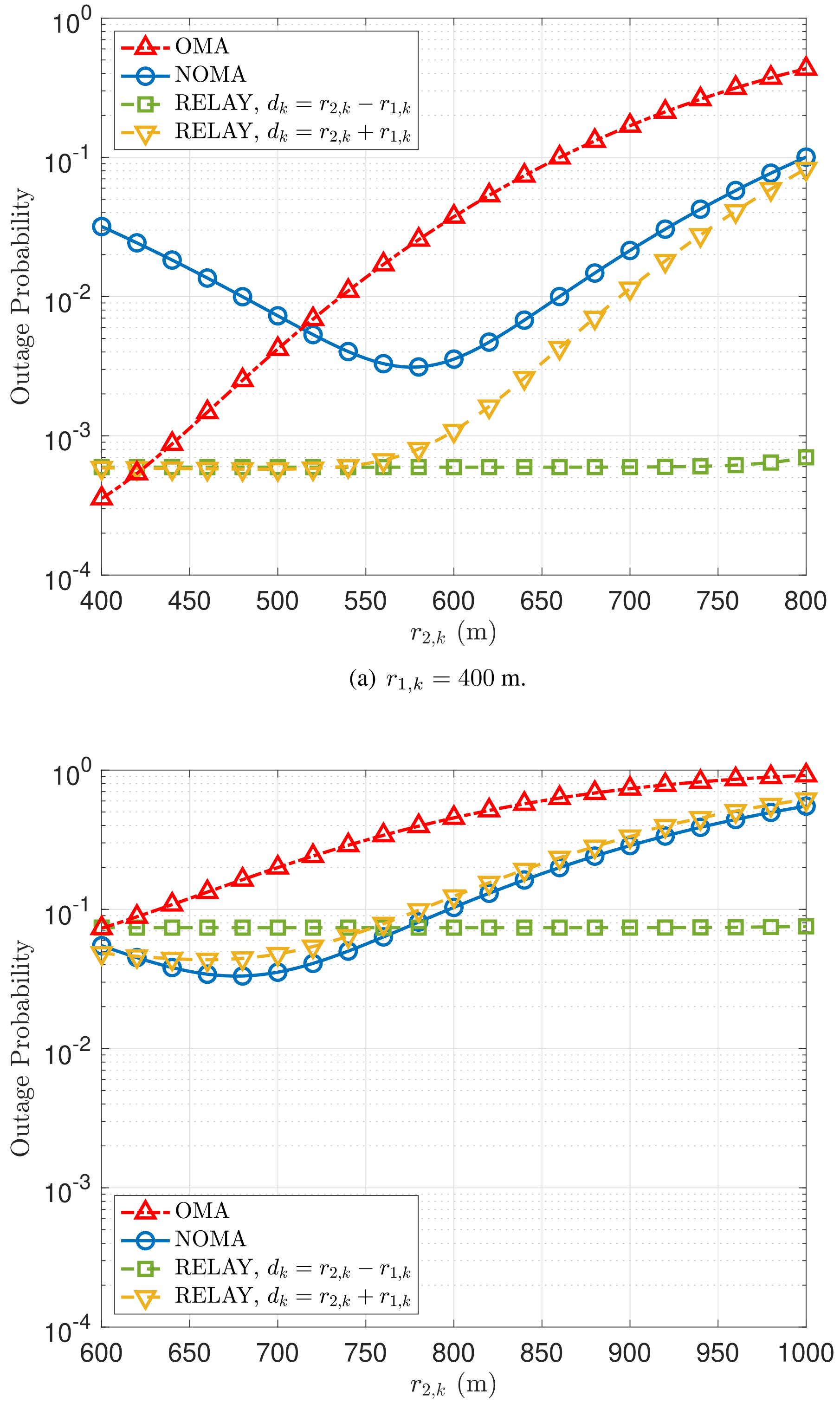
Outage Probabilities Versus Time Ratio β for RELAY

Finally, the performance dependence of RELAY on the time ratio β is investigated that determines the fraction of the second phase to be used for the signal transmission of the cell-edge sensor node $S_{2,k}$ for various cases of ξ. The results are shown in Fig. 5.10 with $H = 600$ m and $r_{\mathcal{C}} = 800$ m, where it is observed that there is an optimal value of β depending on ξ. In all the cases, the optimal value of β is slightly higher than 0.5, which indicates that more time should be devoted to the signal transmission of the cell-edge sensor nodes even with the assistance of the center area sensor nodes.

Here, for a given altitude H, ξ and β have separately optimized. It would be of significant interest to *jointly* optimize these parameters such that the outage probability can be minimized. Nevertheless, due to the unwieldy mathematical expressions involved in the resulting outage probabilities, the joint optimization of ξ, β, and H would be challenging, and thus will be left as future work.

5.6 Conclusion

In this chapter, the performance of UAV data collection in wireless powered sensor networks has investigated. Depending on how all the sensor nodes within a coverage area transmit their signals to UAV, the two advanced schemes based on the power-domain NOMA using SIC and the cooperative relaying (RELAY) have been compared, along with the conventional OMA scheme. For each scheme, the two user pairing strategies have studied in order to enhance the performance in the uplink transmission. To this end, we have developed mathematical expressions for their outage probabilities. The comparisons of each scheme with two pairing strategies have revealed that for the case of NOMA, BBP strategy outperforms BWP strategy, while BWP strategy turns out to be preferable in the case of RELAY.



(a) $r_{1,k} = 400$ m.

(b) $r_{1,k} = 600$ m.

Figure 5.8: Comparison of the outage probabilities of the kth pair ($\hat{P}_{\text{out},k}^{\text{NOMA}}$, $P_{\text{out},k}^{\text{RELAY}}$, and $P_{\text{out},k}^{\text{OMA}}$) as a function of the node locations $(r_{1,k}, r_{2,k}, d_k)$ with (a) $r_{1,k} = 400$ m and (b) $r_{1,k} = 600$ m. (The UAV altitude is fixed at $H = 600$ m.)

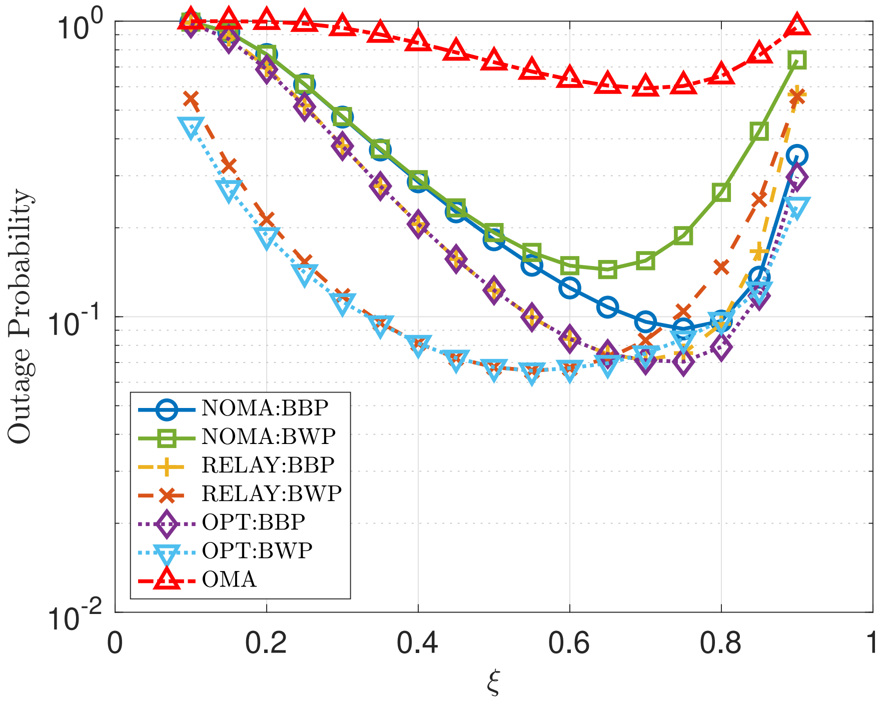


Figure 5.9: Comparison of the outage probabilities of the four different schemes (NOMA, OMA, RELAY, and OPT) based on the two node pairing strategies with respect to the energy transmission time ratio ξ. (The sensor node topology is given in Fig. 5.3, the coverage radius is $r_{\mathcal{C}} = 800$ m, and UAV altitude is $H = 600$ m.)

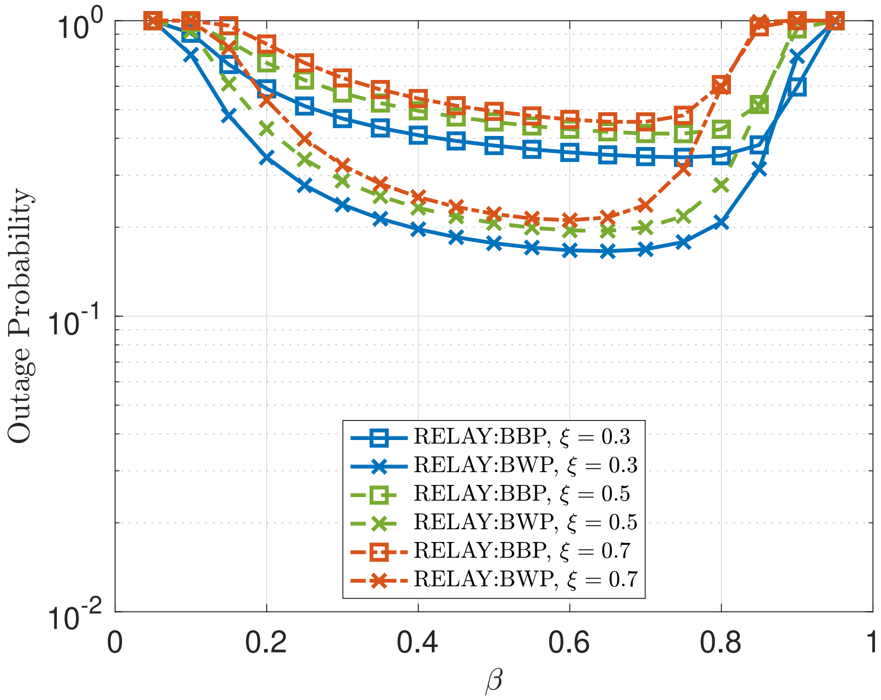


Figure 5.10: Comparison of the outage probabilities of RELAY based on the two node pairing strategies with respect to the relaying time ratio β and several different energy transmission time ratio ξ. (The sensor node topology is given in Fig. 5.3, the coverage radius is $r_{\mathcal{C}} = 800$ m, and UAV altitude is $H = 600$ m.)

Chapter 6

Conclusion

6.1 Summary

We have proposed several modern wireless relaying cooperative networks and investigated the transmission performance and PHY security performance. They are summarized as follows:

- In Chapter 3, it is analyzed the outage probabilities of a multiple-antenna equipped cooperative relaying network with a single eavesdropper without CSI information. The cooperative devices that had successfully decoded the information from source serve as relays whereas the remaining devices serve as jammers. The multiple-antenna equipped devices form a beam to destination via accessing the full CSI to destination. The closed-form expression of the main channel, the asymptotic lower bound of the eavesdropper channel, and the approximated closed-form expression of the secrecy outage probability have derived. The numerical comparisons have shown that the analytical expressions and simulation results using Monte-Carlo method match well, suggesting the accuracy of our analytical approach.

- In Chapter 4, the performance of the UAV swarm cooperative relaying network over Rician fading channels was investigated in the presence of a single UAV eavesdropper. Depending on how the UAV swarm is selected for relay or how it is divided into relays and jammers, the four specific models are introduced, and for each model, the mathematical expressions are developed for the transmission outage probabilities of both main channel and eavesdropping channel. The numerical comparisons with Monte-Carlo simulation results have shown that the analytical expressions match well with simulations, thus suggesting the accuracy of our analytical approach.

- In Chapter 5, the performance of UAV data collection in wireless powered sensor networks has investigated. Depending on how all the sensor nodes within a coverage area transmit their signals to UAV, the two advanced schemes, one based on the power-domain NOMA using SIC, and the other based on the cooperative relaying (RELAY) have been compared, along with the conventional OMA scheme. For each scheme, the two user pairing strategies have been studied in order to enhance the performance in the uplink transmission. To this end, mathematical expressions have been developed for their outage probabilities. The comparisons of each scheme with two pairing strategies have revealed that for the case of NOMA, BBP strategy outperforms BWP strategy, while BWP strategy turns out to be preferable in the case of RELAY.

6.2 Future Work

The remaining issues left for future work include the following.

- In Chapter 3, the transmission scenario can be extended from single-antenna to multiple-antenna, i.e., MIMO scenario. Moreover, we need to optimize the power allocation at the relay. This optimization issue can be solved by Karush-Kuhn-Tucker (KKT) condition. Specifically, one of the solutions based on the water-filling algorithm considering the eigenvectors of the matrix of the channel gain coefficients was proposed in [148]. Moreover, the system modeling without eavesdropper channel state information needs further investigation.

- In Chapter 4 and Chapter 5, it is ideally assumed that the UAV as the relaying device where the transmitter and receiver are fixed in the air. UAV-enabled communication networks set up outdoors in practical scenarios are easily affected by complex environments, e.g., wind, obstacles characteristics in the wild transmission, the acceleration in the movement, and physical shakings. Although the trajectory design is a hot topic of the UAV-enabled data collection and broadcasting communication, most of the research works are simply defining the movement of UAVs as uniform linear motion. The highly realistic movement model of UAV-enabled communication needs further investigation.

- In the work of Chapter 4, the A2A and A2G wireless communication channels based on the UAV transmission are modeled by fixed coefficients, which may not be practical. Although several researches on realistic A2G wireless communication models have been proposed, the realistic A2A wireless communication fading channels need further investigation. Furthermore, in order to improve the energy efficiency of beyond fifth-generation (B5G) wireless communication, multiple antenna scenarios should be considered, e.g., massive multiple-input-multiple-output (MIMO), and reconfigurable intelligent surface (RIS).

- Furthermore, in Chapter 5, it has not addressed complexity issues as well as implementation challenges. For example, even though RELAY outperforms NOMA in many scenarios, the associated complexity upon implementation of RELAY based on the decode and forward principle should be considerably higher than that of NOMA based on SIC. The energy harvesting model of sensor nodes requires further investigation, and the energy consumption required for signal processing should be also taken into consideration. The synchronization issues among sensor nodes as well as the effect of practical constraints with respect to actual modulation and coding should be of significant importance. Also, in order to implement the OPT scheme, how to autonomously identify the best scheme for each pair needs to be established.

Appendix A

Appendix of Chapter 4

A.1 Proof of Theorem 1

In (4.25), $|h|^2$ and $|j_1|^2$ follow the PDF of $f_Z(z)$ in (4.2) with Rician factor given by K_G and K_A, respectively. The corresponding CDF is then expressed as

$$F_Z(z) = 1 - Q_1\left(\sqrt{2K}, \sqrt{\frac{2(K+1)}{\Omega}z}\right). \tag{A.1.1}$$

From (4.25), it may be written

$$\begin{aligned}\mathrm{Pr}_{L,1}^{\mathrm{ORSJ}}(\gamma_{\mathrm{th}}) &= \mathrm{Pr}\left(|h|^2 < \frac{\kappa_A P_j}{\kappa_G P_0 \gamma_{\mathrm{th}}}|j_1|^2\right)\\ &= \int_0^\infty \left[1 - Q_1\left(\sqrt{2K_G}, \sqrt{\frac{2(K_G+1)}{\Omega}}\sqrt{\frac{\kappa_A P_j \gamma_{\mathrm{th}}}{\kappa_G P_0}z}\right)\right] f_Z(z)dz\\ &= 1 - \underbrace{\int_0^\infty Q_1\left(\sqrt{2K_G}, \sqrt{\frac{2(K_G+1)}{\Omega}}\sqrt{\frac{\kappa_A P_j \gamma_{\mathrm{th}}}{\kappa_G P_0}z}\right) f_Z(z)dz,}_{\triangleq H_2}\end{aligned} \tag{A.1.2}$$

where $f_Z(z)$ is given by (4.2) with $K = K_A$.

Under the assumption of $K_A = K_G = K$, simplification of (A.1.2) becomes feasible. Specifically, the second term of (A.1.2) in this case, denoted by H_2 in what follows, can be expressed as [91]

$$\begin{aligned}H_2 &= \left(\frac{K+1}{\Omega}\right)e^{-K}\int_0^\infty e^{-\frac{(K+1)z}{\Omega}} I_0\left(2\sqrt{\frac{K(K+1)z}{\Omega}}\right) Q_1\left(\sqrt{2K}, \sqrt{\frac{2(K+1)}{\Omega}}\sqrt{\frac{\kappa_A P_j z \gamma_{\text{th}}}{\kappa_G P_0}}\right) dz \\ &= \left(\frac{K+1}{\Omega}\right)e^{-K}\left[\frac{1}{p}e^{\frac{c^2}{4p}} + \frac{2}{c}\left(\frac{c}{2p+\beta^2}\right)e^{\frac{c^2-2p\alpha^2}{2p+\beta^2}} I_0\left(\frac{\alpha\beta c}{2p+\beta^2}\right)\right. \\ &\quad \left. - \frac{e^{\frac{c^2}{4p}}}{p} Q_1\left(\frac{\beta c}{\sqrt{2p(2p+\beta^2)}}, \alpha\sqrt{\frac{2p}{2p+\beta^2}}\right)\right] \end{aligned} \tag{A.1.3}$$

where $\alpha = \sqrt{2K}$, $\beta = \sqrt{\frac{2\kappa_A P_j \gamma_{\text{th}}(K+1)}{\kappa_G P_0 \Omega}}$, $c = 2\sqrt{\frac{K(K+1)}{\Omega}}$, and $p = \frac{K+1}{\Omega}$. This leads to (4.28). In a similar manner, the lower bound of (4.29) can be obtained.

A.2 Proof of Theorem 2

The lower bound defined by (4.47) can be expressed as

$$\begin{aligned}\Pr_L^{\text{ORSJ-E}}(\gamma_{\text{th}}) &= \Pr\left(\frac{P_0 Z}{P_j \gamma_{\text{th}}} < |v_1|^2\right) \\ &= 1 - Q_1\left(\sqrt{2K_A}, \sqrt{\frac{2(K_A+1)}{\Omega}\frac{P_0 Z}{P_j \gamma_{\text{th}}}}\right)\end{aligned} \tag{A.2.1}$$

where $Z = \mathbb{B}_1|f_1|^2 + \mathbb{B}_2|f_2|^2$. The MGF of Z under the assumption of $K_A = K_G = K$ is given from (4.44) as

$$\mathcal{M}_Z(s) = \left(1 - q + \frac{e^{-K+\frac{K(1+K)}{1+K+s\Omega}} q(1+K)}{1+K+s\Omega}\right)^2. \tag{A.2.2}$$

Using inverse Laplace transform, we can derive the PDF of Z as

$$\begin{aligned}f_Z(z) &= \mathcal{L}^{-1}\left(\mathcal{M}_Z(s)\right) \\ &= (1-q)^2\delta(z) + \frac{2e^{-K-\frac{(1+K)z}{\Omega}}(1-q)q(1+K)}{\Omega} I_0\left(2\sqrt{\frac{K(1+K)}{\Omega}}\sqrt{z}\right) \\ &\quad + e^{-2K-\frac{(1+K)z}{\Omega}} q^2 \sqrt{\frac{(1+K)^3 z}{2K\Omega^3}} I_1\left(2\sqrt{\frac{2K(1+K)}{\Omega}}\sqrt{z}\right).\end{aligned} \tag{A.2.3}$$

Hence, the corresponding lower bound for the outage probability of eavesdropper in ORSJ can be expressed as

$$\mathrm{Pr}_L^{\mathrm{ORSJ-E}}(\gamma_{\mathrm{th}}) = 1 - \int_0^\infty Q_1\left(\sqrt{2K_A}, \sqrt{\frac{2(K_A+1)}{\Omega}\frac{P_0 z}{P_j\gamma_{\mathrm{th}}}}\right) f_Z(z)dz \tag{A.2.4}$$

In (A.2.4), the integral contains Marcum-Q function, modified Bessel function of the first kind, and exponential function, but it can be expressed in a simpler form using [91], which leads to the expression (4.48) in Theorem 2.

A.3 Proof of Theorem 3

From (4.51), by defining $Z = \mathbb{B}_1|f_1|^2 + \mathbb{B}_2|f_2|^2$, the outage probability lower bound of eavesdropper can be expressed as

$$\begin{aligned}\mathrm{Pr}_L^{\mathrm{ORSMJ-E}}(\gamma_{\mathrm{th}}) &= \mathrm{Pr}\left(\frac{P_0 Z}{P_j\gamma_{\mathrm{th}}} < \sum_{n=1}^{N}|v_n|^2\right) \\ &= 1 - Q_N\left(\sqrt{2NK_A}, \sqrt{\frac{2(1+K_A)}{\Omega}}\sqrt{\frac{P_0 Z}{P_j\gamma_{\mathrm{th}}}}\right)\end{aligned} \tag{A.3.1}$$

which stems from the fact that the sum of N squared i.i.d Rician random variables is non-central chi-squared distribution with $2N$ degrees of freedom [102, 149]. Under the assumption of $K_A = K_G = K$ and using the PDF of Z, i.e., (A.2.3) in Appendix A.2, we have the following expression:

$$\mathrm{Pr}_L^{\mathrm{ORSMJ-E}}(\gamma_{\mathrm{th}}) = 1 - \int_0^\infty f_Z(z) Q_N\left(\sqrt{2NK}, \sqrt{\frac{2(1+K)}{\Omega}}\sqrt{\frac{P_0 z}{P_j\gamma_{\mathrm{th}}}}\right) dz. \tag{A.3.2}$$

Substituting [150, vol.4 eq.(3.15.2.2)], [150, vol.4 eq.(3.15.2.17)], and [91, eq.(22),(24)-(25)] into (A.3.2), the final expression of Theorem 3 can be obtained.

A.4 Proof of Theorem 4

Similar to the proof of Theorem 3, by defining $Y = \mathbb{B}_1 |f_1|^2$, from (4.55) we have

$$\begin{aligned}\mathrm{Pr}_L^{\mathrm{MRCMJ-E}}(\gamma_{\mathrm{th}}) &= \mathrm{Pr}\left(\frac{\kappa_G P_0 Y}{\kappa_A P_j \gamma_{\mathrm{th}}} < \sum_{n=1}^{N} |v_n|^2\right)\\ &= 1 - Q_N\left(\sqrt{2NK_A}, \sqrt{\frac{2(1+K_A)}{\Omega}}\sqrt{\frac{\kappa_G P_0 Y}{\kappa_A P_j \gamma_{\mathrm{th}}}}\right)\end{aligned} \tag{A.4.1}$$

Similar to Z in the proof of Theorem 3, the PDF of Y is expressed as

$$f_Y(y) = (1-q)\delta(y) + qe^{-\left(\frac{(1+K_G)y}{\Omega}+K_G\right)}\left(\frac{1+K_G}{\Omega}\right) I_0\left(2\sqrt{\frac{(K_G+1)K_G y}{\Omega}}\right). \tag{A.4.2}$$

Therefore, we have

$$\mathrm{Pr}_L^{\mathrm{MRCMJ-E}}(\gamma_{\mathrm{th}}) = 1 - \int_0^{\infty} f_Y(y) Q_N\left(\sqrt{2NK_A}, \sqrt{\frac{2(1+K_A)}{\Omega}}\sqrt{\frac{\kappa_G P_0 y}{\kappa_A P_j \gamma_{\mathrm{th}}}}\right) dy. \tag{A.4.3}$$

Under the assumption of $K_A = K_G = K$ and substituting [150, vol.4 eq.(3.15.2.2)], [150, vol.4 eq.(3.15.2.17)], and [91, eq.(22),(24)-(25)] into (A.4.3), the expression shown in Theorem 4 can be obtained.

Bibliography

[1] K. J. R. Liu, A. K. Sadek, W. Su, and A. Kwasinski, *Cooperative Communications and Networking*. New York City, NY, USA: Cambridge University Press, 2009.

[2] P. N. Son and H. Y. Kong, "Cooperative communication with energy-harvesting relays under physical layer security," *IET Commun.*, vol. 9, no. 17, pp. 2131–2139, Nov. 2015.

[3] R. Fan, J. Cui, S. Jin, K. Yang, and J. An, "Optimal node placement and resource allocation for UAV relaying network," *IEEE Commun. Lett.*, vol. 22, no. 4, pp. 808–811, Apr. 2018.

[4] M. Ju and H.-C. Yang, "Optimum design of energy harvesting relay for two-way decode-and-forward relay networks under max-min and max-sum criterions," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 6682–6697, Oct. 2019.

[5] K. Sultan, "Best relay selection schemes for NOMA based cognitive relay networks in underlay spectrum sharing," *IEEE Access*, vol. 8, pp. 190 160–190 172, 2020.

[6] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity-part I: System description," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1938, Nov. 2003.

[7] ——, "User cooperation diversity-part II: Implementation aspects and performance analysis," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1939–1948, Nov. 2003.

[8] R. U. Nabar, H. Bolcskei, and F. W. Kneubuhler, "Fading relay channels: Performance limits and space-time signal design," *IEEE J. Sel. Areas Commun.*, vol. 22, no. 6, pp. 1099–1109, Aug. 2004.

[9] H. Cui, L. Song, and B. Jiao, "Multi-pair two-way amplify-and-forward relaying with very large number of relay antennas," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2636–2645, May 2014.

[10] S. Luo and K. C. Teh, "Amplify-and-forward based two-way relay arq system with relay combination," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 299–302, Feb. 2015.

[11] D. Li, "Amplify-and-forward relay sharing for both primary and cognitive users," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2796–2801, Apr. 2016.

[12] Y. Dong, M. J. Hossain, and J. Cheng, "Performance of wireless powered amplify and forward relaying over Nakagami-m fading channels with nonlinear energy harvester," *IEEE Commun. Lett.*, vol. 20, no. 4, pp. 672–675, Apr. 2016.

[13] S. Li, K. Yang, M. Zhou, J. Wu, L. Song, Y. Li, and H. Li, "Full-duplex amplify-and-forward relaying: Power and location optimization," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8458–8468, Sep. 2017.

[14] K. M. Rabie and B. Adebisi, "Enhanced amplify-and-forward relaying in non-Gaussian PLC networks," *IEEE Access*, vol. 5, pp. 4087–4094, 2017.

[15] L. Jiang and H. Jafarkhani, "mmWave amplify-and-forward MIMO relay networks with hybrid precoding/combining design," *IEEE Trans. Wireless Commun.*, vol. 19, no. 2, pp. 1333–1346, Feb. 2020.

[16] A. S. Ibrahim, A. K. Sadek, W. Su, and K. J. R. Liu, "Cooperative communications with relay-selection: When to cooperate and whom to cooperate with?" *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2814–2827, Jul. 2008.

[17] M. R. Bhatnagar, R. K. Mallik, and O. Tirkkonen, "Performance evalution of best-path selection in a multihop decode-and-forward cooperative system," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2722–2728, Apr. 2016.

[18] Y. Gu and S. Aissa, "RF-based energy harvesting in decode-and-forward relaying systems: Ergodic and outage capacities," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6425–6434, Nov. 2015.

[19] G. T. Djordjevic, K. Kansanen, and A. M. Cvetkovic, "Outage performance of decode-and-forward cooperative networks over Nakagami-m fading with node blockage," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 5848–5860, Sep. 2016.

[20] H. Liu, Z. Ding, K. J. Kim, K. S. Kwak, and H. V. Poor, "Decode-and-forward relaying for cooperative NOMA systems with direct links," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8077–8093, Dec. 2018.

[21] R. Fan, S. Atapattu, W. Chen, Y. Zhang, and J. Evans, "Throughput maximization for multi-hop decode-and-forward relay network with wireless energy harvesting," *IEEE Access*, vol. 6, pp. 24 582–24 595, 2018.

[22] O. M. Kandelusy and S. M. H. Andargoli, "Outage performance of decode-and-forward (DF)-based multiuser spectrum sharing relay system with direct link in the presence of primary users' power," *IET Commun.*, vol. 12, no. 3, pp. 246–254, Feb. 2018.

[23] E. Li, X. Wang, Z. Wu, S. Hao, and Y. Dong, "Outage analysis of decode-and-forward two-way relay selection with different coding and decoding schemes," *IEEE Syst. J.*, vol. 13, no. 1, pp. 125–136, Mar. 2019.

[24] M. Asadpour, B. Van den Bergh, D. Giustiniano, K. A. Hummel, S. Pollin, and B. Plattner, "Micro aerial vehicle networks: an experimental analysis of challenges and opportunities," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 141–149, Jul. 2014.

[25] K. Namuduri, S. Chaumette, J. H. Kim, and J. P. G. Sterbenz, *UAV Networks and Communications*. Cambridge University Press, 2017.

[26] K. P. Valavanis and G. J. Vachtsevanos, *Handbook of Unmanned Aerial Vehicles*. Springer, 2015.

[27] F. Ono, H. Ochiai, and R. Miura, "A wireless relay network based on unmanned aircraft system with rate optimization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7699–7708, Nov. 2016.

[28] M. M. Azari, F. Rosas, K.-C. Chen, and S. Pollin, "Ultra reliable UAV communication using altitude and cooperation diversity," *IEEE Trans. Commun.*, vol. 66, no. 1, pp. 330–344, Jan. 2018.

[29] M. M. Azari, F. Rosas, and P. Sofie, "Cellular connectivity for UAVs: Network modeling, performance analysis, and design guidelines," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3366–3381, Jul. 2019.

[30] W. Wang, X. Li, M. Zhang, K. Cumannan, D. W. K. Ng, G. Zhang, J. Tang, and O. A. Dober, "Energy-constrained UAV-assisted secure communications with position optimization and cooperative jamming," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4476–4489, Jul. 2020.

[31] H. Shakhatreh, A. H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N. S. Othman, A. Khreishah, and M. Guizani, "Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges," *IEEE Access*, vol. 7, pp. 48 572–48 634, 2019.

[32] W. Ejaz, M. A. Azam, S. Saadat, F. Iqbal, and A. Hanan, "Unmanned aerial vehicle enabled IoT platform for disaster management," *Energies*, vol. 12, no. 14, p. 2706, Jul. 2019.

[33] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[34] J. Zhao, F. Gao, Q. Wu, S. Jin, Y. Wu, and W. Jia, "Beam tracking for UAV mounted SatCom on-the-move with massive antenna array," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 2, pp. 363–375, Feb. 2018.

[35] Y. Zeng, R. Zhang, and T. J. Lim, "Throughput maximization for UAV-enabled mobile relaying systems," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 4983–4996, Dec. 2016.

[36] Y. Zhang, Z. Mou, F. Gao, L. Xing, J. Jiang, and Z. Han, "Hierarchical deep reinforcement learning for backscattering data collection with multiple UAVs," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3786–3800, Mar. 2021.

[37] J. Zhao, Y. Wang, Z. Fei, X. Wang, and Z. Miao, "NOMA-aided UAV data collection system: Trajectory optimization and communication design," *IEEE Access*, vol. 8, pp. 155 843–155 858, 2020.

[38] F. Luo, C. Jiang, J. Du, J. Yuan, Y. Ren, S. Yu, and M. Guizani, "A distributed gateway selection algorithm for UAV networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, Mar. 2015.

[39] R. Duan, J. Wang, C. Jiang, Y. Ren, and L. Hanzo, "The transmit-energy vs computation-delay trade-off in gateway-selection for heterogenous cloud aided multi-UAV systems," *IEEE Trans. Commun.*, vol. 67, no. 4, pp. 3026–3039, Apr. 2019.

[40] M. Vaezi, R. Schober, Z. Ding, and H. V. Poor, "Non-orthogonal multiple access: Common myths and critical questions," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 174–180, Oct. 2019.

[41] M. Vaezi and H. V. Poor, "NOMA: An information-theoretic perspective," in *Multiple Access Techniques for 5G Wireless Networks and Beyond*, M. Vaezi, Z. Ding, and H. V. Poor, Eds. Cham: Springer International Publishing, 2019, pp. 167–193.

[42] F. Mokhtari, M. R. Milli, F. Eslami, F. Ashtiani, B. Makki, M. Mirmohseni, M. Nasiri-Kenari, and T. Svensson, "Download elastic traffic rate optimization via NOMA protocols," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 713–727, Jan. 2019.

[43] Z. Ding, M. Peng, and H. V. Poor, "Cooperative non-orthogonal multiple access in 5G systems," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1462–1465, Aug. 2015.

[44] S. M. R. Islam, N. Avazov, O. A. Dobre, and K.-s. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 721–742, Secondquarter 2017.

[45] 3GPP, "Study on network-assisted interference cancellation and suppression (NAICS) for LTE v.12.0.1," 3rd Generation Partnership Project (3GPP), Sophia Antipolis, France, Rep. TR 36.866, Mar. 2014.

[46] MediaTek, "Study on downlink multiuser superposition transmission (MUST) for LTE," 3rd Generation Partnership Project (3GPP), Hsinchu, Taiwan, Rep. TR 36.859, Apr. 2015.

[47] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks," in *Wireless Network Security*, Y. Xiao, X. S. Shen, and D.-Z. Du, Eds. Boston, MA, USA: Springer, 2007, ch. 5, pp. 103–135.

[48] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, Second Quarter 2006.

[49] T. T. Karygiannis and L. Owens, "Wireless network security: 802.11, bluetooth and handheld devices," Gaithersburg, MD, USA, Nov. 2002.

[50] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. IEEE Annu. Symp. Found. of Comput. Sci. (FOCS)*, Santa Fe, NM, USA, Nov. 1994.

[51] R. K. Nichols and P. C. Lekkas, *Wireless Security: Models, Threats, and Solutions*. New York, NY, USA: McGraw-Hill, 2002.

[52] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, United Kingdom: Cambridge University Press, 2011.

[53] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

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

[55] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[56] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[57] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[58] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.

[59] P. Mukherjee, J. Xie, and S. Ulukus, "Secure degree of freedom of one-hop wireless networks with no eavesdropper CSIT," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1898–1922, Mar. 2017.

[60] I. Krikidis, J. S. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative network," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[61] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1544–1554, Mar. 2013.

[62] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[63] X. Liao, Y. Zhang, Z. Wu, Y. Shen, X. Jiang, and H. Inamura, "On security-delay trade-off in two-hop wireless networks with buffer-aided relay selection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1893–1906, Mar. 2018.

[64] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[65] ——, "Secure transmission with multiple antennas – Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[66] R. Feng, M. Dai, and H. Wang, "Distributed beamforming in MISO SWIPT system," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5440–5445, Jun. 2017.

[67] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Trans. Signal Process.*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[68] B. Medepally and N. B. Mehta, "Voluntary energy harvesting relays and selection in cooperative wireless networks," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3543–3553, Nov. 2010.

[69] H. Al-Tous and I. Barhumi, "Reinforcement learning framework for delay sensitive energy harvesting wireless sensor networks," *IEEE Sensors J.*, vol. 21, no. 5, pp. 7103–7113, Mar. 2021.

[70] K. W. Choi, A. A. Aziz, D. Setiawan, N. M. Tran, L. Ginting, and D. I. Kim, "Distributed wireless power transfer system for Internet of Things devices," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2657–2671, Aug. 2018.

[71] A. Goldsmith, *Wireless Communications*. Cambridge, United Kingdom: Cambridge university press, 2005.

[72] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[73] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 1–6.

[74] E. R. Alotaibi and K. A. Hamdi, "Relay selection for multi-destination in cooperative networks with secrecy constraints," in *Proc. IEEE Veh. Technol Conf. Fall (VTC-Fall)*, Vancouver, Canada, Sep. 2014, pp. 1–5.

[75] ——, "Secrecy outage probability analysis for cooperative communication with relay selection under non-identical distribution," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Doha, Qatar, Apr. 2016, pp. 1–6.

[76] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[77] W. Wang, X. Li, M. Zhang, K. Cumanan, D. W. K. Ng, G. Zhang, J. Tang, and O. A. Dobre, "Energy-constrained uav-assisted secure communications with position optimization and cooperative jamming," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4476–4489, Jul. 2020.

[78] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, Jul. 2017.

[79] X. Liu, Z. Li, and C. Wang, "Secure decode-and-forward relay SWIPT systems with power splitting scheme," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7341–7354, Aug. 2018.

[80] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-Eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[81] D. H. Ibrahim, E. S. Hassan, and S. A. El-Dolil, "Improving physical layer security in two-way cooperative networks with multiple eavesdroppers," in *Proc. of Int. Conf. Inform. Syst.*, Cairo, Egypt, Dec. 2014.

[82] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. L. Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[83] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage program," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.

[84] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multiantenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, Jun. 2013.

[85] L. Gui, B. He, X. Zhou, C. Yu, F. Shu, and J. Li, "Energy-efficient wireless powered secure transmission with cooperative jamming for public transportation," *IEEE Trans. Green Commun. Netw.*, vol. 3, no. 4, pp. 876–885, Dec. 2019.

[86] A. Nuttall, "Some integrals involving the Q_M function," *IEEE Trans. Inf. Theory*, vol. 21, no. 1, pp. 95–96, 1975.

[87] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 8th ed., D. Zwillinger and V. Moll, Eds. Waltham, MA, USA: Academic Press, 2014.

[88] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *J. Commun. Netw.*, vol. 14, no. 4, pp. 364–373, Aug. 2012.

[89] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2019.

[90] J. Hu and N. C. Beaulieu, "Accurate closed-from approximations to Ricean sum distributions and densities," *IEEE Commun. Lett.*, vol. 9, no. 2, pp. 133–135, Feb. 2005.

[91] N. Y. Ermolova and O. Tirkkonen, "Laplace transform of product of generalized Marcum Q, Bessel I, and power functions with applications," *IEEE Trans. Signal Process.*, vol. 62, no. 11, pp. 2938–2944, Jun. 2014.

[92] T. Shen and H. Ochiai, "A UAV-aided selective relaying with cooperative jammers for secure wireless networks over Rician fading channels," in *Proc. IEEE Veh. Technol. Conf. Fall (VTC-Fall 2019)*, Honolulu, HI, USA, Sep. 2019.

[93] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal LAP altitude for maximum coverage," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 569–572, Dec. 2014.

[94] F. Ono, H. Ochiai, and R. Miura, "A wireless relay network based on unmanned aircraft system with rate optimization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7699–7708, Nov. 2016.

[95] D. W. Matolak and R. Sun, "Air–ground channel characterization for unmanned aircraft systems —Part I: Methods, measurements, and models for over-water settings," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 26–44, Jan. 2017.

[96] H. Liu, P. L. Yeoh, K. J. Kim, P. V. Orlik, and H. V. Poor, "Secrecy performance of finite-sized in-band selective relaying systems with unreliable backhaul and cooperative eavesdroppers," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1499–1516, Jul. 2018.

[97] Q. Wang, Z. Chen, H. Li, and S. Li, "Joint power and trajectory design for physical-layer secrecy in the UAV-aided mobile relaying system," *IEEE Access*, vol. 6, pp. 62 849–62 855, 2018.

[98] K. J. Kim, P. L. Yeoh, P. V. Orlik, and H. V. Poor, "Secrecy performance of finite-sized cooperative single carrier systems with unreliable backhaul connections," *IEEE Trans. Signal Process.*, vol. 64, no. 17, pp. 4403–4416, Sep. 2016.

[99] P. L. Yeoh, N. Yang, and K. J. Kim, "Secrecy outage probability of selective relaying wiretap channels with collaborative eavesdropping," in *Proc. of 2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[100] F. W. Olver, D. W. Lozier, R. F. Boisvert, and C. W. Clark, *NIST Handbook of Mathematical Functions*, 1st ed. Cambridge University Press, 2010.

[101] H. Ochiai, P. Mitran, H. V. Poor, and V. Tarokh, "Collaborative beamforming for distributed wireless ad hoc sensor networks," *IEEE Trans. Signal Process.*, vol. 53, no. 11, pp. 4110–4124, Nov. 2005.

[102] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. McGraw-Hill, 2008.

[103] Y. Zou, J. Zhu, B. Zheng, and Y.-D. Yao, "An adaptive cooperation diversity scheme with best-relay selection in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 58, no. 10, pp. 5438–5445, Oct. 2010.

[104] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels*, 2nd ed. Hoboken, N.J: Wiley-Interscience, 2005.

[105] D. Torrieri and M. C. Valenti, "The outage probability of a finite Ad Hoc network in Nakagami fading," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3509–3518, Nov. 2012.

[106] H. Liu, S.-J. Yoo, and K. S. Kwak, "Opportunistic relaying for low-altitude UAV swarm secure communications with multiple eavesdroppers," *J. Commun. Netw.*, vol. 20, no. 5, pp. 496–508, Oct. 2018.

[107] A. Shaw and K. Mohseni, "A fluid dynamic based coordination of a wireless sensor network of unmanned aerial vehicles: 3-d simulation and wireless communication characterization," *IEEE Sensors J.*, vol. 11, no. 3, pp. 722–736, 2010.

[108] T. Shen and H. Ochiai, "A UAV-aided data collection for wireless powered sensor network over Rician fading channels," in *Proc. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2019.

[109] ——, "A UAV-enabled wireless powered sensor network based on NOMA and cooperative relaying with altitude optimization," *IEEE Open J. of Commun. Soc.*, vol. 2, pp. 21–34, 2021.

[110] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Mobile unmanned aerial vehicles (UAVs) for energy-efficient Internet of Things communications," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7574–7589, Nov. 2017.

[111] C. Zhan, Y. Zeng, and R. Zhang, "Energy-efficient data collection in UAV enabled wireless sensor network," *IEEE Wireless Commun. Lett.*, pp. 328–331, Jun. 2018.

[112] Y. Zeng and R. Zhang, "Energy-efficient UAV communication with trajectory optimization," *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3747–3760, Mar. 2017.

[113] V. V. Chetlur and H. S. Dhillon, "Downlink coverage analysis for a finite 3-D wireless network of unmanned aerial vehicles," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 4543–4558, Jul. 2017.

[114] Q. Wu, Y. Zeng, and R. Zhang, "Joint trajectory and communication design for multi-UAV enabled wireless networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 2109–2121, Mar. 2018.

[115] H. Ghazzai, B. M. Ghorbel, A. Kadri, M. J. Hossain, and H. Menouar, "Energy-efficient management of unmanned aerial vehicles for underlay cognitive radio systems," *IEEE Trans. Green Commun. Netw.*, vol. 1, no. 4, pp. 434–443, Dec. 2017.

[116] H. He, S. Zhang, Y. Zeng, and R. Zhang, "Joint altitude and beamwidth optimization for UAV-enabled multiuser communications," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 344–347, Feb. 2018.

[117] Q. Wu and R. Zhang, "Common throughput maximization in UAV-enabled OFDMA systems with delay consideration," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6614–6627, Dec. 2018.

[118] J. Lyu, Y. Zeng, and R. Zhang, "UAV-aided offloading for cellular hotspot," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3988–4001, Mar. 2018.

[119] Z. Yang, C. Pan, M. Shikh-Bahaei, W. Xu, M. Chen, M. Elkashlan, and A. Nallanathan, "Joint altitude, beamwidth, location and bandwidth optimization for UAV-enabled communications," *IEEE Commun. Lett.*, vol. 22, no. 8, Aug. 2018.

[120] M. Alzenad, A. El-Keyi, and H. Yanikomeroglu, "3-D placement of an unmanned aerial vehicle base station for maximum coverage of users with different QoS requirements," *IEEE Wireless Commun. Lett.*, vol. 7, no. 1, pp. 38–41, Feb. 2018.

[121] M. M. Azari, F. Rosas, K.-C. Chen, and S. Pollin, "Ultra reliable UAV communication using altitude and cooperation diversity," *IEEE Trans. Commun.*, vol. 66, no. 1, pp. 330–344, Jan. 2018.

[122] Y. Cai, Z. Wei, R. Li, D. W. K. Ng, and J. Yuan, "Joint trajectory and resource allocation design for energy-efficient secure UAV communication systems," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4536–4553, Jul. 2020.

[123] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[124] S. Bi, Y. Zeng, and R. Zhang, "Wireless powered communication networks: An overview," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 10–18, May 2016.

[125] S. Gautam, E. Lagunas, S. Chatzinotas, and B. Ottersten, "Relay selection and resource allocation for SWIPT in multi-user OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2493–2508, May 2019.

[126] Z. Ali, G. A. S. Sidhu, S. Zhang, L. Xing, and F. Gao, "Achieving green transmission with energy harvesting based cooperative communication," *IEEE Access*, vol. 6, pp. 27 507–27 517, May 2018.

[127] Y. Liu, Z. Qin, M. Elkashlan, Z. Ding, A. Nallanathan, and L. Hanzo, "Nonorthogonal multiple access for 5G and beyond," *Proc. IEEE*, vol. 105, no. 12, pp. 2347–2381, Dec. 2017.

[128] S. M. R. Islam, N. Avazov, O. A. Dobre, and K. S. Kwak, "Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 721–742, 2017.

[129] Z. Ding, P. Fan, and H. V. Poor, "Impact of user pairing on 5G nonorthogonal multiple-access downlink transmissions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6010–6023, Aug. 2016.

[130] Z. Wei, L. Yang, D. W. K. Ng, J. Yuan, and L. Hanzo, "On the performance gain of NOMA over OMA in uplink communication systems," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 536–568, Jan. 2020.

[131] Y. Liu, Z. Qin, Y. Cai, Y. Gao, G. Y. Li, and A. Nallanathan, "UAV communications based on non-orthogonal multiple access," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 52–57, Feb. 2019.

[132] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "UAV-enabled communication using NOMA," *IEEE Trans. Commun.*, vol. 67, no. 7, pp. 5126–5138, Jul. 2019.

[133] A. Farajzadeh, O. Ercetin, and H. Yanikomeroglu, "UAV data collection over NOMA backscatter networks: UAV altitude and trajectory optimization," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, May 2019, pp. 1–7.

[134] R. Duan, J. Wang, C. Jiang, H. Yao, Y. Ren, and Y. Qian, "Resource allocation for multi-UAV aided IoT NOMA uplink transmission systems," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 7025–7037, Aug. 2019.

[135] W. Mei and R. Zhang, "Uplink cooperative NOMA for cellular-connected UAV," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 644–656, Jun. 2019.

[136] X. Pang, G. Gui, N. Zhao, W. Zhang, Y. Chen, Z. Ding, and F. Adachi, "Uplink precoding optimization for NOMA cellular-connected UAV networks," *IEEE Trans. Commun.*, vol. 68, no. 2, pp. 1271–1283, Feb. 2020.

[137] T. Z. H. Ernest, A. S. Madhukumar, R. P. Sirigina, and A. K. Krishna, "NOMA-aided UAV communications over correlated Rician shadowed fading channels," *IEEE Trans. Signal Process.*, vol. 68, pp. 3103–3116, 2020.

[138] Y. Sun, D. Xu, D. W. K. Ng, L. Dai, and R. Schober, "Optimal 3D-trajectory design and resource allocation for solar-powered UAV communication systems," *IEEE Trans. Commun.*, vol. 67, no. 6, pp. 4281–4298, Feb. 2019.

[139] D. Xu, Y. Sun, D. W. K. Ng, and R. Schober, "Multiuser MISO UAV communications in uncertain environments with no-fly zones: Robust trajectory and resource allocation design," *IEEE Trans. Commun.*, vol. 68, no. 5, pp. 3153–3172, May 2020.

[140] Y. Zeng, J. Xu, and R. Zhang, "Energy minimization for wireless communication with rotary-wing UAV," *IEEE Trans. Commun.*, vol. 18, no. 4, pp. 2329–2345, Apr. 2019.

[141] A. F. Molisch, *Wireless Communications*. IEEE Press, 2006.

[142] Iskandar and S. Shimamoto, "Channel characterization and performance evaluation of mobile communication employing stratospheric platform," *IEICE Trans. Commun.*, vol. E89-B, no. 3, pp. 937–944, Mar. 2006.

[143] H. Ochiai, P. Mitran, and V. Tarokh, "Variable-rate two-phase collaborative communication protocols for wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4299–4313, Sep. 2006.

[144] J. A. Nelder and R. Mead, "A simplex method for function minimization," *The Computer Journal*, vol. 7, no. 4, pp. 308–313, 1965.

[145] G. K. Karagiannidis, N. C. Sagias, and P. T. Mathiopoulos, "$N*$ Nakagami: A novel stochastic model for cascaded fading channels," *IEEE Trans. Commun.*, vol. 55, no. 8, pp. 1453–1458, Aug. 2007.

[146] Y. A. Brychkov, O. I. Marichev, and N. V. Savischenko, *Handbook of Mellin Transforms*. CRC Press, Oct. 2018.

[147] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless charging technologies: Fundamentals, standards, and network applications," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1413–1452, 2016.

[148] P. He, L. Zhao, S. Zhou, and Z. Niu, "Water-filling: A geometric approach and its application to solve generalized radio resource allocation problems," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3637–3647, Jul. 2013.

[149] J. Hu and N. Beaulieu, "Accurate closed-form approximations to Ricean sum distributions and densities," *IEEE Commun. Lett.*, vol. 9, no. 2, pp. 133–135, Feb. 2005.

[150] A. P. Prudnikov, J. A. Brychkov, and O. I. Marichev, *Integrals and Series*. Gordon and Breach, 1986.

Publications

Journals

- T. Shen and H. Ochiai, “A UAV-Enabled Wireless Powered Sensor Network Based on NOMA and Cooperative Relaying With Altitude Optimization,” *IEEE Open Journal of the Communication Society*, vol. 2, pp. 21-34, 2021.

Conference Papers

- T. Shen and H. Ochiai, “A UAV-Aided Selective Relaying with Cooperative Jammers for Secure Wireless Networks over Rician Fading Channels,” *IEEE Vehicular Technology Conference Fall (VTC-Fall 2019)*, Honolulu, HI, USA, Sep. 2019.

- T. Shen and H. Ochiai, “A UAV-Aided Data Collection for Wireless Powered Sensor Network over Rician Fading Channels,” *IEEE Consumer Communications & Networking Conference (CCNC 2019)*, Las Vegas, NV, USA, Jan. 2019.