JYU DISSERTATIONS 861

Xinying Kilpi-Chen

Secure Transmission Strategies in UAV-Assisted Wireless Networks

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION
TECHNOLOGY

JYU DISSERTATIONS 861

Xinying Kilpi-Chen

Secure Transmission Strategies in UAV-Assisted Wireless Networks

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksen auditoriossa 3
joulukuun 16. päivänä 2024 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 3, on December 16, 2024 at 12 o'clock noon.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2024

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

ISBN 978-952-86-0443-3 (PDF)
URN:ISBN:978-952-86-0443-3
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-952-86-0443-3

To the stronger me
and
my family.

ABSTRACT

Kilpi-Chen, Xinying
Secure Transmission Strategies in UAV-Assisted Wireless Networks
Jyväskylä: University of Jyväskylä, 2024, 62 p. (+included articles)
(JYU Dissertations
ISSN 2489-9003; 861)
ISBN 978-952-86-0443-3 (PDF)

As the fifth/sixth generation (5G/6G) wireless transmission has become increasingly ubiquitous and inevitable, ensuring information security becomes more crucial than ever. Therefore, this dissertation focuses on achieving transmission security in unmanned aerial vehicle (UAV)-assisted wireless networks via physical layer security (PLS) and covert communication techniques while also enhancing energy efficiency, transmission performance, and secrecy throughput. First, an energy-efficient UAV data collection and transmission scheme is proposed to prevent eavesdropping. This research aims to maximize the energy efficiency of UAV data collection and secure performance via optimizing the trajectory, flight duration, user scheduling, UAV transmit power, and blocklength simultaneously. Simulation results prove that the proposed scheme can enhance energy efficiency and guarantee information security. Next, a secure intelligent reflecting surface (IRS)-on-UAV network is designed and optimized to defend against an eavesdropper. The beamforming vectors of confidential signals and artificial noise signals, as well as the phase-shift matrix and location of IRS, are jointly optimized to maximize the secrecy rate while constraining the eavesdropping rate within its limit. Simulation results validate the effectiveness and security of the proposed approach. Finally, PLS is introduced into covert communication to increase secrecy throughput. The purpose of this research is to provide more secure data transmission in covert communication using PLS technology to avoid eavesdropping even if Alice fails and Willie detects her. Simulation results confirm the significant improvements in security performance.

Keywords: Beamforming, covert communication, joint optimization, physical layer security, unmanned aerial vehicle

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Kilpi-Chen, Xinying
Turvalliset tiedonsiirtostrategiat UAV-avusteisissa langattomissa verkoissa
Jyväskylä: University of Jyväskylä, 2024, 62 s. (+artikkelit)
(JYU Dissertations
ISSN 2489-9003; 861)
ISBN 978-952-86-0443-3 (PDF)

Viidennen/kuudennen sukupolven (5G/6G) langattomasta lähetyksestä on tullut yhä yleisempää ja väistämättömämpää, joten tietoturvan varmistamisesta tulee entistä tärkeämpää. Tästä syystä tämä väitöskirja keskittyy tiedonsiirtovarmuuden saavuttamiseen miehittämättömissä ilma-alusten (unmanned aerial vehicle, UAV) tukemissa langattomissa verkoissa fyysisen kerroksen turvallisuuden (physical layer security, PLS) ja suojattujen kommunikaatiotekniikoiden avulla, samalla kun parannetaan energiatehokkuutta, lähetyksen suorituskykyä ja salassapitoa. Ensinnäkin esitetään energiatehokasta UAV-tiedonkeruu- ja -siirtojärjestelmää salakuuntelun estämiseksi. Tässä tutkimuksessa pyritään maksimoimaan UAV-tiedonkeruun energiatehokkuus ja turvattu suorituskyky optimoimalla lentorata, lennon kesto, käyttäjämäärittely, UAV-lähetysteho ja eston pituus samanaikaisesti. Simulaatiotulokset osoittavat, että ehdotettu järjestelmä voi parantaa energiatehokkuutta ja varmistaa tietoturvan. Toisekseen suojatun älykkään heijastavan pinnan (intelligent reflecting surface) omaava IRS-UAV-verkko on suunniteltu ja optimoitu suojaamaan salakuuntelulta. Luottamuksellisten signaalien ja keinotekoisten kohinasignaalien keilanmuodostusvektorit sekä IRS:n vaihesiirtomatriisi ja sijainti on optimoitu yhdessä maksimoimaan salausastetta ja samalla rajoittamaan salakuuntelua sen rajoissa. Simulaatiotulokset vahvistavat ehdotetun lähestymistavan tehokkuuden ja turvallisuuden. Lopuksi PLS otetaan käyttöön suojatussa viestinnässä salassapitokyvyn lisäämiseksi. Tämän tutkimuksen tarkoituksena on tarjota suojattu tiedonsiirto salaisessa viestinnässä PLS-tekniikoiden avulla, vaikka Alice epäonnistuisi ja Willie havaitsisi hänet. Simulaatiotulokset vahvistavat merkittävät parannukset tietoturvassa.

Avainsanat: Aaltoryhmän muodostus, suojattu viestintä, yhteisoptimointi, fyysisen kerroksen turvallisuus, miehittämätön ilma-alus

Author
Xinying Kilpi-Chen
Faculty of Information Technology
University of Jyväskylä
Finland

Supervisors
Professor Timo Hämäläinen
Faculty of Information Technology
University of Jyväskylä
Finland

Professor Zheng Chang
Faculty of Information Technology
University of Jyväskylä
Finland

Professor Ilkka Pölönen
Faculty of Information Technology
University of Jyväskylä
Finland

Reviewers
Professor Yan Zhang
Department of Informatics
University of Oslo
Norway

Associate Professor Sheng Zhou
Department of Electronic Engineering
Tsinghua University
China

Opponent
Associate Professor Hirley Alves
Faculty of Information Technology and Electrical Engineering
University of Oulu
Finland

ACKNOWLEDGEMENTS

It’s been a truly meaningful and enjoyable journey over these four and half years of my Ph.D. life. Remarkably, I completed my doctoral study, found my Mr.right, and even welcomed our new little family member. I am deeply grateful for all of the people helped me settle into this new country, overcome challenges in research, and provided warm support to guide me through dark times.

I would like to express my grateful and respect to my first supervisor Prof. Tapani Ristaniemi. Though we never had the chance to meet in person, none of this would have been possible without his decision to accept me in the first place. I am equally indebted to Prof. Timo Hämäläinen, who later became my first supervisor and guided me toward becoming a doctor. Timo’s mentorship provided me with the freedom to explore my research interests, and his enthusiasm, passion, and promptness in work were truly inspiring. Our communication was always smooth and timely. Tragically, life took an unexpected turn. Though we had planned to complete my studies by the end of this year, he is no longer here to witness it. I was deeply shocked and heartbroken by his passing and had hoped he would be present at my dissertation defense, hammer in hand. Unfortunately, reality seldom aligns with our wishes.

I owe profound gratitude to Prof. Zheng Chang, whose guidance illuminated my research journey during its darkest moments. True to his word, he took care of my academic progress, providing sharp, to-the-point suggestions and invaluable guidance. When I struggled to respond to reviewers’ comments, his eye-opening advice brought profound clarity and insight. I deeply admire his wisdom and sharp mind, making our discussions efficient and productive. He could quickly identify the weak points and offer precise suggestions for improvement. Moreover, I will always remember the kind words of my new supervisor, Prof. Ilkka Pölönen. When I inquired about course credits, he replied, “if you say that you have participated 12 times, I will believe you,” offering trust and support when I needed it most after Timo’s passing. I am deeply thankful for Ilkka’s confidence in me and his willingness to supervise the final stages of my doctoral studies, enabling me to complete my dissertation as planned.

I would like to express my heartfelt gratitude to Dr. Xiaowei Pang. You have been a radiant light throughout my doctoral journey, bringing me hope and joy. I would also like to thank Yujie Wu and Chao Wang, along with Xiaowei, for their companionship and the daily joy they brought into my life. I am sincerely grateful to Jiaqi Zheng, Yalin Sun, Liting Song, Jaakko Varis, Xin Zuo, Jing Liu, and Mingan Luan for their support in helping me start up, settle down, and thrive. I extend my deepest gratitude and respect to Riitta, who has been with me since the beginning of this journey and has become like family to me. She has shown me that anything is possible in life and that it is never too late to start. As long as you have the will, you can achieve it.

A special thanks goes to my family. My dearest husband Santeri Kilpi-Chen, my pebble solid like a rock and comfort like silk, has supported me with countless warm hug and unwavering love to ease every thorn along this way. My beloved son Olavi Xi Kilpi-Chen, has never threw hard time on mama, neither pregnant sickness nor whole night after birth crying. I would like to express grateful to my mom Guiqin Zhang who support and trust me like always, and my brother Xinyu Chen who traveled half of the globe to help me travel and relax with his little nephew. I would also like to thank to my parents-in-law Irene and Petteri Kilpi, who helped to take care of Olavi during summer, have made this dissertation happen earlier than I could have done it. I am deeply grateful to my cousin, Hong Chen, for taking care of my parents, which has allowed me to focus more fully on my studies.

Jyväskylä 20.11.2024
Xinying Kilpi-Chen

LIST OF ACRONYMS

5G	The Fifth Generation
6G	The Sixth Generation
AI	Artificial Intelligence
AN	Artificial Noise
CSI	Channel State Information
FA	False Alarm
IoT	Internet of Things
IRS	Intelligent Reflecting Surface
LoS	Line-of-Sight
MD	Miss Detection
MIMO	Multiple-Input and Multiple-Output
MRT	Maximum Ratio Transmission
NLoS	Non-Line-of-Sight
NOMA	Non-Orthogonal Multiple Access
PA	Power Allocation
PLS	Physical Layer Security
PSD	Power Spectral Density
QoS	Quality of Service
SCA	Successive Convex Approximation
SDR	Semidefinite Relaxation
SINR	Signal-to-Interference-Plus-Noise Ratio
SRL	Square Root Law
THz	Terahertz
UAV	Unmanned Aerial Vehicle
URLLC	Ultra-Reliable and Low-Latency Communication
V2X	Vehicle-to-Everything

LIST OF FIGURES

LIST OF TABLES

CONTENTS

LIST OF INCLUDED ARTICLES

I Xinying Chen, Nan Zhao, Zheng Chang, Timo Hämäläinen, and Xianbin Wang. UAV-aided secure short-packet data collection and transmission. *IEEE Transactions on Communications*, 71(4), 2475–2486, https://www.doi.org/10.1109/TCOMM.2023.3244954, 2023.

II Xinying Chen, Zheng Chang, and Timo Hämäläinen. Secure transmission for IRS-on-UAV-assisted wireless networks. *IEEE Transactions on Communications*, submitted, 2024.

III Xinying Chen, Zheng Chang, Nan Zhao, and Timo Hämäläinen. IRS-based secure UAV-assisted transmission with location and phase shifting optimization. *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1672–1677, https://www.doi.org/10.1109/ICCWorkshops57953.2023.10283558, 2023.

IV Xinying Chen, Zheng Chang, and Timo Hämäläinen. Enhancing covert secrecy rate in a zero-forcing UAV jammer-assisted covert communication. *IEEE Wireless Communications Letters*, accepted for publication, 2024.

V Xinying Chen, Zheng Chang, and Timo Hämäläinen. Achieving improved security in UAV-assisted covert communication networks. *2024 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pp. 323–328, https://doi.org/10.1109/ICCCWorkshops62562.2024.10693776, 2024.

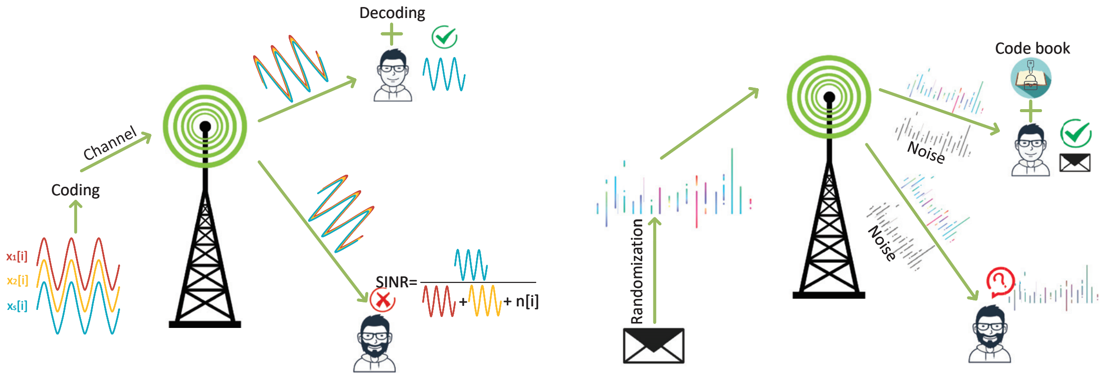
1 INTRODUCTION

With the applications of the fifth generation (5G) wireless communication into commercial service, wireless data transmission has advanced to speeds of up to 1 Gbps, millisecond-level delay, support for high-speed mobility up to 500 km/h, as well as ultra large capacity of over 1 M/km^2 (ITU 2017; Shafi et al. 2017). Meanwhile, it also fueled the development of auto-drive, vehicle-to-everything (V2X), and telemedicine, which, on the other hand, are driving the evolution of the next generation wireless networks, i.e., the sixth generation (6G). The vision of 6G includes intelligent, deep, holographic, and ubiquitous, which cannot be achieved merely through the terrestrial communication networks (W. Jiang et al. 2021). Therefore, the integration of non-terrestrial networks, including low Earth orbit satellites and unmanned aerial vehicles, will play an important role in the forthcoming wireless communications.

1.1 Research Background and Motivation

The unmanned aerial vehicle (UAV) has been studied extensively due to its high mobility and easy deployment, especially in fulfilling the air-space-ground-sea full coverage in 6G (Geraci et al. 2022). The integration of UAVs into wireless communications can improve communication quality via establishing line-of-sight (LoS) channel connections and achieve better transmission performance. However, the broadcast characteristic of LoS links can meanwhile result in information leakage and enable malicious eavesdroppers to obtain confidential information from the transmitters (Papa et al. 2024). This risk will become more pronounced in the upcoming 6G networks, where the Internet of Things (IoT) contains more confidential personal or location information. Therefore, ensuring secure transmission is a critical issue required to be addressed in 6G (Aggarwal, Kumar, and Tanwar 2021).

Information security has always been crucial and its importance has surged with the growing prevalence of wireless communications in daily life, ranging from biological data or financial accounts to industrial data or national security information (Bloch et al. 2021). Due to the widespread accessibility of wireless communication, its transmission security has become a critical study area and received significant research attention, where the prevalent solutions are cryptography, physical layer security (PLS), and covert communication (X. Chen, An, et al. 2023). The cryptography encrypts data with keys before sending to provide protection, which requires the corresponding decryption key to interpret the ciphertext (Ke et al. 2020). However, the ciphertext is still vulnerable and can be cracked by brute force. Therefore, this thesis focuses on providing secure transmission through PLS and covert communication methods in UAV-assisted networks. The conceptual system models of PLS and covert communication are illustrated in Figure 1 (X. Wang et al. 2024).



(a) PLS

(b) Covert communication

FIGURE 1 System model of PLS and covert communications

As shown in Figure 1 (a), PLS leverages the diversity, heterogeneity, and time-variability of channel links, combined with channel coding and signal processing to achieve secure transmission for legitimate users. PLS prevents malicious eavesdroppers from intercepting the transmission by reducing their received signal-to-interference-plus-noise ratio (SINR) lower than the decoding threshold (Kihero et al. 2024). In addition, PLS can also improve the communication performance as well as guarantee the security by introducing artificial noise (AN) or applying beamforming, i.e., enhancing the channel capacity. On the other hand, referring to Figure 1 (b), covert communication randomizes confidential signals and embeds them into environmental noise to avoid being noticed by wardens, where the malicious wardens monitor and compare the received signal power with the preset power detection threshold to decide whether the transmitter is transmitting or not (Z. Liu, J. Liu, et al. 2018). In covert communications, the randomization methodologies for legitimate users include transmit power randomization, AN randomization, location randomization, and Gaussian signaling. The ultimate objective of covert communication is to maximize transmission performance while guaranteeing stealth.

Integrating UAV into wireless communication can leverage its mobility, fast deployment, and cost-efficiency to achieve higher quality of service (QoS), enhanced network coverage, and flexible configuration. However, the inevitable security hazard should also be taken into consideration and alleviated (H. Wang et al. 2018). A significant amount of research work has focused on secure transmission in UAV-assisted wireless communication networks, where the PLS and covert communication methods have been proven to be effective (X. Chen, An, et al. 2023; Khan et al. 2022). Typical PLS-related work applies power allocation (PA), beamforming, AN, or intelligent reflecting surface (IRS) to obtain a higher security rate while keeping the eavesdropping rate below the decoding threshold. Recently, covert communication has gained significant attention for its ability to enhance the security in wireless networks by concealing signals in noise. Owing to the "no detection, no decoding" policy at wardens, covert communication is no doubt robustly secure protection for wireless signals. Additionally, the cooperation of PLS and covert communication techniques can achieve more comprehensive security.

Inspired by the effectiveness of PLS and covert communication in obtaining security for wireless networks, this thesis proposes several novel schemes to ensure secure transmission for UAV-related networks via both PLS and covert communication. The objective of this thesis is to provide secure transmission solutions for mobile UAV-assisted networks across various scenarios, contributing to the development of wireless secure transmission solutions via PLS and covert communication techniques.

1.2 Research Aims

This thesis focuses on enhancing transmission security in UAV-assisted wireless networks through PLS as well as covert communication technologies. The application of UAVs can provide flexible network configuration, high mobility, and extensive coverage for wireless communications. UAVs can extend wireless communication from terrestrial coverage to air-ground communication, thereby improving user transmission performance thanks to its high probability of LoS links. However, these advantages also heightens the threat to user information security by increasing vulnerability to eavesdropping and detection. Therefore, the secure transmission in UAV-related wireless networks is of crucial importance. Unlike upper-layer encryption methods, PLS offers benefits such as lightweight implementation, easy scalability, and resistance to cracking (J. Wang et al. 2022). On the other hand, covert communication fundamentally conceals the transmission (X. Jiang et al. 2021).

Considerable amount of research has been conducted on PLS-based wireless secure transmission with various techniques employed to enhance the security. The security improving techniques include PA, multiple antennas, AN, and beamforming/precoding (Kihero et al. 2024). Nevertheless, most existing studies focus on traditional communication networks without accounting for the importance of short-packet transmissions, which is of extreme importance in the IoT of 5G/6G (Feng and H.-M. Wang 2021). Additionally, IRS has gained tremendous interests due to its flexibility manipulation of channel state information (CSI). However, utilizing IRS to improve UAV-related network security is relatively overlooked. Consequently, in order to tackle the security problems of finite blocklength and IRS-based solutions in PLS, the following issues are investigated:

- How to improve the transmission performance for legitimate users while ensuring the security?
- How to improve the energy efficiency in a UAV-assisted energy constrained network?
- How to characterize the secure metrics and ensure confidentiality in time-intolerant UAV networks?
- How to utilize the channel reconfiguration characteristic of IRS to provide secure transmission?

Indeed PLS can provide secure wireless transmission by reducing the received SINR of legitimate user's signal at eavesdroppers. This can be achieved by either lowering the received power of legitimate signal or increasing interference at the eavesdroppers. However, the comprehensive protection cannot be assured as the improvement of decoding algorithm. The recent emerging covert communication can prevent wardens from detecting the existence of legitimate transmission, which leads to a more comprehensive stealth. In this way, the warden will not attempt to decode confidential information as he remains unaware of the transmission (An et al. 2024). Thus, to achieve a more comprehensive security, covert communication can be applied alongside PLS. And the following questions should be taken into account:

- How can PLS and covert communication be integrated, and how can their security metrics be quantified?
- How can randomness be introduced in UAV-related LoS channels?
- How can the mobility of UAV be leveraged in covert communication scenarios?

The principle goal of this research is to propose secure transmission schemes for UAV-related networks via PLS and covert communication methods under specific scenarios. The secure transmission schemes proposed in this thesis aim to address the security problem of time-intolerant UAV-network, utilize IRS to enhance secure wireless transmission, and, for the first time, integrate PLS with covert communication for enhanced security.

1.3 Contributions

To achieve the secure transmission objectives outlined in Section 1.2, this dissertation investigates several key scenarios.

First, a secure UAV-assisted finite blocklength data collection and transmission scheme is proposed in Article I to address and alleviate the risks associated with LoS channels and long-distance communications. The energy efficiency problem is tackled via joint UAV trajectory and user schedule optimization. Additionally, the proposed scheme utilizes PA to reduce the eavesdropping rate and guarantee information security.

Next, multi-antenna and IRS are leveraged to accomplish transmission security and improve legitimate user performance in Articles II and III. The reconfiguration of IRS and the mobility of UAV are exploited in Article III to maximize the secrecy rate while maintaining the eavesdropping rate lower than the required threshold. Additionally, the above-mentioned scheme is extended in Article II, which exploits the advantages of AN and beamforming to further boost the secure performance for legitimate users.

Last, inspired by the effectiveness of covert communication and PLS, an novel enhanced secure covert communication scheme is proposed in Articles IV and V, where covert communication and PLS techniques are initially integrated to provide a more comprehensive protection. Traditionally, PLS and covert communication target different phases to prevent malicious eavesdropping or detection. The secrecy covert rate is first introduced to quantify the security performance after combining the two techniques. Gaussian signaling and zero-forcing techniques are exploited to introduce randomness at the warden while eliminating interference at the legitimate receiver.

1.4 Dissertation Structure

This dissertation aims to enhance the secure transmission in UAV-assisted wireless networks via PLS and covert communication methods. It is organized into five chapters as follows:

Chapter 1: This chapter introduces the background and motivations for the research conducted in this thesis. Research problems are discussed and summarized, followed by the contributions of this research. Finally, the structure of this thesis is outlined.

Chapter 2: This chapter discusses the relevant technologies and theoretical knowledge critical to this dissertation. It begins with explaining the preliminary communication principles of UAV communications, followed by an exploration of secure transmission technologies and an introduction of the interference management techniques.

Chapter 3: The related state-of-the-art research on wireless UAV-assisted secure transmission is comprehensively reviewed and discussed, where the limitations and shortcomings are addressed. Additionally, a detailed review concerning wireless secure communication is demonstrated, including both PLS and covert communications. IRS-related work is also reviewed and compared.

Chapter 4: The proposed UAV-assisted secure transmission schemes are illustrated, and the effectiveness of the proposed schemes is evaluated. Research results are discussed under three specific scenarios, i.e., energy-efficient secure UAV data collection and transmission, multi-antenna IRS-on-UAV secure transmission, and joint secure transmission via PLS and covert communication.

Chapter 5: Innovative contributions of this research are summarized, and the potential future research directions are discussed.

2 RELATED PRINCIPLE TECHNOLOGIES

This chapter briefly outlines the key concepts and principles relevant to the dissertation. First, the fundamental communication theory in UAV-assisted networks is explained. Then, The secure transmission techniques are categorized into PLS and covert communication, providing a clear narrative on both of them. Following this, the fundamentals of interference management are explained. Last, the main points of this chapter is concluded.

2.1 UAV Wireless Communications

Benefiting from the characteristics of high mobility, low energy cost, and easy deployment, UAV plays important roles in both current and next-generation wireless communications (Y. Bai et al. 2023). In addition, due to the advantages of lightweight structure and multifunctionality, UAVs can be utilized for coverage extending strategy by serving as a small aerial platform to temporarily enlarge user access capacity in high-density communication networks. Furthermore, UAVs can also be controlled remotely as a terminal user to collect data efficiently.

To sum up, the advantages of UAV-assisted wireless communication can be listed as follows.

LoS Links: UAV can adjust its hovering location or trajectory to establish LoS channel links between itself and other users, which can reduce the path loss and improve transmission performance.

High Mobility: Owing to its small size, UAVs can be remotely controlled for rapid deployment in emergency communications. The flexibility and small volume enable UAVs to adjust swiftly according to emergency situations.

Low Cost: The characteristics of mobility and easy configuration allow UAVs highly adaptable to various communication scenarios. In addition, the low cost and flexibility also allow for the construction of UAV swarm system rapidly and with network setup cost-effective.

Compared with other communication systems, the UAV-related communication offers significant advantage of establishing LoS channel links, which can enhance the overall communication performance. Particularly, the links in UAV-related communication can be categorized into UAV-to-UAV links and UAV-to-terrestrial user links.

UAV-to-UAV Links

The communication links between UAVs are primarily established as LoS links (Burhanuddin et al. 2022). Nevertheless, complex communication scenarios may involve multiple propagation paths, such as direct(LoS), reflected, and scattered paths. The corresponding non-line-of-sight (NLoS) components remaining are extremely small and negligible compared with the LoS components. Therefore, the channel coefficient h_L for UAV-to-UAV links can be modeled as LoS channel, which can be expressed as

$$h_L = \sqrt{\frac{\rho_0}{d_{UU}^{\alpha_U}}} g_L, \tag{1}$$

where ρ_0 represents the reference power gain at 1m, d_{UU} represents the distance between two UAVs, α_U is the large-scale path loss exponent between UAVs. g_L is the complex LoS component, which follows $|g_L| = 1$.

UAV-to-Terrestrial User Links

Different from the UAV-to-UAV communication links, the channel links of UAV-to-terrestrial users subject to more complex environmental factors, which is also highly related to the altitude of UAVs (Y. Liu, Huang, et al. 2024). Without loss of generality, research work assumes these channel links follow a large-scale path loss and a small-scale Rician fading, which can be described as

$$h_R = \frac{\rho_0}{d_{UT}^{\alpha_T}} \left(\frac{K_0}{1+K_0} g_L + \frac{1}{1+K_0} g_N \right), \tag{2}$$

where d_{UT} and α_T represent the distance and the large-scale path loss exponent between the UAV and the terrestrial user, respectively. K_0 is the Rician factor related to surrounding environment. Similar to (1), g_L represents the LoS component. g_N is the NLoS component, following unit complex Gaussian distribution $g_N \sim \mathcal{CN}(0, 1)$. In some cases, the channel links within UAV-to-terrestrial users consist mostly with LoS channels, where the channel coefficients of UAV-to-terrestrial users follow (1).

In summary, the CSI in UAV-related networks typically follows either LoS or Rician fading. Although legitimate users can obtain better performance benefiting from air-to-ground channel links, it can also be leveraged by malicious users, such as eavesdroppers and detecting wardens. The primary approaches of achieving secure transmission in wireless networks involve cryptography, PLS and covert communications. This dissertation primarily focuses on providing secure transmission against eavesdropping through PLS and detection via covert communications.

2.2 Principles of Secure Transmission

Both PLS and covert communications leverage the inherent characteristics of physical layer to ensure secure transmission. On the one hand, PLS focuses on reducing the SINR at eavesdroppers or improving the secrecy rate at legitimate receivers via exploiting the differences of CSI between legitimate users and eavesdroppers. On the other hand, covert communication aims to achieve the non-existence of transmitter at the wardens by embedding the transmission into environmental noise.

2.2.1 Physical Layer Security

Unlike the complicated encryption schemes, PLS exploits the physical random characteristics of channel links, i.e., time variability, reciprocity, and disparity, combined with coding and signal processing techniques to realize secure transmission. Owing to its lightweight, compatible, and resistance to crack, PLS has gained significant interest in wireless secure transmission. The primary concept of PLS is to interfere eavesdropper as much as possible while guaranteeing the performance of legitimate users, and thereby achieve transmission security (Cao, Zhao, et al. 2020).

We introduce the principles of PLS briefly via an example, as shown in Figure 2. A transmitter Tx communicates with a target receiver Rx securely with the assistance of a jammer J to avoid being eavesdropped by an eavesdropper E. The

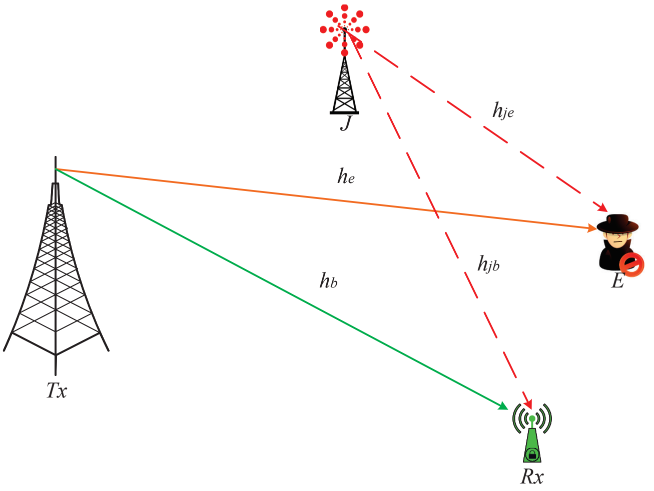


FIGURE 2 Jamming-assisted PLS transmission system

transmit power of transmitter is P_a, and the jamming power of J is P_j. The channel coefficients between the transmitter and receiver, transmitter and eavesdropper, jammer and receiver, and jammer and eavesdropper can be denoted as h_b, h_e, h_{jb}, h_{je}, respectively. The secrecy rate between the legitimate transmitter and receiver can be expressed as

$$R_s = \left[\log_2\left(\frac{P_a|h_b|^2}{P_j|h_{jb}|^2+\sigma_b^2}\right) - \log_2\left(\frac{P_a|h_e|^2}{P_j|h_{je}|^2+\sigma_e^2}\right)\right]^+, \tag{3}$$

where σ_b^2 and σ_e^2 represent the noise variance at the legitimate receiver and the eavesdropper, respectively. It is defined that $[x]^+ = \max(0, x)$. From (3), we can see that the jamming signals not only interfere with the SINR at the eavesdropper, but also influence the performance of the legitimate receiver. Therefore, the jammer should be properly designed and optimized in practical networks. For example, the jamming location can be strategically optimized to pose worse jamming channel conditions at legitimate receiver than the eavesdropper, which can result in severe interference at eavesdropper and lead to larger secrecy rate.

2.2.2 Covert Communications

Since the milestone research conducted by Bash, Goeckel, and Towsley (2013) was published, covert communication has gained significant interest. This technique conceals the transmitted signals to avoid being detected by wardens, where the wardens cannot detect the existence of transmission then will not attempt to decode the secure information, and thus leads to the security of wireless communications.

The typical research process in covert communications can be divided into two steps, which are the covert transmission by Alice and the detection by Willie. In one aspect, Alice transmits stealthy signals $x[i]$ with probability π_1 to Bob, aiming to avoid being detected by Willie while maintaining transmission performance. Alice remains silent in the remaining π_0 probability time. It is commonly assumed $\pi_1 = \pi_0 = 0.5$ in practical research to maximize the uncertainty at Willie and reduce his correct detection probability for Alice's transmission (Bash, Goeckel, and Towsley 2013). In another aspect, Willie enhances his correct detecting probability of Alice's transmission via properly adjusting his detection parameters, such as power detection threshold and his location. Assume the received environmental noise at Willie is $n[i]$. There are two possible status of Alice's transmission, which leads to two corresponding cases of the received signals at Willie

$$\begin{aligned} &\mathcal{H}_1 : y_w[i] = n[i], \\ &\mathcal{H}_0 : y_w[i] = x[i] + n[i], \end{aligned} \tag{4}$$

where $\mathcal{H}_1$ represents that Alice transmits to Bob, and $\mathcal{H}_0$ represents that Alice keeps silent. In covert communication, Willie compares his received signal power with the preset power detection threshold ξ to determine whether Alice is transmitting $\mathcal{D}_1$ or keeping silent $\mathcal{D}_1$. The decision rule can be described as follows

$$\bar{P}_w = \frac{1}{n}\sum_{i=1}^{n} |y_w[i]|^2 \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \xi, \tag{5}$$

where n is the transmission channel links utilized by Alice. According to the decision rule in (5), Willie makes his decision based on the averaged received power $\bar{P}_w$. Willie determines that Alice is transmitting when $\bar{P}_w \geq \xi$, and concludes Alice keeps silent when $\bar{P}_w \leq \xi$. From the decision rule, it is obvious that the power detection threshold ξ has significant impact on Willie's correct detection probability. Figure 3 summarizes the process of decision making in covert communications.

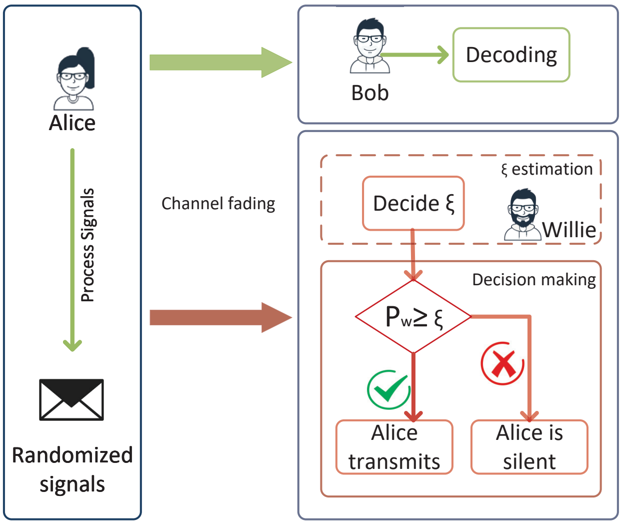


FIGURE 3 Decision process for covert communications

There are two types of mistakes that Willie may make during his detection, namely false alarm (FA) and miss detection (MD). The probability that Willie makes FA mistake can be described as $\alpha = \mathbb{P}\{\mathcal{D}_1|\mathcal{H}_0\}$, which represents the likelihood that Willie mistakenly believes Alice is transmitting while she is actually silent. Conversely, the MD probability that Willie may make can be described as $\beta = \mathbb{P}\{\mathcal{D}_0|\mathcal{H}_1\}$, which indicates that Alice is transmitting but Willie assumes she is silent. The objective of Willie is to minimize his error detection probability $\alpha + \beta$ by optimizing his power detection threshold ξ. Based on the constructive conclusion given by Bash, Goeckel, and Towsley (2013), the error detection probability of Willie satisfies

$$\alpha + \beta = 1 - \mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1) \geq 1 - \sqrt{\frac{1}{2}\mathcal{D}(\mathbb{P}_0||\mathbb{P}_1)}, \tag{6}$$

where $\mathbb{P}_0$ and $\mathbb{P}_1$ are the probability density functions of the received signals at Willie when Alice is silent or transmitting, respectively. In addition, $\mathcal{V}_T(\mathbb{P}_0, \mathbb{P}_1)$ is the total variation distance between $\mathbb{P}_0$ and $\mathbb{P}_1$, and $\mathcal{D}(\mathbb{P}_0||\mathbb{P}_1)$ denotes the relative entropy, also known as the Kullback-Leibler divergence, between $\mathbb{P}_0$ and $\mathbb{P}_1$.

By optimizing Willie's power detection threshold ξ, the minimum error detection probability in (6) can be achieved. Further combining with the decision rule in (5), the optimal ξ can be derived through the following function.

$$\frac{\mathbb{P}_1}{\mathbb{P}_0} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} 1. \tag{7}$$

Consequently, Alice needs to introduce sufficient uncertainty at Willie to ensure that even with his optimal detection strategy, the error detection probability of Willie remains no less than $1 - \epsilon$, i.e., $\alpha + \beta \geq 1 - \epsilon$. In the existing research, the common methods of introducing uncertainty to Willie include utilizing small-scale fading, randomizing transmit power (of Alice, jammer, and relay), Gaussianizing the transmit signals, and randomizing locations, where the goal is to randomize the received power at Willie and thus confuses his decision-making process (X. Chen, Chang, et al. 2024).

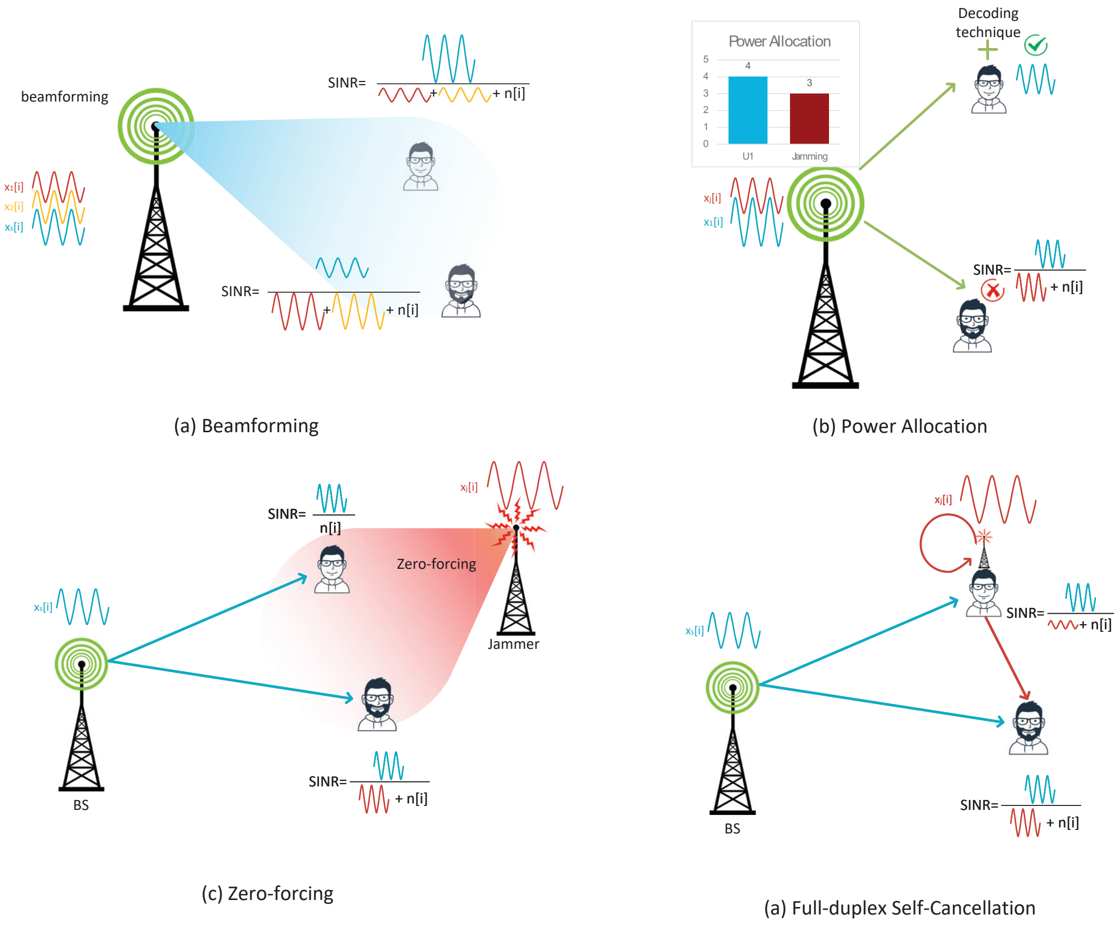
2.3 Interference Management Techniques

Introducing artificial noise into wireless communication can not only interfere the malicious eavesdroppers or wardens, but also influence the transmission performance of legitimate users. However, the above-mentioned risks can be mitigated by properly managing the artificial noise, which aims to maximize the disruptive effects on illegal users while minimizing the interference on legitimate users. Benefiting from its efficient in enhancing the communication reliability and performance, the interference management can be widely used in wireless networks (Jameel et al. 2019).

In this section, we briefly introduce the interference management techniques of AN related to PLS and covert communications, which are illustrated in Figure 4 and can be listed as follows.

Beamforming When the CSIs between jammer and eavesdroppers are available, a multi-antenna jammer can perform maximum ratio transmission (MRT) towards malicious users, which enables the jammer focus its interference signals directly pointing at the eavesdroppers and maximize the noise interference correspondingly. In addition, the beamforming can also be employed at a transmitter, which adjusts its signal beam to align it into the same subspace with legitimate users and realizes MRT to reduce information leakage and improve security.

Power Allocation Power allocation involves the optimization and distribution of transmission resources, which is closely linked to interference management. Improper resource allocation can lead to conflicts in resource usage, resulting in significant interference. Optimizing transmit power allocation for specific users,



(a) Beamforming

(b) Power Allocation

(c) Zero-forcing

(a) Full-duplex Self-Cancellation

FIGURE 4 Typical applications of interference management

based on the requirements of network topology and service demands, has transformed interference from a limiting factor into a valuable resource. For example, by adjusting the power allocation between secure signals and jamming signals, the trade-off between the transmission performance and security can be balanced.

Zero-Forcing By designing the precoding vector at the jammer, the received signals at the receiver can be orthogonal to the decoding matrix after passing through the fading channel. This enables the received jamming signals to be effectively zero-forced, and thus eliminates the interference at the legitimate receiver. However, the effectiveness of zero-forcing technique heavily relies on the acquisition of perfect CSI. With the imperfect CSI, zero-forcing technique may not achieve satisfying and optimal results, which may leave residual noise at the legitimate users, reducing its effectiveness.

Full-Duplex Interference Self-Cancellation Regardless utilizing the external jammer, the legitimate receiver can also be exploited as a full-duplex jammer by further equipping with transmit antennas. It can simultaneously emit jamming signals with transmit antennas and receive signals from the transmitter with its receiving antennas. With the parameters setting of its own jamming signals, the full-duplex receiver can effectively cancel out its self-interference. However, due to the limitation of cancelation technology, the self-interference cannot be fully eliminated, which still requires careful design of the network to optimize the full-duplex performance.

Effectively utilizing the interference in wireless networks can improve both communication quality and performance. In addition, leveraging interference can also enhance the transmission security in both PLS and covert communications.

Chapter Summary

This chapter outlined the key techniques in secure transmission of UAV-related wireless networks. The basic concepts of UAV networks were discussed and the channel in UAV-assisted communication were classified as well. Then, the principles of PLS and covert communication were briefly introduced. At last, the interference management techniques were discussed.

3 CURRENT STATE-OF-THE-ART RESEARCH

This chapter provides a state-of-the-art research overview and comprehensive literature review. The current research and related work are elaborated upon in the areas of UAV communications, PLS, IRS-assisted wireless communications, and covert communications.

3.1 Research on UAV Communications

As an unmanned remotely or software controlled aircraft, UAV has been widely applied in fields such as aerial photography, precision farming, traffic control, research & rescue, intelligent logistics, and emergency communications. Although the development of UAVs is still constrained by battery capacity, their market has been developed rapidly in the past decade, and is estimated to reach 67.64 billion dollars by 2029. As key technique to unlock the potential of drones, wireless communication has gain significant attentions from researchers. Figure 5 demonstrates the typical scenarios of UAV-related communications in 6G. Zeng, R. Zhang, and Lim (2016b) discussed the fundamental network architecture, channel settings, opportunities, and challenges in UAV-related wireless communication networks, providing valuable insights for future research directions. Khawaja et al. (2019) summarized the state-of-the-art channel measuring and modeling methods related to UAV-assisted wireless communication, which provides important references for UAV-related network design.

Benefiting from the rapid development of 5G and the emergence of 6G, UAVs have been exploited in various applications (Mozaffari, Lin, and Hayes 2021). On the one hand, the reliable communication links provided by 5G networks enable UAV to be controlled remotely to fly safe and efficiently. This has fueled the flourish of UAV videos and live streaming, which requires fast transmission rate in air-to-ground links and highly rely on the reliable channel links and bandwidth (Song et al. 2024). The dense deployment of base stations and the development of wireless communication technologies in 5G and 6G enable

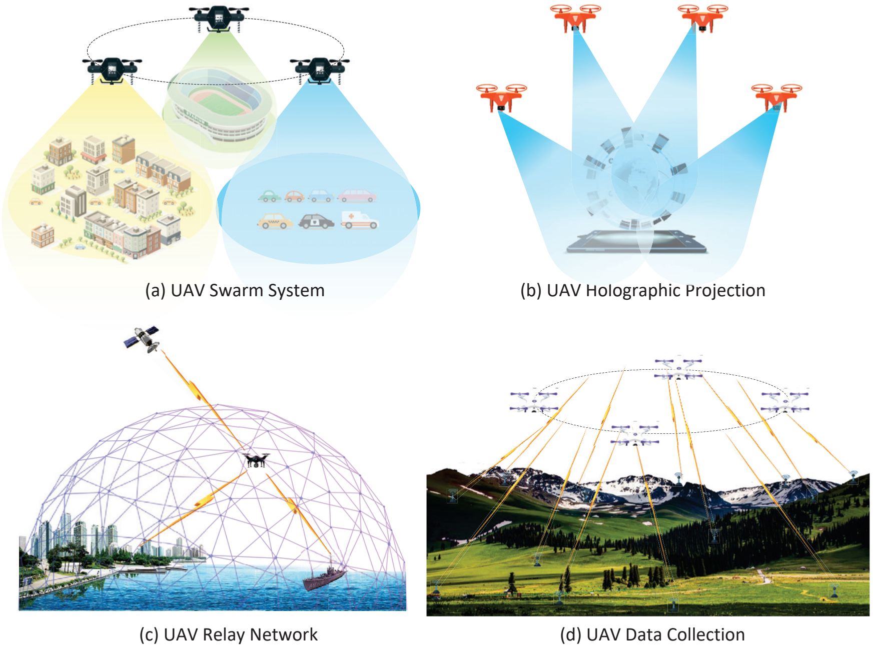


FIGURE 5 Typical scenarios for UAVs in 6G.

the functionality to fulfill these requirements. On the other hand, the volume of UAVs and other communication equipments have become smaller, profiting from progress made in manufacturing industry and device miniaturizing, and thus base stations and relays have become light weight and can be installed on drones (Wilson et al. 2022). As new aerial communication platforms, UAVs can provide data access through air-ground links when terrestrial infrastructure is damaged or the base stations cannot provide enough access points, which can improve the QoS of terrestrial users (Cao, Luo, et al. 2024).

The mobility of UAVs brings new opportunities and challenges for air-to-ground network design, which include the algorithms for UAV to adjust flying altitude to avoid obstacles or link blockages. In addition, UAV can also be exploited in IoT sensing networks to collect sensing data, which includes UAV trajectory design to improve the communication throughput as well as reduce the energy consumption (T. Wang et al. 2024). However, while trajectory optimization can increase the communication throughput of the network, which may also result in a larger delay and cannot satisfy the requirement of ultra-reliable and low-latency communication (URLLC) scenarios (Wu and R. Zhang 2018). The trajectory optimization is critical for the performance of UAV-related networks, i.e., mobile sensing (S. Zhang, H. Zhang, et al. 2019), mobile relays (Jeong, Simeone, and Kang 2018), mobile cloud computing (Zeng, Xu, and R. Zhang 2018), and mobile multicast (Zeng, R. Zhang, and Lim 2016a). Wu, L. Liu, and R. Zhang (2019) explored a strategy to balance the trade-off within transmission delay, energy consumption, and throughput.

The LoS channel links in UAV-related networks contribute significantly to the advanced transmission performance, but also introduce potential risks of information leakage (Ye et al. 2024). Literature has proved that UAV communications can enhance system capacity, frequency efficiency, transmission rate, and resource allocation by leveraging the advanced characteristic of above-mentioned technologies (Azari et al. 2022; X. Chen, Z. Yang, et al. 2020; Deng, Fang, and X. Wang 2023). However, secure transmission must be considered when integrating UAV communications with other advanced techniques, such as non-orthogonal multiple access (NOMA), terahertz (THz) communication, massive multiple-input and multiple-output (MIMO), IRS, and artificial intelligence (AI). PLS and covert communication techniques can be adopted in wireless UAV communications to avoid information leakage.

3.2 Research on Physical Layer Security

Transmission security can be earliest traced back to the pioneering research conducted by Shannon in 1949, where he discussed the information security from the perspective of information theory (Shannon 1949). Additionally, Wyner first proposed the eavesdropping model in 1975, realizing information security by leveraging the channel variability of physical layer characteristics between legitimate channels and eavesdropping channels (Wyner 1975). Based on the above-mentioned pioneer, Csiszar and Korner (1978) applied the eavesdropping channel on the broadcast channels and discussed the secrecy capacity. On the other hand, the fast development of channel coding also enables PLS gain more attention.

3.2.1 Conventional Physical Layer Security

The research regarding to PLS can be divided into two categories:

1. The research on secrecy rate and secrecy capacity from the perspective of information theory.
2. The research on system design from the perspective of optimization and signal processing.

The former one focuses on the secrecy capacity and achievable secrecy rate while the later one devotes to design practical systems through signal processing techniques and optimization strategies. D. Wang, B. Bai, et al. (2019) surveyed the optimization methods in PLS, and summarized the primary corresponding techniques including resource allocation, beamforming, relay selection & cooperation. In addition, this work also categorized the latest literature to four types regarding to their optimization objectives, namely maximize the secrecy rate, minimize the secrecy outage probability, minimize the power consumption, and maximize energy efficiency.

The channel fading in wireless PLS networks is often utilized to achieve secure transmission. The goal is to create more favorable channel conditions for legitimate receivers than for eavesdroppers through signal processing techniques

(Trappe 2015). These techniques include multiple antennas schemes, AN generation, cooperative jamming/relay strategies (L. Sun and Du 2017). Kapetanovic, G. Zheng, and Rusek (2015) discussed the challenges and opportunities associated with MIMO in PLS, where passive eavesdropping attack was pointed to have limited influence on secrecy capacity but was harmful for channel estimation piloting, and three effective schemes of detecting active attack were proposed as well. Jameel et al. (2019) surveyed the strategies of cooperative jamming/relay for PLS and discussed the network designs, which also pointed out the multi-antenna technique can achieve its upper secrecy limit via enlarging the signal disparity between secure user and eavesdroppers. Y. Liu, H.-H. Chen, and L. Wang (2017) summarized the well-known multi-antenna-related secure transmission techniques including beamforming, zero-forcing, AN precoding, and convex precoding. In addition, examples of the state-of-the-art research are listed and summarized in Table 1, where the techniques employed to achieve secure transmission and the objectives of the proposed schemes are outlined.

TABLE 1 Research status on PLS-related work

Reference	Secure Techniques	Objective
Zhao et al. (2020)	Beamforming, power allocation, NOMA	Common user transmission rate maximization
W. Zhang et al. (2019)	AN, beamforming	Secrecy rate maximization
T. Zheng et al. (2024)	NOMA, power allocation	Energy consumption minimization
Nimi and Babu (2024)	Cooperative relay, full-duplex jamming, NOMA	Secrecy outage probability minimization

3.2.2 UAV-Related Physical Layer Security

Integrating UAVs into wireless communication systems can extend transmission range, improve performance, and introduce new communication dimensions. However, the open accessability and highly favorable air-to-ground LoS links result in significant security risks in wireless communications. On the one hand, the signals sent by UAVs via their LoS channels can be intercepted by malicious eavesdroppers easily, which may increase the risk of information leakage. On the other hand, UAV is vulnerable to be attacked by malicious jammer with active interference, which also needs to be addressed crucially. To mitigate these risks, PLS techniques can be adapted to UAV-related wireless communications to ensure secure transmissions and prevent information leakage.

The advanced characteristics of UAV, i.e., high mobility and flexible deployment, can be combined with resource allocation technologies to enhance secure performance. Specifically, UAV can dynamically adjust its power to improve security (Z. Liu, Zhu, et al. 2024). Cui et al. (2018) exploited the mobility of UAV to prevent eavesdropping via optimizing the trajectory and dynamic transmit power. The transmit power will be lowered or shut down when UAV is close to an eavesdropper to prevent eavesdropping, on the contrary, it will be increased when the UAV is close to a legitimate user to achieve better performance. When only the location of eavesdropper and its statistical CSI is available, Y. Chen and Z. Zhang (2019) proposed an incorporating AN beamforming and friendly UAV jammer assisted scheme to achieve secure transmission. When the location of passive eavesdropper is unknown, a cooperative multi-antenna UAV jammer can be leveraged to emit jamming signals into the null space of legitimate user while posing significant interference on malicious eavesdropper, where the system secrecy capacity can be increased and the security can be guaranteed (Y. Zhou et al. 2018). On the other hand, the multi-antenna-based beamforming and IRS can also be exploited to guarantee secure transmission in UAV-assisted networks. Ouyang et al. (2022) proposed an energy-efficient secure beamforming scheme to maximize the worst case secrecy energy efficiency in a millimeter-wave UAV network. S. Li, Duo, Renzo, et al. (2021) proposed an IRS-assisted secure scheme under imperfect CSI of eavesdropping channels, where the trajectory of UAV, the transmit power of transmitter, and the phase-shifting matrix of IRS were jointly optimized to maximize the averaged secrecy rate under the worst case. Apart from the security issue in UAV-related communication, another critical challenge required to be account for is the energy efficiency, which is resulted from the energy constraint of UAVs.

3.3 Research on IRS

Due to the inherent randomness of wireless channels, receivers often experience significant random fading resulting from multi-path, which can be successfully solved by the reconfiguration of an IRS. The increase of distance between source transmitter and destination receiver correspondingly results in a greater path loss at the received signals, which has become a major bottleneck in improving the frequency and energy efficiency in wireless communication systems. To overcome this limitation, IRS has gained considerable attention as a potential solution to improve the wireless transmission channel quality and boost the overall transmission performance (Gong et al. 2020). Consisted with numerous reconfigurable passive elements, i.e., printed dipoles with low-cost, forming a large array of metasurfaces, IRS has the characteristics of low energy consumption, cost-effectiveness, and low complexity. Each reflection element adjusts the phase and the amplitude of incoming signals independently to shape a determined reflected signals realizing intelligent design of wireless channel links. IRS adjusts the reflection coefficients of its elements in order to superimpose the reflected signals with those after other channel paths, enlarge the desired signals, and reduce the interference (Y. Liu, X. Liu, et al. 2021). However, the additional distance introduced by IRS also results in a reduction of received signal power.

TABLE 2 Related work of UAV-assisted IRS communications

Reference	Scenario	Optimization Parameters	Maximization Objective
S. Li, Duo, Yuan, et al. (2020)	Single antenna UAV downlink serves a terrestrial user	Trajectory, $\boldsymbol{\Theta}$	Average capacity
Ge et al. (2020)	Multiple IRSs assist UAV downlink transmission	Trajectory, $\boldsymbol{\Theta}$, BF matrix	Average received signal power
Pang et al. (2022)	IRS-assisted UAV secure transmission	Trajectory, $\boldsymbol{\Theta}$, BF matrix	Secrecy rate
Jiao et al. (2020)	IRS-on-UAV secure transmission with two users	BF matrix, $\boldsymbol{\Theta}$, L_{IRS}	Strong user rate
Q. Zhang, Saad, and Bennis (2019)	Energy harvesting based IRS-on-UAV mmWave network	$\boldsymbol{\Theta}$, L_{IRS}	Capacity
Wei et al. (2023)	IRS-on-UAV secure transmission against multi-eavesdropper	BF matrix, $\boldsymbol{\Theta}$, L_{IRS}	Sum secrecy rate

Benefiting from the lightweight and compact size, an IRS can be installed on building exteriors, roofs, or UAVs to be integrated into wireless networks to assist terrestrial communications (S. Zhang and R. Zhang 2020), enhance indoor communications (Mei et al. 2022), provide higher PLS (J. Chen et al. 2019), and boost signals (Lian et al. 2023). Table 2 reviews the IRS-related studies in UAV-assisted networks, where the considered scenarios, the optimized parameters, and the objective of the proposed schemes are summarized. In this context, $\boldsymbol{\Theta}$ represents the phase-shift matrix of IRS, L_{IRS} denotes the location of IRS, and BF matrix stands for the beamforming matrix of the transmitter, respectively. Applying IRS in UAV-related communications can benefit the mobility, better CSI, and the adaptive coverage. However, the increased security risks resulting from the air-to-ground or air-to-air links also need to be considered and mitigated.

3.4 Research on Covert Communications

Spread spectrum communications were widely applied in military telecommunications in the early 20th century, which hides the confidential signals by utilizing a wider transmission bandwidth. The spread spectrum communication transmit confidential signals over a wide bandwidth B_w that is significantly broader than the required bandwidth B_r, e.g., $B_r \ll B_w$, in order to effectively reduce the power spectral density (PSD) of transmit signals lower than environmental noise PSD and thus hide the information. Although the spread spectrum communication had been rapidly developed at the beginning, the fundamental performance threshold was still missing, resulting in the difficulties of evaluating its effectiveness and thus hindered the further development. Covert communication was first proposed by Simmons in 1983, where he illustrated the well known prison model of Alice, Bob and Willie (Simmons 1984). However, this novel concept of hiding information without being noticed and thus guaranteeing the security did not gain a lot of attention. Until covert communication was proposed again on the first Information Hiding Workshop, where researchers recognized the potential of this technique and began conducting studies on it (Anderson 1996). Bash, Goeckel, and Towsley (2013) published a revolutionary paper and presented the square root law (SRL), which brings the new era of covert communication research. Following this milestone work, researchers have built upon the fundamental principle of SRL and conducted research under three scopes, namely the SRL-related theoretic performance limits, encoding schemes, and practical scenarios.

By introducing uncertainty at Willie, covert communication can randomize his received signal power and conceal the transmission behavior of Alice. The primary techniques adopted by covert communication to introduce uncertainty at Willie can be categorized as follows.

Channel fading: The randomness of channel fading and environmental noise can be leveraged to confuse Willie. The small-scale channel fading can introduce randomness at Willie to prevent him from correctly deciding whether Alice is transmitting or not (H.-M. Wang et al. 2020; L. Wang 2021).

Power randomization: The transmit power and jamming power can be randomized to introduce uncertainty at Willie, where the transmitted signal power still follows random distribution after arriving at Willie, enabling it hide into environmental noise and avoid being noticed (R. Sun et al. 2021; C. Wang et al. 2021).

Gaussian signaling: Leveraging Gaussian signaling can randomize the amplitude and phase, which leads to the random distribution of the received signal power at Willie (Y. Li et al. 2022; W. Yang et al. 2021).

Location randomization: The transmitter randomizes its location to introduce uncertainty at Willie. This method utilizes the distance randomization, which consequentially leverages the channel fading, to provide covertness (T.-X. Zheng et al. 2019; X. Zhou et al. 2019).

The high mobility, fast deployment, and flexibility of UAV enable it highly suitable to be integrated into covert communication networks and develops critical functions. As for the role of UAV, it can serve as Alice, Bob, Willie, or jammer in covert communications. While the LoS channels inhering in UAV communication can enhance transmission performance for legitimate users, they can also, on the other hand, lead to a more precise detection of Willie, thus resulting in the failure of covert communication. Thus, the challenge of maintaining stealth in UAV-based covert communication is an important research area. Yan, Hanly, and Collings (2021) investigated a covert communication between an UAV Alice and a terrestrial Bob, where the impact of UAV's locations on the covertness of legitimate user are considered under six scenarios. It was concluded and proved that the closest location can provide better transmission performance, but may not always be the optimal choice for covert communications. D. Wang, Z. Zheng, et al. (2021) studied a covert network where UAVs serve as Bob and Willie. Perfect and imperfect Gaussian signaling were adopted at the host transmitter and Alice respectively to realize covert transmission. Rao et al. (2022) introduced an UAV jammer to assist the terrestrial covert communication. The trajectory of the UAV jammer was optimized to minimize the interference on legitimate Bob while guaranteeing the covertness, where the optimal trajectory was obtained via a geometric method.

Both covert communication and PLS can provide secure transmission mechanisms for wireless networks. They guarantee the security from different aspects, and thus can be combined to provide a more secure transmission. While both of PLS and covert communication have been extensively researched individually, the combination of them to achieve a even more secure transmission remains unexplored.

Chapter Summary

This chapter provided a comprehensive discussion of the research landscape and detailed review of the state-of-the-art literature. We investigated conventional and UAV-related PLS work, and proposed potential research area for future exploration. In addition, we also narrated the research status and presented a thorough review in UAV, IRS, and covert communications.

4 RESEARCH RESULTS

This thesis primarily advances secure transmission in UAV-related networks through three key contributions including enhancing energy efficiency in UAV data collection, improving secrecy performance by leveraging IRS, and boosting secure data throughput by integrating PLS and covert communication.

4.1 Energy Efficiency in UAV-Assisted PLS Networks

Included articles

I Xinying Chen, Nan Zhao, Zheng Chang, Timo Hämäläinen, and Xianbin Wang (2023), UAV-aided secure short-packet data collection and transmission. *IEEE Transactions on Communications*, 71(4), 2475–2486, https://www.doi.org/10.1109/TCOMM.2023.3244954.

Objectives

The characteristics of high mobility and flexible deployment enable UAVs to be widely applied in wireless communications, particularly in IoT networks, where the data collected by remote sensors can be gathered efficiently and transmitted rapidly via a drone. Additionally, benefiting from the LoS channels introduced by UAVs, the transmission performance can be significantly enhanced. On the contrary, the information leakage risk also increases due to the perfect LoS links. Therefore, ensuring the security in UAV-assisted communications is crucial, and the characteristic of low computational complexity makes PLS ideally suiting for the UAV-IoT networks. The performance metrics of IoT short-packet communications are different from the conventional information theory, necessitating specific adaptations. On the other hand, the limited energy endurance of UAVs caused by the battery capacity is also a critical bottleneck problem in UAV-related communications. One of the primary solutions to enhance UAV endurance is improving its energy efficiency through trajectory design. To address the above-mentioned challenges, we proposed a PLS-based energy-efficient short-packet secure data collection and transmission scheme.

Model & Optimization

The system model is illustrated in Figure 6. A UAV collects finite blocklength data from a group of randomly distributed terrestrial sensors, and then pre-codes the collected data and transmits it to a base station receiver while avoiding being eavesdropped by a terrestrial eavesdropper, where the nearest estimated location of the eavesdropper is provided. LoS fading is considered between the sensors and the UAV due to the openness of the area. First, in the data collection phase, we aim to maximize the energy efficiency of UAV by jointly optimizing the data collection trajectory **w** of the UAV, the user slot assignment **t**, and the entire duration T are jointly optimized to improve the energy efficiency.

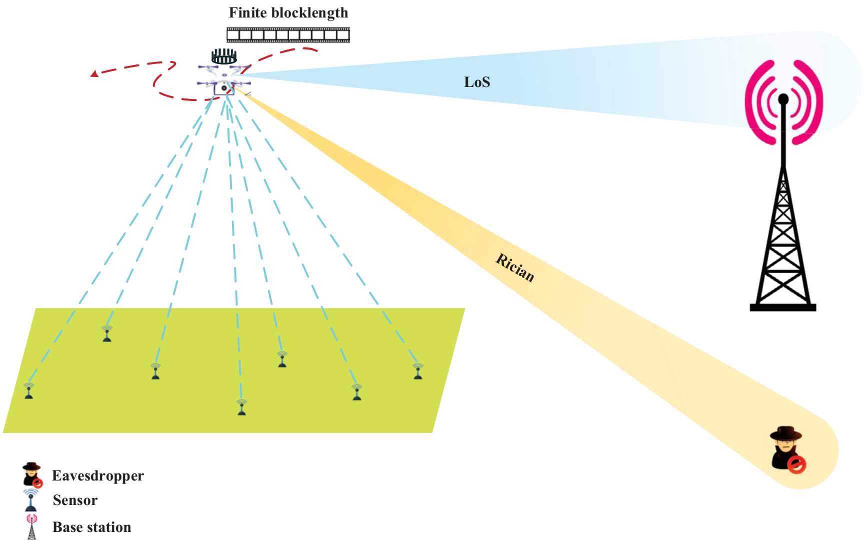


FIGURE 6 System model of energy-efficient UAV short-packet data collection and transmission

The optimization problem can be summarized as follows:

$$\max_{\mathbf{w},\mathbf{t},T} r_{tc} \tag{8a}$$

such that

$$w[1] = w[N], \tag{8b}$$

$$\Delta_{\mathrm{UAV}}[n] \leq \Delta t V_{\max}, \tag{8c}$$

$$\Delta_{\mathrm{UAV}}[n] \leq \theta H, \tag{8d}$$

$$\sum_{n=1}^{N} t_i[n] P_s \Delta t \leq E_i, \tag{8e}$$

$$\sum_{n=1}^{N} R_i[n] \Delta t \geq B_i, \tag{8f}$$

$$\sum_{i=1}^{S} t_i[n] \leq 1, \tag{8g}$$

$$0 \leq t_i[n] \leq 1. \tag{8h}$$

The term r_{tc} represents the energy efficiency of the data-collecting UAV. Constraints (8b), (8c), and (8d) ensure that the UAV returns to its original location after data collection, the displacement between time slots does not exceed its maximum flight velocity, and is relatively small compared to its altitude. Constraint (8e) guarantees that the energy consumption of each sensor remains within its battery capacity. Additionally, constraint (8f) ensures that the UAV collects all the data that each sensor required to transmit. Finally, **t** is a boolean variable, where (8g) and (8h) constraint only one sensor can transmit data within each slot. With the expression of r_{tc} in (8a) and some of the constraints being non-convex, the constructed optimization problem is non-convex and difficult to tackle. To address this optimization problem, we adopt the first-order Taylor expansion and successive convex approximation (SCA) to iteratively obtain the suboptimal trajectory, flight duration, and user slot assignment. Since each subproblem is solved optimally in each iteration with r_{tc} non-decrease, which guarantees the iterative process at least converge to a local optimal solution.

Subsequently, the UAV adopts MRT precoding to improve the transmission performance, and adjusts the transmit power P_a as well as the blocklength N_u to achieve a higher sum secrecy rate $\sum_{n=1}^{N} R_s[n]$, ensuring security against eavesdropping. The optimization problem can be summarized as follows:

$$\max_{P_a, N_u} \sum_{n=1}^{N} R_s[n] \tag{9a}$$

such that

$$P_a \leq P_{a_{\max}}, \tag{9b}$$

$$N_u \leq N_{u_{\max}}, \tag{9c}$$

$$R_e[n] \leq r, \tag{9d}$$

$$p_{\text{out}}[n] \leq \xi, \tag{9e}$$

where constraint (9b) limits the maximum allowed transmit power of the UAV, while (9c) restricts the blocklength transmitted by the UAV to the base station. Constraint (9d) ensures secure communication by preventing eavesdropping, and (9e) imposes a transmission outage probability limit for legitimate users. To solve this optimization problem, monotonicity analysis and traversal algorithm are combined to derive the optimal value P_a and N_u.

Results

In Figure 7, the trajectory of proposed energy-efficient data collection scheme is compared with that of the benchmark, where the UAV flies directly over each node to collect data sequentially. From the results, we can see that the trajectory of proposed energy-efficient scheme is shorter than that of the benchmark in order to save energy. Furthermore, Figure 8 compares the performance of the proposed scheme and the benchmark in terms of energy efficiency and sum collected data, under varying data requirements and transmit power of each node. From the results, we can see that our proposed scheme surpasses the benchmark in both energy efficiency and the sum collected data metrics. From Figure 9, we can conclude that both the optimal P_a and R_s increase as the eavesdropping rate threshold gets larger. Additionally, we can also see that the corresponding optimal blocklength N of UAV first increases then stabilizes as r rises.

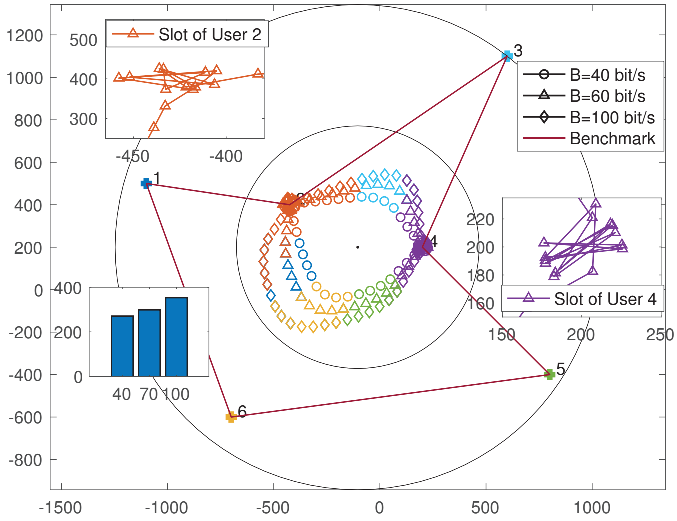
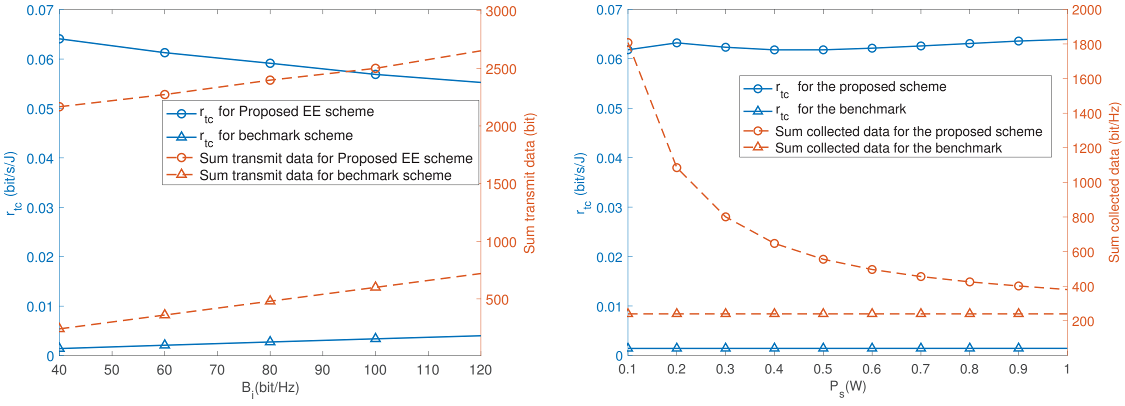


FIGURE 7 Trajectory comparison between proposed energy-efficient scheme and benchmark.



(a) Impact of the data required to be transmitted B_i at each sensor node

(b) Impact of transmit power P_s at each sensor node

FIGURE 8 Comparison of energy efficiency r_{tc} and sum collected data between the proposed scheme and benchmark

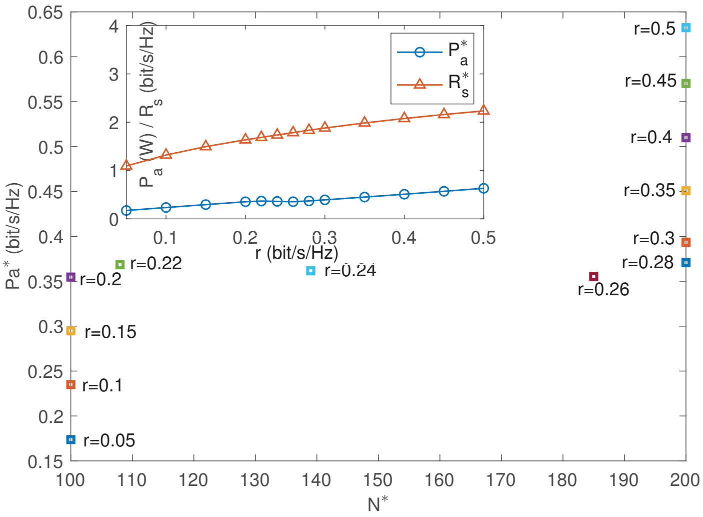


FIGURE 9 Impact of eavesdropping rate threshold r on the optimal transmit power P_a of UAV and secrecy rate R_s

Conclusion & Discussion

This research proposed a secure data collection and transmission scheme in short-packet UAV-assisted wireless communication aiming to enhance the energy efficiency and guarantee the security via optimizing the trajectory, user slot assignment, flight duration, transmit power, and data blocklength. The simulation results have proved that our proposed scheme can achieve greater energy efficiency compared with the benchmark and guarantee the eavesdropping rate below the acceptable threshold.

Contribution

Xinying Kilpi-Chen is the primary author of the article, contributing to manuscript writing&revising, system model design, problem optimization, and performance evaluation. Zheng Chang supervised the work and contributed to the system model validation as well as manuscript refinement. Nan Zhao and Timo Hämäiläinen supervised the work and revised the manuscript.

4.2 Security Enhancement in IRS-on-UAV Networks

Included articles

II Xinying Chen, Zheng Chang and Timo Hämäläinen (2024). Secure transmission for IRS-on-UAV-assisted wireless networks. *IEEE Transactions on Communications*, submitted.

III Xinying Chen, Zheng Chang, Nan Zhao and Timo Hämäläinen (2023). IRS-based secure UAV-assisted transmission with location and phase shifting optimization. *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, pp. 1672–1677, IEEE. https://www.doi.org/10.1109/ICCWorkshops57953.2023.10283558.

Objectives

Wireless communication security is a crucial issue due to the broadcasting nature of channels, which becomes even more critical with the involvement of UAVs. UAV-aided transmission can leverage the perfect LoS channels to achieve higher rate at legitimate users, which, on the contrary, can also be exploited by malicious users. Therefore, the security is an essential parameter in UAV-aided transmissions. Similar to UAVs, IRSs also have the advantages of flexible deployment, easy configuration, and compact size. Moreover, IRS can also modify channel fading properties by programming the amplitude and phase-shift of its passive reconfigurable reflection elements, which can be utilized to improve the performance of legitimate users and increase the fading at malicious eavesdroppers. By combining IRS and UAV, the mobility of UAV can be leveraged to further improve the transmission rate at legitimate users through location optimization. Furthermore, the multi-antenna beamforming and AN jamming can be adopted to further improve both network performance and security. Inspired by the above-mentioned advanced techniques, we propose a PLS-based IRS-on-UAV assisted secure transmission scheme, which leverages AN, beamforming, and IRS to improve the performance and security of legitimate user and reduce the eavesdropping rate.

Model & Optimization

The system model is shown in Figure 10, where IRS-on-UAV is utilized to enhance the received confidential signals at legitimate Bob while weakening them at eavesdropper Eav. In this system, the BS transmits confidential information to Bob while also emitting AN to prevent eavesdropping. Meanwhile, beamforming is also utilized by base station to improve the received confidential signal power at Bob and enhance the received jamming signals at Eav. An IRS is mounted on a UAV to assist the secure transmission, by enhancing/suppressing the received signals at Bob/Eav.

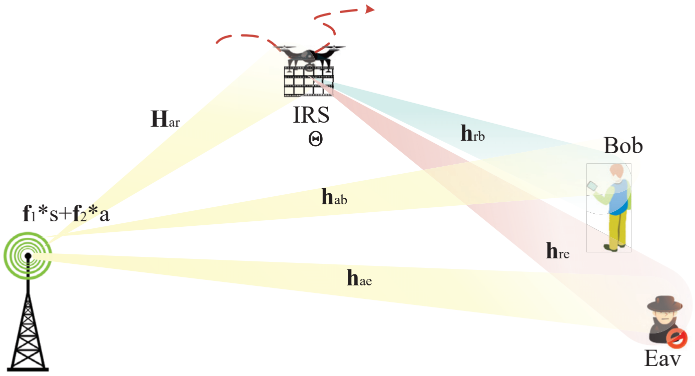


FIGURE 10 System model of IRS-on-UAV assisted secure transmission

To improve the secure transmission performance at legitimate Bob while maintaining a constrained eavesdropping rate at Eav, the beamforming vectors $\mathbf{f}_1$ and $\mathbf{f}_2$ including transmit/jamming power split ratio, phase-shift matrix $\boldsymbol{\Theta}$ and location L_r of IRS are jointly optimized to maximize the secrecy rate R_s with the eavesdropping rate constraint satisfied. The optimization problem can be summarized as follows:

$$\max_{\mathbf{f}_1,\mathbf{f}_2,\boldsymbol{\Theta},L_r} \quad R_s \tag{10a}$$

such that

$$R_b \geq R_{\min}, \tag{10b}$$
$$\theta_i \in [0, 2\pi), \tag{10c}$$
$$\mathbf{f}_1^H\mathbf{f}_1 + \mathbf{f}_2^H\mathbf{f}_2 \leq P_{a_{\max}}, \tag{10d}$$
$$R_e \leq r_e, \tag{10e}$$

where (10b) ensures that the transmission rate exceeds the required threshold to maintain transmission performance, while (10d) limits the transmit and jamming power of the precoding vectors. Additionally, (10c) imposes restrictions on the phase-shift matrix. The eavesdropping rate is constrained in (10e), which provides an additional layer of security beyond R_s. Given the non-convex objective function and constraints in (11), it is evident that this optimization problem is non-convex and challenging to solve. To address this, we alternately optimized $(\mathbf{f}_1, \mathbf{f}_2)$, $\boldsymbol{\Theta}$ and L_r, treating the other two parameters as constants until reaching convergence. Furthermore, we employed SCA, semidefinite relaxation (SDR), and first-order Taylor expansion techniques to iteratively solve the problem.

Results

In Figure 11, the impact of beamforming vectors at base station on the transmission performance is analyzed and compared with two benchmark schemes. One scheme sets transmit power equals to jamming power, while the other does not employ any jamming signals. From the results, we can see that the proposed precoding vector optimization scheme can achieve higher secrecy rate compared with other two benchmark schemes. In Figure 12, our proposed scheme is compared with benchmark schemes that IRS employs MRT and direct reflection, respectively. The results show that our proposed scheme leads to a higher secrecy rate. The influence of UAV's location optimization on security performance of the proposed scheme is also compared with other fixed locations in Figure 13. It is observed that the location optimization of proposed scheme can achieve better security performance. Lastly, the proposed scheme is compared with other benchmark schemes of without location optimization and without phase shift optimization respectively in Figure 14. It is evident that our proposed scheme can offer superior secrecy performance with the same setting compared with other two benchmark schemes.

Conclusion & Discussion

This research proposed a secure transmission scheme leveraging an IRS-on-UAV to reconfigure the channel links and improve the security performance against an eavesdropper. The secrecy rate between legitimate users was maximized via jointly optimizing the precoding vectors of both AN and confidential signals, the phase shift matrix of IRS, and the location of UAV while satisfying the eavesdropping constraint. Article II extends the optimization parameters and adjusts to a more practical channel setting from Article III. Simulation results have extensively compared the proposed scheme with other benchmark schemes, demonstrating its effectiveness and reliability in providing more secure transmission.

Contribution

Xinying Kilpi-Chen is the primary author of the articles, responsible for manuscript writing&revision, system model design, problem optimization, and performance evaluation. Zheng Chang supervised these the work, contributing to system design and manuscripts revision. Timo Hämäiläinen also supervised the work and revised the manuscripts.

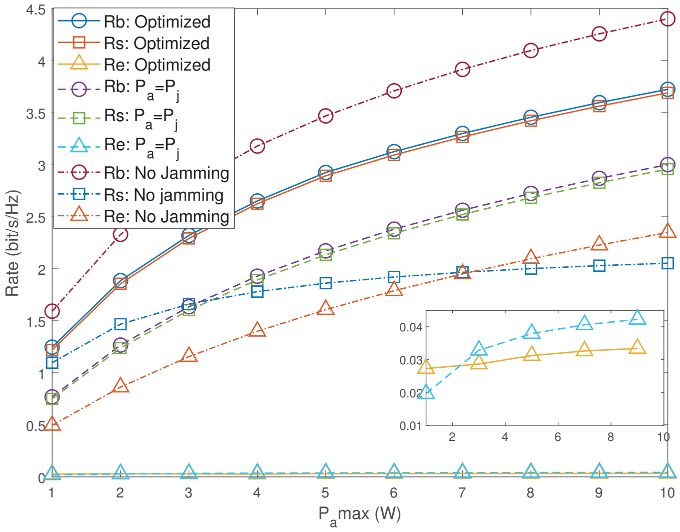


FIGURE 11 Comparison of beamforming optimization and benchmarks

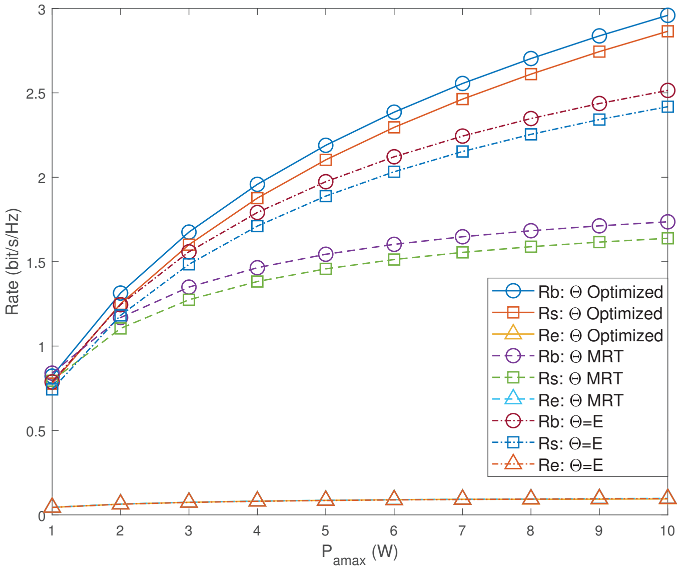


FIGURE 12 Comparison of phase-shift matrix optimization and benchmarks

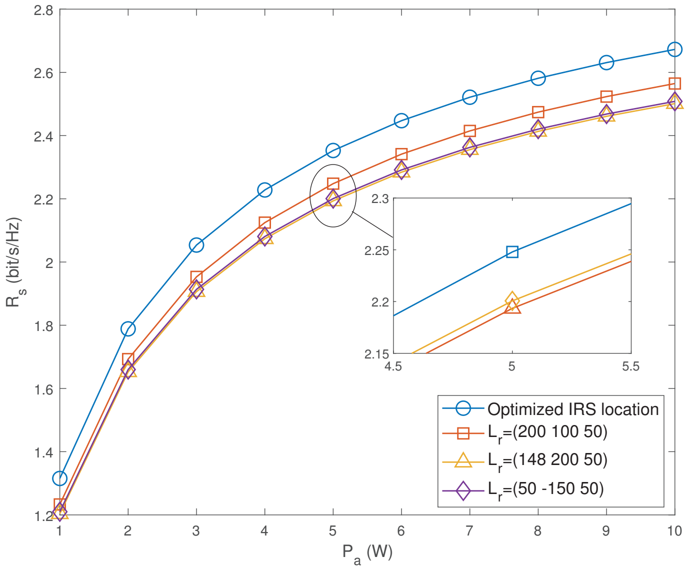


FIGURE 13 Comparison of location optimization and fixed locations of UAV

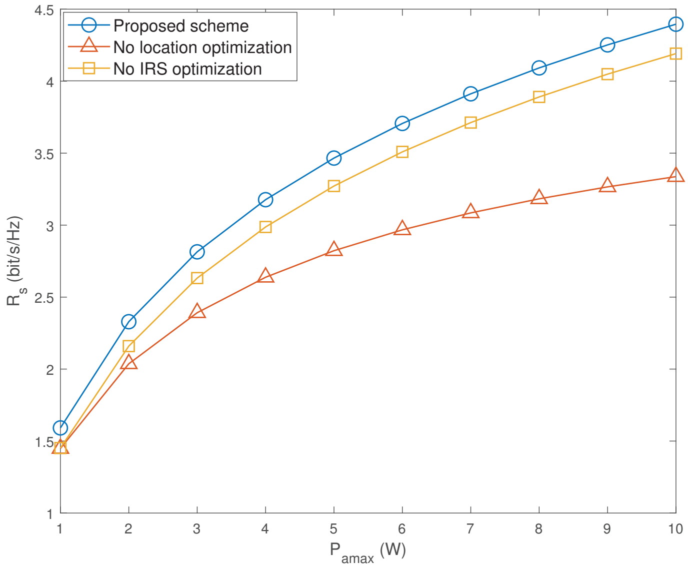


FIGURE 14 Comparison of the proposed scheme and schemes without location or IRS optimization

4.3 Security Improvement in Covert Communications via PLS

Included articles

IV Xinying Chen, Zheng Chang, and Timo Hämäläinen (2024). Enhancing covert secrecy rate in a zero-forcing UAV jammer-assisted covert communication. *IEEE Wireless Communications Letters*, accepted for publication.

V Xinying Chen, Zheng Chang, and Timo Hämäläinen (2024). Achieving improved security in UAV-assisted covert communication networks. *IEEE International Conference on Communications in China Workshops (ICCC Workshops)*, pp. 323–328, https://doi.org/10.1109/ICCCWorkshops62562.2024.10693776.

Objectives

PLS has been proved to be effective in enhancing security in wireless communications due to its low computational complexity and adaptability. However, it cannot fully eliminate the risk of information leakage, which becomes more serious as eavesdroppers can improve their decoding ability with advanced technologies. As long as the eavesdroppers can intercept the confidential signals from the broadcast channels, secure transmission design is required. The flourish of covert communication shed a light on secure wireless transmission, which can hide the transmission behavior and thus lead to a complete safety for confidential information. Since PLS and covert communication address security from different perspectives, the first challenge is establishing the performance metric to evaluate the effectiveness and security.

Model & Optimization

The system model is shown in Figure 15, where Alice intends to transmit confidential information Bob while avoiding the detection from Willie with the assistance of a UAV jammer. Multi-antenna Alice applies MRT to maximize the transmission rate at Bob and meanwhile utilizes the Rayleigh fading to introduce uncertainty at the warden. The multi-antenna jammer adopts Gaussian signaling to introduce uncertainty at the warden and employs zero-forcing to avoid interfering the transmission performance at Bob. If Willie's location is known, the jammer can hover above him to achieve maximum jamming. To evaluate the secrecy performance in the novel PLS-enhanced covert communication, we define the covert secrecy rate, which is the sum of the secrecy rate when Willie correctly detects Alice's transmission and the transmission rate when Willie MD. Alice's security can be guaranteed under both of the cases. This approach accounts for the fact that even if Alice's transmission is detected, security can still be maintained within the secrecy rate capacity. In addition, the key in covert communications is to introduce uncertainty at the warden to confuse its detection, and how to effectively introduce uncertainty in UAV-assisted LoS links remains an open

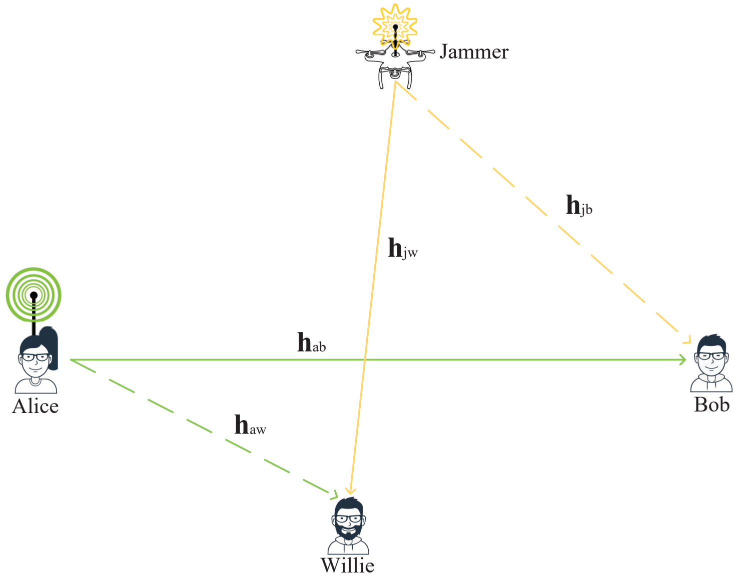


FIGURE 15 System model of UAV-assisted security enhanced covert communication

challenge.

The optimization goal is to maximize the covert secrecy rate R_{cs} while ensuring that the error detection probability p_e^* exceeds a given threshold and the eavesdropping rate R_e stays below a specified constraint via jointly optimizing the transmit power of Alice P_a and the jamming power of the UAV jammer P_j. The optimization problem can be summarized as follows:

$$\max_{P_a,P_j} R_{cs} \tag{11a}$$

such that

$$\begin{aligned} p_e^* &\geq \epsilon, && (11b)\\ R_e &\leq r_e, && (11c)\\ R_b &\geq r, && (11d)\\ P_a &\leq P_{a_{\max}}, && (11e)\\ P_j &\leq P_{j_{\max}}, && (11f) \end{aligned}$$

where constraint (11b) ensures the success of covert communication, while (11c) prevents eavesdropping. The transmission performance of legitimate users is maintained through (11d). Constraints (11e) and (11f) set the transmit and jamming power limits, respectively. Probability theory was employed to derive the optimal error detection probability and its corresponding power detection threshold. The classification and discussion method was used to determine the upper limit of P_a/P_j concerning covertness. Finally, the optimal transmit and jamming powers were jointly obtained through monotonicity analysis.

Results

The influence of the power detection threshold of Willie on his error detection probability is investigated and compared between Monte Carlo simulation results and theoretical calculation results in Figure 16. It is observed that the Monte Carlo simulations match perfectly with our theoretical results. The results show that there exists an optimal detection threshold to minimize the error detection probability. In Figure 17, the impact of jamming power limits on the optimal transmit power of Alice and the achievable covert secrecy rate is illustrated. From the results, we can see that with the given minimum allowed error detection probability constraint, the optimal transmit power increases with the jamming power upper-limit and thus lead to the increase of achievable covert secrecy rate. Figure 18 compares the performance of proposed scheme with other benchmark schemes, namely without MRT optimization ($M = 1$), without zero-forcing ($N = 1$), and without transmit power optimization ($P_a = 0.1$ W). The results show that our proposed scheme can achieve higher covert secrecy rate than other benchmark schemes while maintaining the covertness.

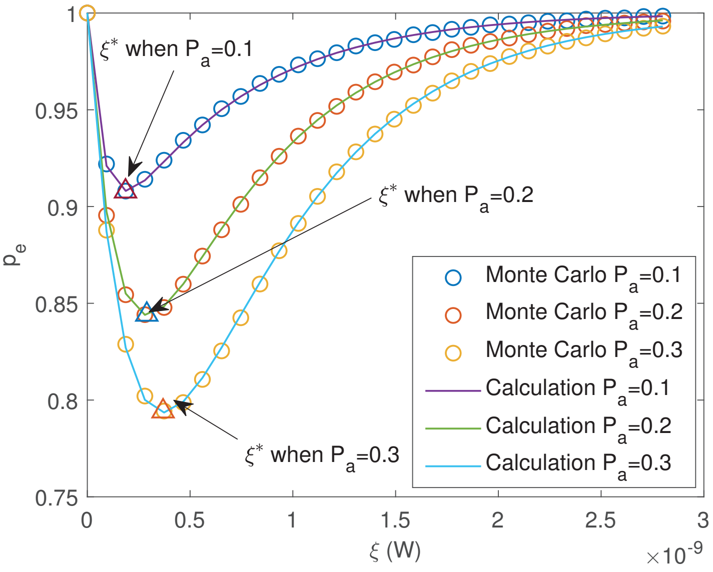


FIGURE 16 The impact of power detection threshold ξ on error detection probability p_e

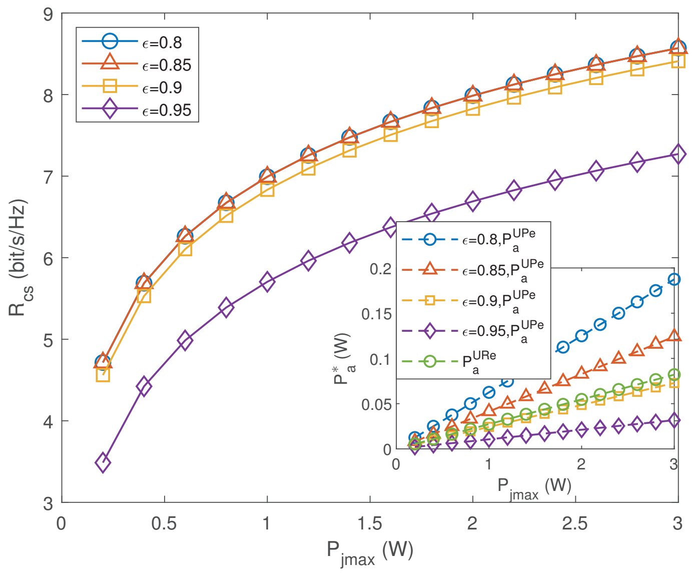


FIGURE 17 Impact of the jamming power upper-limit P_{jmax} on the achievable covert secrecy rate R_{cs}

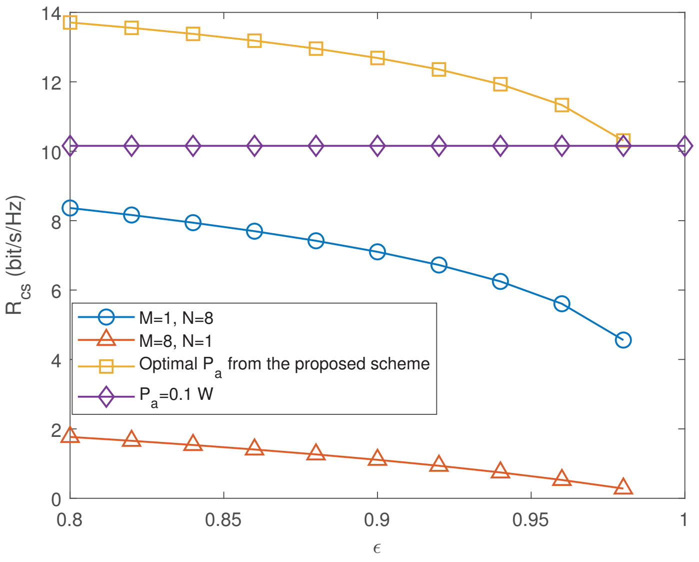


FIGURE 18 Comparison of proposed more secure covert scheme and other benchmarks

Conclusion & Discussion

The results have proved the effectiveness of our proposed zero-forcing UAV jammer-assisted scheme in enhancing secure performance of covert communication. The Gaussian signaling and small-scale channel fading can successfully introduce uncertainty at Willie and hide the transmission of Alice. In addition, the zero-forcing technique applied at the UAV jammer can effectively interfere Willie's eavesdropping without affecting Bob's reception. The secure transmitted data is significantly increased compared with conventional covert communication schemes. Article IV further extends the conclusion and results from Article V.

Contribution

Xinying Kilpi-Chen is the primary author of the articles, who is responsible for manuscripts writing&revision, system model design, problem optimization, and performance evaluation. Zheng Chang supervised the work, and contributed to the system model validation, manuscripts refinement, and crafting responses to reviewers comments. Timo Hämäiläinen also supervised the work and revised the manuscripts.

Chapter Summary

This chapter offered a brief overview concerning to the objective, system models & optimization, and related results of the included publications. In addition, the contributions related to the listed publications were also highlighted.

5 CONCLUSION

This dissertation has been dedicated to improving the security and transmission performance in UAV-related networks. The key findings of the dissertation are summarized to provide a clear and concise overview, along with insightful directions for future research.

5.1 Key Findings

To improve the security of UAV-assisted wireless communications, this dissertation proposed and discussed several PLS and covert communication schemes to improve transmission secrecy. Specifically, PLS-based schemes were proposed to achieve secure and energy-efficient data collection as well as boost transmission performance with the assistance of an IRS. Furthermore, PLS was integrated with covert communication for the first time to enhance secrecy performance.

The research highlighted that UAV-related wireless communications are inherently more vulnerable to eavesdropping or detection. Both PLS and covert communication can promise secure transmission with specific techniques, such as power allocation, AN, beamforming, IRS, and Gaussian signaling. The key outcomes of the included articles can be concluded as follows.

- To achieve security as well as improve energy efficiency in a UAV data collection IoT network, a joint optimization of trajectory and data collection strategy, along with a power allocation secure transmission scheme, was proposed.
- To guarantee the information confidentiality and improve the transmission performance, an IRS was introduced to enhance the transmission and secure performance. Meanwhile, beamforming and AN were utilized together with the IRS to achieve a higher secrecy rate.
- To boost the security performance of covert communications, PLS was initially incorporated into covert communications, where the covert secrecy

rate was defined and the transmission strategy was designed to further improve the securely transmitted data throughput under both correct and incorrect detection of the warden.

5.2 Limitations and Future Work

This dissertation provided several effective solutions for secure transmission in UAV-related wireless communications using PLS and covert communication techniques. While the proposed schemes yielded promising results, there remain several potential directions for future research to further extend and enhance this work, which could be listed and discussed as follows:

Imperfect CSI Scenarios Acquiring accurate CSI in wireless communications demands substantial resources, and the precision of CSI cannot be guaranteed. Therefore, enhancing transmission and secrecy performance in CSI-based secure transmissions under imperfect CSI conditions remains a critical challenge. Machine learning methods can also be leveraged to improve the accuracy of CSI estimation.

Advanced Uncertainty Introduction Methods The pivotal reason for covert communication to successfully obscure the existence of transmission is the uncertainty introduced to Willie. Most existing research relies on AN to hide the confidential signals, which raise up the trade-off between covertness and resource efficiency. Therefore, investigating more efficient uncertainty introduction methods is critical.

Unequal Prior Probabilities Integrating PLS-related secure transmission methods into covert communication is still at the early stage of the research. Investigating whether unequal prior probabilities could further enhance uncertainty and improve security performance is worth exploring.

Extensibility of Schemes for Complex Networks The schemes proposed in this dissertation are mostly focusing on illustrating a relatively simple network structures and demonstrating the secure transmission. Future work could explore how these schemes can be extended to more complex and incorporate scenarios, which involve multiple transmitters and receivers. Therefore, our proposed strategies can better reflect practical network applications.

YHTEENVETO (SUMMARY IN FINNISH)

Miehittämättömän ilma-alusavusteisen (unmanned aerial vehicle, UAV) langattoman viestinnän turvallisuuden parantamiseksi tässä väitöskirjassa ehdotettiin ja käsiteltiin useita fyysisen kerroksen turvallisuuden (physical layer security, PLS) ja piiloviestintämenetelmiä lähetyssalaisuuden parantamiseksi. Erityisesti ehdotettiin PLS-pohjaisia järjestelmiä turvallisen ja energiatehokkaan tiedonkeruun saavuttamiseksi sekä tiedonsiirron tehostamiseksi älykkään heijastavan pinnan (intelligent reflecting surface, IRS) avulla. Lisäksi PLS integroitiin suojattuun viestintään ensimmäistä kertaa salassapitokyvyn parantamiseksi.

Tutkimus osoitti, että UAV:hen liittyvä langaton viestintä on luonnostaan alttiimpi salakuuntelulle tai havaitsemiselle. Sekä PLS että suojattu viestintä voivat luvata salatun tiedonsiirron tietyillä tekniikoilla, kuten tehon allokoinnilla, keinotekoisella kohinalla (artificial noise, AN), keilan muodostamisella, IRS:llä ja Gaussin signaloinnilla. Mukana olevien artikkeleiden keskeiset tulokset voidaan tiivistää seuraavasti.

- Liikeradan ja tiedonkeruustrategian yhteisoptimointia yhdessä suojatun tehonjakojärjestelmän kanssa ehdotettiin UAV-tiedonkeruulle IoT-verkon turvallisuuden ja energiatehokkuuden parantamiseksi.
- Tietojen luottamuksellisuuden takaamiseksi ja lähetyksen suorituskyvyn parantamiseksi otettiin käyttöön IRS, joka tehostaa tiedonsiirtoa ja turvallista suorituskykyä. Yhteisoptimointia ja AN:ta käytettiin yhdessä IRS:n kanssa korkeamman salassapitoasteen saavuttamiseksi.
- Suojatun viestinnän turvallisuussuorituskyvyn parantamiseksi PLS sisällytettiin alun perin suojattuun viestintään, jossa määriteltiin suojauksen salaisuusaste ja lähetysstrategia suunniteltiin parantamaan edelleen turvallisesti välitetyn tiedon kulkua sekä vartijan oikean että virheellisen havaitsemisen yhteydessä.

BIBLIOGRAPHY

Aggarwal, S., Kumar, N., and Tanwar, S. 2021. Blockchain-Envisioned UAV Communication Using 6G Networks: Open Issues, Use Cases, and Future Directions. IEEE Internet of Things Journal 8 (7), 5416–5441.

An, J., Kang, B., Ouyang, Q., Pan, J., and Ye, N. 2024. Covert Communications Meet 6G NTN: A Comprehensive Enabler for Safety-Critical IoT. IEEE Network 38 (4), 17–24.

Anderson, R. 1996. Information Hiding: First International Workshop, Cambridge, UK, May 30 – June 1, 1996 Proceedings. Springer.

Azari, M. M., Solanki, S., Chatzinotas, S., and Bennis, M. 2022. THz-Empowered UAVs in 6G: Opportunities, Challenges, and Trade-offs. IEEE Communications Magazine 60 (5), 24–30.

Bai, Y., Zhao, H., Zhang, X., Chang, Z., Jäntti, R., and Yang, K. 2023. Toward Autonomous Multi-UAV Wireless Network: A Survey of Reinforcement Learning-Based Approaches. IEEE Communications Surveys & Tutorials 25 (4), 3038–3067.

Bash, B. A., Goeckel, D., and Towsley, D. 2013. Limits of Reliable Communication with Low Probability of Detection on AWGN Channels. IEEE Journal on Selected Areas in Communications 31 (9), 1921–1930.

Bloch, M., Günlü, O., Yener, A., Oggier, F., Poor, H. V., Sankar, L., and Schaefer, R. F. 2021. An Overview of Information-Theoretic Security and Privacy: Metrics, Limits and Applications. IEEE Journal on Selected Areas in Information Theory 2 (1), 5–22.

Burhanuddin, L. A. b., Liu, X., Deng, Y., Challita, U., and Zahemszky, A. 2022. QoE Optimization for Live Video Streaming in UAV-to-UAV Communications via Deep Reinforcement Learning. IEEE Transactions on Vehicular Technology 71 (5), 5358–5370.

Cao, Y., Zhao, N., Chen, Y., Jin, M., Ding, Z., Li, Y., and Yu, F. R. 2020. Secure Transmission via Beamforming Optimization for NOMA Networks. IEEE Wireless Communications 27 (1), 193–199.

Cao, Y., Luo, Y., Yang, H., and Luo, C. 2024. UAV-Based Emergency Communications: An Iterative Two-Stage Multiagent Soft Actor–Critic Approach for Optimal Association and Dynamic Deployment. IEEE Internet of Things Journal 11 (16), 26610–26622.

Chen, J., Liang, Y.-C., Pei, Y., and Guo, H. 2019. Intelligent Reflecting Surface: A Programmable Wireless Environment for Physical Layer Security. IEEE Access 7, 82599–82612.

Chen, X., An, J., Xiong, Z., Xing, C., Zhao, N., Yu, F. R., and Nallanathan, A. 2023. Covert Communications: A Comprehensive Survey. IEEE Communications Surveys & Tutorials 25 (2), 1173–1198.

Chen, X., Chang, Z., Liu, M., Zhao, N., Hämäläinen, T., and Niyato, D. 2024. UAV-IRS Assisted Covert Communication: Introducing Uncertainty via Phase Shifting. IEEE Wireless Communications Letters 13 (1), 103–107.

Chen, X., Yang, Z., Zhao, N., Chen, Y., Wang, J., Ding, Z., and Yu, F. R. 2020. Secure Transmission via Power Allocation in NOMA-UAV Networks With Circular Trajectory. IEEE Transactions on Vehicular Technology 69 (9), 10033–10045.

Chen, Y. and Zhang, Z. 2019. UAV-Aided Secure Transmission in MISOME Wiretap Channels With Imperfect CSI. IEEE Access 7, 98107–98121.

Csiszar, I. and Korner, J. 1978. Broadcast channels with confidential messages. IEEE Transactions on Information Theory 24 (3), 339–348.

Cui, M., Zhang, G., Wu, Q., and Ng, D. W. K. 2018. Robust Trajectory and Transmit Power Design for Secure UAV Communications. IEEE Transactions on Vehicular Technology 67 (9), 9042–9046.

Deng, C., Fang, X., and Wang, X. 2023. UAV-Enabled Mobile-Edge Computing for AI Applications: Joint Model Decision, Resource Allocation, and Trajectory Optimization. IEEE Internet of Things Journal 10 (7), 5662–5675.

Feng, C. and Wang, H.-M. 2021. Secure Short-Packet Communications at the Physical Layer for 5G and Beyond. IEEE Communications Standards Magazine 5 (3), 96–102.

Ge, L., Dong, P., Zhang, H., Wang, J.-B., and You, X. 2020. Joint Beamforming and Trajectory Optimization for Intelligent Reflecting Surfaces-Assisted UAV Communications. IEEE Access 8, 78702–78712.

Geraci, G., Garcia-Rodriguez, A., Azari, M. M., Lozano, A., Mezzavilla, M., Chatzinotas, S., Chen, Y., Rangan, S., and Renzo, M. D. 2022. What Will the Future of UAV Cellular Communications Be? A Flight From 5G to 6G. IEEE Communications Surveys & Tutorials 24 (3), 1304–1335.

Gong, S., Lu, X., Hoang, D. T., Niyato, D., Shu, L., Kim, D. I., and Liang, Y.-C. 2020. Toward Smart Wireless Communications via Intelligent Reflecting Surfaces: A Contemporary Survey. IEEE Communications Surveys & Tutorials 22 (4), 2283–2314.

ITU 2017. Minimum requirements related to technical performance for IMT-2020 radio interface(s). Report ITU-R M.2410-0. International Telecommunication Union.

Jameel, F., Wyne, S., Kaddoum, G., and Duong, T. Q. 2019. A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. IEEE Communications Surveys & Tutorials 21 (3), 2734–2771.

Jeong, S., Simeone, O., and Kang, J. 2018. Mobile Edge Computing via a UAV-Mounted Cloudlet: Optimization of Bit Allocation and Path Planning. IEEE Transactions on Vehicular Technology 67 (3), 2049–2063.

Jiang, W., Han, B., Habibi, M. A., and Schotten, H. D. 2021. The Road Towards 6G: A Comprehensive Survey. IEEE Open Journal of the Communications Society 2, 334–366.

Jiang, X., Chen, X., Tang, J., Zhao, N., Zhang, X. Y., Niyato, D., and Wong, K.-K. 2021. Covert Communication in UAV-Assisted Air-Ground Networks. IEEE Wireless Communications 28 (4), 190–197.

Jiao, S., Fang, F., Zhou, X., and Zhang, H. 2020. Joint Beamforming and Phase Shift Design in Downlink UAV Networks with IRS-Assisted NOMA. Journal of Communications and Information Networks 5 (2), 138–149.

Kapetanovic, D., Zheng, G., and Rusek, F. 2015. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. IEEE Communications Magazine 53 (6), 21–27.

Ke, Y., Zhang, M.-Q., Liu, J., Su, T.-T., and Yang, X.-Y. 2020. Fully Homomorphic Encryption Encapsulated Difference Expansion for Reversible Data Hiding in Encrypted Domain. IEEE Transactions on Circuits and Systems for Video Technology 30 (8), 2353–2365.

Khan, W. U., Lagunas, E., Ali, Z., Javed, M. A., Ahmed, M., Chatzinotas, S., Ottersten, B., and Popovski, P. 2022. Opportunities for Physical Layer Security in UAV Communication Enhanced with Intelligent Reflective Surfaces. IEEE Wireless Communications 29 (6), 22–28.

Khawaja, W., Guvenc, I., Matolak, D. W., Fiebig, U.-C., and Schneckenburger, N. 2019. A Survey of Air-to-Ground Propagation Channel Modeling for Unmanned Aerial Vehicles. IEEE Communications Surveys & Tutorials 21 (3), 2361–2391.

Kihero, A. B., Furqan, H. M., Sahin, M. M., and Arslan, H. 2024. 6G and Beyond Wireless Channel Characteristics for Physical Layer Security: Opportunities and Challenges. IEEE Wireless Communications 31 (3), 295–301.

Li, S., Duo, B., Renzo, M. D., Tao, M., and Yuan, X. 2021. Robust Secure UAV Communications With the Aid of Reconfigurable Intelligent Surfaces. IEEE Transactions on Wireless Communications 20 (10), 6402–6417.

Li, S., Duo, B., Yuan, X., Liang, Y.-C., and Di Renzo, M. 2020. Reconfigurable Intelligent Surface Assisted UAV Communication: Joint Trajectory Design and Passive Beamforming. IEEE Wireless Communications Letters 9 (5), 716–720.

Li, Y., Zhang, Y., Wang, J., Xiang, W., Xiao, S., Chang, L., and Tang, W. 2022. Performance Analysis for Covert Communications Under Faster-Than-Nyquist Signaling. IEEE Communications Letters 26 (6), 1240–1244.

Lian, Z., Su, Y., Wang, Y., Ji, P., Jin, B., Zhang, Z., and Xie, Z. 2023. A Novel Geometry-Based 3-D Wideband Channel Model and Capacity Analysis for IRS-Assisted UAV Communication Systems. IEEE Transactions on Wireless Communications 22 (8), 5502–5517.

Liu, Y., Chen, H.-H., and Wang, L. 2017. Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges. IEEE Communications Surveys & Tutorials 19 (1), 347–376.

Liu, Y., Liu, X., Mu, X., Hou, T., Xu, J., Di Renzo, M., and Al-Dhahir, N. 2021. Reconfigurable Intelligent Surfaces: Principles and Opportunities. IEEE Communications Surveys & Tutorials 23 (3), 1546–1577.

Liu, Y., Huang, C., Chen, G., Song, R., Song, S., and Xiao, P. 2024. Deep Learning Empowered Trajectory and Passive Beamforming Design in UAV-RIS Enabled Secure Cognitive Non-Terrestrial Networks. IEEE Wireless Communications Letters 13 (1), 188–192.

Liu, Z., Liu, J., Zeng, Y., and Ma, J. 2018. Covert Wireless Communications in IoT Systems: Hiding Information in Interference. IEEE Wireless Communications 25 (6), 46–52.

Liu, Z., Zhu, B., Xie, Y., Ma, K., and Guan, X. 2024. UAV-Aided Secure Communication With Imperfect Eavesdropper Location: Robust Design for Jamming Power and Trajectory. IEEE Transactions on Vehicular Technology 73 (5), 7276–7286.

Mei, W., Zheng, B., You, C., and Zhang, R. 2022. Intelligent Reflecting Surface-Aided Wireless Networks: From Single-Reflection to Multireflection Design and Optimization. Proceedings of the IEEE 110 (9), 1380–1400.

Mozaffari, M., Lin, X., and Hayes, S. 2021. Toward 6G with Connected Sky: UAVs and Beyond. IEEE Communications Magazine 59 (12), 74–80.

Nimi, T. and Babu, A. V. 2024. Full-Duplex Cooperative NOMA Network With Multiple Eavesdroppers and Non-Ideal System Imperfections: Analysis of Physical Layer Security and Validation Using Deep Learning. IEEE Transactions on Vehicular Technology 73 (11), 17192–17208. DOI: 10.1109/TVT.2024.3427331.

Ouyang, J., Ni, S., Xu, B., Lin, M., and Zhu, W.-P. 2022. Robust Secure Energy Efficient Beamforming for mmWave UAV Communications With Jittering. IEEE Communications Letters 26 (7), 1638–1642.

Pang, X., Zhao, N., Tang, J., Wu, C., Niyato, D., and Wong, K.-K. 2022. IRS-Assisted Secure UAV Transmission via Joint Trajectory and Beamforming Design. IEEE Transactions on Communications 70 (2), 1140–1152.

Papa, A., Mankowski, J. von, Vijayaraghavan, H., Mafakheri, B., Goratti, L., and Kellerer, W. 2024. Enabling 6G Applications in the Sky: Aeronautical Federation Framework. IEEE Network 38 (1), 254–261.

Rao, H., Xiao, S., Yan, S., Wang, J., and Tang, W. 2022. Optimal Geometric Solutions to UAV-Enabled Covert Communications in Line-of-Sight Scenarios. IEEE Transactions on Wireless Communications 21 (12), 10633–10647.

Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., De Silva, P., Tufvesson, F., Benjebbour, A., and Wunder, G. 2017. 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice. IEEE Journal on Selected Areas in Communications 35 (6), 1201–1221.

Shannon, C. E. 1949. Communication theory of secrecy systems. Bell System Technical Journal 28 (4), 656–715.

Simmons, G. J. 1984. The prisoners' problem and the subliminal channel. In Advances in Cryptology: Proceedings of Crypto 83. Springer, 51–67.

Song, C., Han, B., Ji, X., Li, Y., and Su, J. 2024. AI-Driven Multipath Transmission: Empowering UAV-Based Live Streaming. IEEE Network 38 (2), 202–210.

Sun, L. and Du, Q. 2017. Physical layer security with its applications in 5G networks: A review. China Communications 14 (12), 1–14.

Sun, R., Yang, B., Ma, S., Shen, Y., and Jiang, X. 2021. Covert Rate Maximization in Wireless Full-Duplex Relaying Systems With Power Control. IEEE Transactions on Communications 69 (9), 6198–6212.

Trappe, W. 2015. The challenges facing physical layer security. IEEE Communications Magazine 53 (6), 16–20.

Wang, C., Li, Z., Shi, J., and Ng, D. W. K. 2021. Intelligent Reflecting Surface-Assisted Multi-Antenna Covert Communications: Joint Active and Passive Beamforming Optimization. IEEE Transactions on Communications 69 (6), 3984–4000.

Wang, D., Zheng, Z., He, G., Qi, P., Zhao, Y., and Li, Z. 2021. Resource Allocation for Covert Wireless Transmission in UAV Communication Networks. In 2021 IEEE Global Communications Conference (GLOBECOM), 01–06.

Wang, D., Bai, B., Zhao, W., and Han, Z. 2019. A Survey of Optimization Approaches for Wireless Physical Layer Security. IEEE Communications Surveys & Tutorials 21 (2), 1878–1911.

Wang, H., Wang, J., Chen, J., Gong, Y., and Ding, G. 2018. Network-connected UAV communications: Potentials and challenges. China Communications 15 (12), 111–121.

Wang, H.-M., Zhang, Y., Zhang, X., and Li, Z. 2020. Secrecy and Covert Communications Against UAV Surveillance via Multi-Hop Networks. IEEE Transactions on Communications 68 (1), 389–401.

Wang, J., Wang, X., Gao, R., Lei, C., Feng, W., Ge, N., Jin, S., and Quek, T. Q. S. 2022. Physical layer security for UAV communications: A comprehensive survey. China Communications 19 (9), 77–115.

Wang, L. 2021. Covert Communication Over the Poisson Channel. IEEE Journal on Selected Areas in Information Theory 2 (1), 23–31.

Wang, T., Pang, X., Liu, M., Zhao, N., Nallanathan, A., and Wang, X. 2024. Offline-Online Design for Energy-Efficient IRS-Aided UAV Communications. IEEE Transactions on Vehicular Technology 73 (2), 2942–2947.

Wang, X., Du, H., Gao, Y., Zhang, J., Niyato, D., and Letaief, K. B. 2024. Secure Body-Centric Internet of Things Networks: Physical Layer Security vs Covert Communication. IEEE Transactions on Wireless Communications 23 (10), 12731–12748.

Wei, W., Pang, X., Tang, J., Zhao, N., Wang, X., and Nallanathan, A. 2023. Secure Transmission Design for Aerial IRS Assisted Wireless Networks. IEEE Transactions on Communications 71 (6), 3528–3540.

Wilson, A. N., Kumar, A., Jha, A., and Cenkeramaddi, L. R. 2022. Embedded Sensors, Communication Technologies, Computing Platforms and Machine Learning for UAVs: A Review. IEEE Sensors Journal 22 (3), 1807–1826.

Wu, Q., Liu, L., and Zhang, R. 2019. Fundamental Trade-offs in Communication and Trajectory Design for UAV-Enabled Wireless Network. IEEE Wireless Communications 26 (1), 36–44.

Wu, Q. and Zhang, R. 2018. Common Throughput Maximization in UAV-Enabled OFDMA Systems With Delay Consideration. IEEE Transactions on Communications 66 (12), 6614–6627.

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

Yan, S., Hanly, S. V., and Collings, I. B. 2021. Optimal Transmit Power and Flying Location for UAV Covert Wireless Communications. IEEE Journal on Selected Areas in Communications 39 (11), 3321–3333.

Yang, W., Lu, X., Yan, S., Shu, F., and Li, Z. 2021. Age of Information for Short-Packet Covert Communication. IEEE Wireless Communications Letters 10 (9), 1890–1894.

Ye, R., Peng, Y., Al-Hazemi, F., and Boutaba, R. 2024. A Robust Cooperative Jamming Scheme for Secure UAV Communication via Intelligent Reflecting Surface. IEEE Transactions on Communications 72 (2), 1005–1019.

Zeng, Y., Xu, X., and Zhang, R. 2018. Trajectory Design for Completion Time Minimization in UAV-Enabled Multicasting. IEEE Transactions on Wireless Communications 17 (4), 2233–2246.

Zeng, Y., Zhang, R., and Lim, T. J. 2016a. Throughput Maximization for UAV-Enabled Mobile Relaying Systems. IEEE Transactions on Communications 64 (12), 4983–4996.

Zeng, Y., Zhang, R., and Lim, T. J. 2016b. Wireless communications with unmanned aerial vehicles: opportunities and challenges. IEEE Communications Magazine 54 (5), 36–42.

Zhang, Q., Saad, W., and Bennis, M. 2019. Reflections in the Sky: Millimeter Wave Communication with UAV-Carried Intelligent Reflectors. In 2019 IEEE Global Communications Conference (GLOBECOM), 1–6.

Zhang, S., Zhang, H., Di, B., and Song, L. 2019. Cellular Cooperative Unmanned Aerial Vehicle Networks With Sense-and-Send Protocol. IEEE Internet of Things Journal 6 (2), 1754–1767.

Zhang, S. and Zhang, R. 2020. Capacity Characterization for Intelligent Reflecting Surface Aided MIMO Communication. IEEE Journal on Selected Areas in Communications 38 (8), 1823–1838.

Zhang, W., Chen, J., Kuo, Y., and Zhou, Y. 2019. Artificial-Noise-Aided Optimal Beamforming in Layered Physical Layer Security. IEEE Communications Letters 23 (1), 72–75.

Zhao, N., Li, Y., Zhang, S., Chen, Y., Lu, W., Wang, J., and Wang, X. 2020. Security Enhancement for NOMA-UAV Networks. IEEE Transactions on Vehicular Technology 69 (4), 3994–4005.

Zheng, T.-X., Wang, H.-M., Ng, D. W. K., and Yuan, J. 2019. Multi-Antenna Covert Communications in Random Wireless Networks. IEEE Transactions on Wireless Communications 18 (3), 1974–1987.

Zheng, T., Chen, X., Wen, Y., Zhang, N., Ng, D. W. K., and Al-Dhahir, N. 2024. Secure Offloading in NOMA-Enabled Multi-Access Edge Computing Networks. IEEE Transactions on Communications 72 (4), 2152–2165.

Zhou, X., Yan, S., Hu, J., Sun, J., Li, J., and Shu, F. 2019. Joint Optimization of a UAV’s Trajectory and Transmit Power for Covert Communications. IEEE Transactions on Signal Processing 67 (16), 4276–4290.

Zhou, Y., Yeoh, P. L., Chen, H., Li, Y., Schober, R., Zhuo, L., and Vucetic, B. 2018. Improving Physical Layer Security via a UAV Friendly Jammer for Unknown Eavesdropper Location. IEEE Transactions on Vehicular Technology 67 (11), 11280–11284.

ORIGINAL PAPERS

I

UAV-AIDED SECURE SHORT-PACKET DATA COLLECTION AND TRANSMISSION

by

Xinying Chen, Nan Zhao, Zheng Chang, Timo Hämäläinen, and Xianbin Wang
2023

IEEE Transactions on Communications, 71(4), 2475–2486,
https://www.doi.org/10.1109/TCOMM.2023.3244954

UAV-Aided Secure Short-Packet Data Collection and Transmission

Xinying Chen, Nan Zhao, *Senior Member, IEEE*, Zheng Chang, *Senior Member, IEEE*, Timo Hämäläinen, *Senior Member, IEEE*, and Xianbin Wang, *Fellow, IEEE*

***Abstract*— Benefiting from the deployment flexibility and the line-of-sight (LoS) channel conditions, unmanned aerial vehicle (UAV) has gained tremendous attention in data collection for wireless sensor networks. However, the high-quality air-ground channels also pose significant threats to the security of UAV-aided wireless networks. In this paper, we propose a short-packet secure UAV-aided data collection and transmission scheme to guarantee the freshness and security of the transmission from the sensors to the remote ground base station (BS). First, during the data collection phase, the trajectory, the flight duration, and the user scheduling are jointly optimized with the objective of maximizing the energy efficiency (EE). To solve the non-convex EE maximization problem, we adopt the first-order Taylor expansion to convert it into two convex subproblems, which are then solved via successive convex approximation. Furthermore, we consider the maximum rate of transmission in the UAV data transmission phase to achieve a maximum secrecy rate. The transmit power and the blocklength of UAV-to-BS transmission are jointly optimized subject to the constraints of eavesdropping rate and outage probability. Simulation results are provided to validate the effectiveness of the proposed scheme.**

***Index Terms*— Data collection, finite blocklength, resource allocation, secure transmission, short-packet transmission, unmanned aerial vehicle.**

I. Introduction

CONSIDERED as a flexible network entity in the beyond fifth generation and the sixth generation (B5G/6G) mobile communications [2], [3], the unmanned aerial vehicle (UAV) aided networks have recently attracted significant attention. The benefits of high mobility, low cost, easy deployment, and line-of-sight (LoS) links allow UAVs to be utilized in different scenarios to improve the wireless network performance [4], [5]. With these advantages, UAVs can be deployed as high-mobility users, fast-configured base stations (BSs), or long-range relays [6]. Specifically, the flexibility of UAV enables efficient data collection for B5G/6G Internet of things (IoTs) [7], [8], [9], which can tackle the challenge of collecting data from remote or extreme environments. Instead of exhaustively collecting data from each user randomly, the energy efficiency (EE) of UAV can be improved via the proper design of trajectory and user scheduling [10], [11], [12]. Wang et al. proposed an efficient data collecting scheme for a non-orthogonal multiple access (NOMA) UAV network to minimize the flight duration in [10] via jointly designing the trajectory, scheduling, and transmit power. To keep the data freshness of wireless sensor networks, Liu et al. proposed an efficient data collection scheme in [11] to minimize the age of information of all the sensors via properly designing the trajectory of UAV collector. In [12], an energy harvesting wireless sensor scheme was studied by Liu et al., where the UAV transfers energy to support the sensor nodes and minimizes the outage probability of data collection.

However, information security threat resulting from the LoS channels cannot be ignored during the UAV data collection process [13], [14], [15], [16]. In [13], Zhang et al. proposed two secure schemes to enable the information security via cooperative dual UAVs with the energy limit of UAV considered. To preserve the privacy of devices, Yang et al. proposed a federal learning based scheme for UAV-assisted networks in [14] to provide reliable and efficient data collection. In [15], Xu et al. utilized blockchain in a UAV-assisted data collection IoT network to guarantee the information security and improve the EE. In [16], Xu et al. investigated the secure transmission in a dual UAV mobile edge computing system under both time division multiple access and NOMA. To tackle the security challenges, many studies have been focused on improving the security in UAV-related systems [17], [18], [19], [20]. In [17], Chen et al. proposed a resource allocation scheme to realize the secure transmission in circular-trajectory UAV-NOMA networks. Wang et al. introduced the simultaneous wireless information and power transfer into NOMA-UAV networks in [18] to provide secure transmission while guaranteeing the energy supplement for passive receivers. In [19], Zhong et al.

Manuscript received 14 May 2022; revised 13 November 2022; accepted 5 February 2023. Date of publication 14 February 2023; date of current version 18 April 2023. The work of Nan Zhao is supported in part by the National Natural Science Foundation of China (NSFC) under Grant 62271099 and 62071105. An earlier version of this paper was presented in part at the IEEE GLOBECOM 2022 [DOI: 10.1109/GLOBECOM48099.2022.10000768]. The associate editor coordinating the review of this article and approving it for publication was J. Liu. *(Corresponding author: Zheng Chang.)*

Xinying Chen is with the Faculty of Information Technology, University of Jyväskylä, 40014 Jyväskylä, Finland, and also with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China (e-mail: cxy@mail.dlut.edu.cn).

Nan Zhao is with the School of Information and Communication Engineering, Dalian University of Technology, Dalian 116024, China (e-mail: zhaonan@dlut.edu.cn).

Zheng Chang is with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610051, China, and also with the Faculty of Information Technology, University of Jyväskylä, 40014 Jyväskylä, Finland (e-mail: zheng.chang@jyu.fi).

Timo Hämäläinen is with the Faculty of Information Technology, University of Jyväskylä, 40014 Jyväskylä, Finland (e-mail: timo.t.hamalainen@jyu.fi).

Xianbin Wang is with the Department of Electrical and Computer Engineering, Western University, London, ON N6A 5B9, Canada (e-mail: xianbin.wang@uwo.ca).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCOMM.2023.3244954.

Digital Object Identifier 10.1109/TCOMM.2023.3244954

leveraged the power and trajectory control over both the UAV transmitter and a friendly UAV jammer to avoid being eavesdropped. Kang et al. integrated the blockchain into UAV communications in [20] to share data securely.

In addition, because of the short packets used in the UAV data collection, the conventional performance analysis based on infinite blocklength cannot characterize the system accurately [21], [22]. This motivates new research to investigate the performance of short-packet transmission, which mainly focuses on improving the reliability and reducing the time delay [23], [24]. When evaluating the performance in typical wireless communications, the infinite blocklength (or sufficient large blocklength) is commonly considered, where the critical performance parameter can be accurately modeled. However, data transmission in IoT applications usually consists of a large amount of time-intolerant and error-intolerant information, where the length of message is short. Thus, applying short packets to UAV-related communications could make the information transmission more effective [25], [26], [27]. In [25], Ranjha and Kaddoum utilized the UAV and reconfigurable intelligent surface to achieve a short-packet IoTs system aiming to minimize the decoding error rate. Ren et al. studied the short-packet communication in UAV-assisted networks [26], where the achievable finite blocklength data rate is investigated under three-dimension channel models. In [27], the blocklength and hovering location of UAV relay were optimized by Pan et al. to minimize the decoding error probability at the receiver.

As observed, using finite blocklength to explore the physical layer security of UAV-aided networks is still under investigation, and the security for IoT networks is also of critical importance. The finite-blocklength security for UAV-assisted data collection and transmission has not been well studied in the aforementioned literature. Thus, in this paper, we propose a short-packet secure UAV data collection scheme to guarantee the information secrecy and freshness. We summarize the main contribution of this paper as follows.

- To our best knowledge, this is the first work considering the secure transmission of short packets for UAV-assisted data collection. Specifically, user scheduling, flight duration, and trajectory are jointly designed to achieve higher EE in the data collection via UAV. Then, in the data transmission to BS, the finite blocklength and transmit power of UAV are jointly optimized to maximize the secrecy rate while restricting the eavesdropping rate and the secrecy outage probability.
- During the first phase of data collection, the trajectory and user scheduling problem is formulated as non-convex, which cannot be solved directly. Thus, we utilize the successive convex approximation (SCA) and first-order Taylor expansion to transfer the non-convex problem into two convex subproblems and solve them iteratively to derive the optimal solution for higher EE.
- We jointly analyze the monotonicity of the lower bound of secrecy rate, the eavesdropping rate and the outage probability to derive the optimal transmit power and the optimal blocklength for the second secure short-packet transmission phase. Without awareness of the channel state information of the eavesdropper, we perform statistical analysis on the eavesdropping rate to derive the optimal solution for the secure transmission.

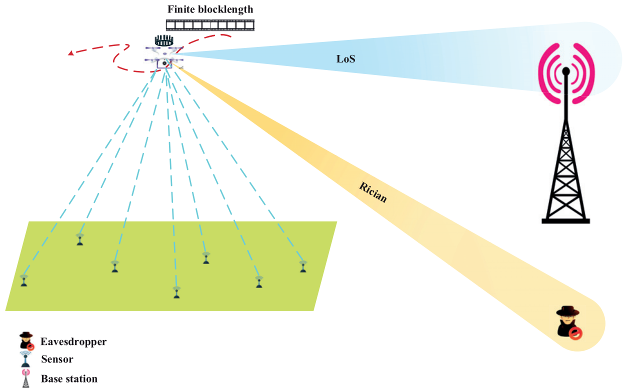


Fig. 1. UAV-assisted short-packet data collection and secure transmission.

The rest of this paper is organized as follows. In Section II, we describe the system model. The EE maximization problem is formulated and optimized in Section III. Then, the secrecy rate maximization for short-packet secure transmission is given and solved in Section IV. We present the simulation results in Section V, and conclude the work in Section VI.

Notation: Boldface lowercase and uppercase letters identify vectors and matrices, respectively. $\mathbb{C}^{M\times N}$ represents the $M \times N$ complex matrix. $\mathbf{a}^H$ and $\|\mathbf{a}\|$ are the conjugate transpose and Euclidean norm of vector $\mathbf{a}$, respectively. $Pr\left\{x\right\}$ and $E\left[x\right]$ are the probability and the expectation of the random variable x. $\mathcal{CN}(\mu,\sigma^2)$ denotes the complex Gaussian distribution with mean μ and variance σ^2. $I_0(*)$ represents the first-kind and the zero-order Bessel function. $\chi^2(k,\lambda)$ represents the non-central chi-square distribution with k degrees of freedom and the non-centrality parameter of λ.

II. System Model

In the network, a UAV collects data from randomly distributed sensors, and then transmits them to the BS, as shown in Fig. 1. The data transmission consists of two parts, namely the data collection phase and the secure transmission phase. The sensors, the BS, and the eavesdropper are all assumed to equip with a single antenna. The UAV is assumed to have a single receiving antenna and multiple transmitting antennas. In the data collection phase, the UAV flies according to its designed trajectory $\mathbf{w}$ and collects data from the sensors according to their scheduling variable $t_i[n]$. After data collection, the UAV transmits the received data via precoding to the legitimate BS while avoiding being eavesdropped by the eavesdropper. The distributed area of sensors is assumed to be much smaller compared with the distance between the UAV and BS, which leads to a tiny impact of the UAV trajectory on the transmission performance towards the BS in the second phase. Therefore, in the proposed scheme, we first design the trajectory of UAV, and then characterize the secure transmission to the BS, which is described as follows.

A. Data Collection Phase

There are S sensors randomly distributed in the square area with the length of each side as L, where the location of the i-th sensor can be expressed as $L_i(x_i, y_i, 0) \in R^{1\times 3}$, $\forall i \in \{1, \cdots, S\}$. During the data collection, the UAV flies over the area with a fixed height H. The data collection phase is conducted for a duration T, which is equally divided into N slots. Therefore, the duration of each time slot can be expressed as $\Delta t = \frac{T}{N}$. Then, the trajectory of UAV can be simplified as $\mathbf{w} = [w[1], \cdots, w[n], \cdots, w[N]]$, where $w[n] = (x[n], y[n], H) \in R^{1\times 3}, \forall n = \{1, \cdots, N\}$ is the location of UAV in the n-th slot. Besides, the UAV can adjust its trajectory $\mathbf{w}$ and speed $v \leq V_{max}$ to achieve better transmission performance, where V_{max} is the maximum achievable speed of UAV. Assume that the UAV returns to its original location after finishing the data collection within T, and we have

$$w[1] = w[N]. \tag{1}$$

In addition, the duration of each slot is small. Thus, $\Delta_{uav}[n] = ||w[n]-w[n-1]||$ can be approximately unchanged compared to H, which is expressed as

$$\Delta_{uav}[n] \leq \Delta t V_{max}, \quad n = 2, \cdots, N, \tag{2}$$

and

$$\Delta_{uav}[n] \leq \theta H, \quad n = 2, \cdots, N, \tag{3}$$

where $0 < \theta \ll 1$.

In the data collection, the i-th sensor should transmit at least B_i bits to the UAV during its assigned time slots. Consider that the UAV adopts time-division multiple access, which indicates that the UAV only serves one user within each time slot. Define a boolean symbol $t_i[n]$, $\forall i \in \{1, \cdots, S\}$ and $\forall n \in \{1, \cdots, N\}$, to describe the scheduling variable for all sensors, where $t_i[n] = 1$ represents that the i-th sensor can send data to the UAV during the n-th slot and $t_i[n] = 0$ indicates that the i-th sensor keeps silence. The scheduling variable $t_i[n]$ can be described as

$$t_i[n] = \{0, 1\}, \quad \forall i \in \{1, \cdots, S\}, \quad \forall n \in \{1, \cdots, N\}, \tag{4}$$

and

$$\sum_{i=1}^{S} t_i[n] \leq 1, \quad \forall n \in \{1, \cdots, N\}. \tag{5}$$

Assume that the channel coefficient $g_{s_i u}$ between the i-th sensor and UAV follows the large-scale LoS channel, which can be described as

$$g_{s_i u} = \sqrt{\frac{\rho_0}{d_{s_i u}^{\alpha}}}, \quad \forall i \in \{1, \cdots, S\}, \tag{6}$$

where ρ_0 is the path loss reference at 1 m for LoS, and α represents the path loss exponent. $d_{s_i u}$ denotes the distance between the i-th sensor and UAV, which can be denoted as

$$d_{s_i u} = ||L_i - w[n]||, \quad \forall i \in \{1, \cdots, S\}. \tag{7}$$

The blocklength of each sensor is assumed to be N_s. Apart from the traditional data rate in an infinite system, the capacity should take the decoding error probability ϵ_s at the UAV into consideration. Thus, the transmission rate of the i-th sensor during the n-th slot can be described as

$$R_i[n] = t_i[n] \log_2 \left[(1 + \gamma_i[n]) - \sqrt{\frac{V_i[n]}{N_s}} \frac{Q^{-1}(\epsilon_s)}{\ln 2} \right], \tag{8}$$

where $Q^{-1}(*)$ represents the inverse Q-function. The signal-to-noise ratio (SNR) $\gamma_i[n]$ can be described as

$$\gamma_i[n] = \frac{P_s \rho_0}{d_{s_i u}^{\alpha} \sigma^2}, \tag{9}$$

where σ^2 represents the variance of the Gaussian noise and P_s is the transmit power of each sensor. In addition, $V_i[n]$ in (8) can be defined as

$$V_i[n] = 1 - (1 + \gamma_i[n])^{-2}. \tag{10}$$

Thus, the total transmitted data D_{sen} from the distributed sensors within the whole duration T can be defined as

$$D_{sen} = \sum_{i=1}^{S} \sum_{n=1}^{N} R_i[n] \Delta t. \tag{11}$$

The UAV is assumed to be rotary-wing, and its propulsion power is much higher than the communication part. Thus, we only consider the propulsion energy in the trajectory design when maximizing the EE. The power consumed by the UAV during the n-th time slot to support flying can be described as (12), shown at the bottom of the next page, where its parameters can be referred to Table I.

TABLE I
PARAMETER DEFINITIONS IN (12)

Parameter	Definition
P_{bld}	Profile power of blades
v_t	Tip speed of rotor blades
r_{drag}	Fuselage drag ratio
ρ_{air}	Density of air
h_{rtor}	Solidity of rotor
S_{rtor}	Disc area of rotor
P_{ind}	Induced power when $\frac{\Delta_{uav}[n]}{\Delta t} = 0$
$\bar{v}$	Mean induced speed of motor

Based on (12), the total propulsion energy consumption E_{uav} of UAV can be calculated as

$$E_{uav} = \sum_{n=1}^{N} P_{uav}[n] \Delta t. \tag{13}$$

Then, the EE r_{tc} can be defined as

$$r_{tc} = \frac{D_{sen}}{E_{uav}}. \tag{14}$$

We also constrain the consumed energy of the i-th sensor to be smaller than its total energy E_i as

$$\sum_{n=1}^{N} t_i[n] P_s \Delta t \leq E_i, \tag{15}$$

and the transmitted data of the i-th sensor to be no smaller than its sensed data B_i as

$$\sum_{n=1}^{N} R_i[n]\Delta t \geq B_i. \tag{16}$$

B. Secure Short-Packet Transmission Phase

After receiving the data from the sensors, the UAV transmits them to the BS with M antennas in blocklength N_u, where the BS locates at $L_b(x_b, y_b, z_b) \in R^{1\times 3}$. Assume that the channel coefficient $\mathbf{g}_b[n]$ in the n-th time slot between the UAV and BS follows the large-scale LoS path loss, which can be expressed as

$$\mathbf{g}_b[n] = \sqrt{\frac{\rho_0}{d_b[n]^\alpha}}\mathbf{h}_b[n], \tag{17}$$

where $d_b[n] \triangleq ||L_b - w[n]||, \forall n \in \{1, \cdots, N\}$, is the distance between the UAV and BS at the n-th slot, and $\mathbf{h}_b[n] \triangleq \{h_{b_1}[n], \cdots, h_{b_M}[n]\} \in \mathbb{C}^{1\times M}$ represents the LoS channel components between the M antennas of UAV and the BS, where $\forall |h_{b_i}[n]| = 1$ for $i \in \{1, \cdots, M\}$ is the channel coefficient for the i-th antenna.

In addition, there exists a terrestrial eavesdropper located near the BS, and the UAV does not know its accurate location. Thus, we analyze the secure transmission under the worst situation, where the closest location of the eavesdropper to the UAV is estimated at $L_e(x_e, y_e, 0) \in R^{1\times 3}$. Assume that the channel coefficient $\mathbf{g}_e[n]$ during each time slot between the UAV and eavesdropper follows a large-scale path loss and a small-scale Rician fading as

$$\mathbf{g}_e[n] = \sqrt{\frac{\rho_0}{d_e[n]^\alpha}}\left(c_L\mathbf{h}_{eL}[n] + c_N\mathbf{h}_{eN}[n]\right) = \sqrt{\frac{\rho_0}{d_e[n]^\alpha}}\mathbf{h}_e[n], \tag{18}$$

which cannot be obtained by the UAV. $d_e[n] \triangleq ||L_e - w[n]||, \forall n \in \{1, \cdots, N\}$, is the distance between the UAV and eavesdropper during the n-th time slot. $c_L = \sqrt{\frac{K}{1+K}}$ and $c_N = \sqrt{\frac{1}{1+K}}$ are the LoS and non-LoS (NLoS) channel coefficients of Rician fading, where K is the Rician factor. The LoS channel component $\mathbf{h}_{eL}[n] \triangleq \{h_{eL_1}[n], \cdots, h_{eL_M}[n]\} \in \mathbb{C}^{1\times M}$ follows $|h_{eL_i}[n]| = 1, \forall i \in \{1, \cdots, M\}$, and the Rayleigh fading component $\mathbf{h}_{eN}[n] \triangleq \{h_{eN_1}[n], \cdots, h_{eN_M}[n]\} \in \mathbb{C}^{1\times M}$ satisfies $h_{eN_i}[n] \sim \mathcal{CN}(0, 1), \forall i \in \{1, \cdots, M\}$.

Assume that the UAV performs the maximum ratio transmission (MRT) via precoding towards the BS, where the precoding vector $\mathbf{u}[n]$ during each slot at the UAV can be described as

$$\mathbf{u}[n] = \frac{\mathbf{h}_b^H[n]}{||\mathbf{h}_b[n]||}. \tag{19}$$

The UAV precodes the transmitted signal of blocklength N_u with transmit power P_a, where the received SNR at the BS during the n-th slot can be described as

$$\gamma_b[n] = \frac{P_a\rho_0|\mathbf{h}_b[n]\mathbf{u}[n]|^2}{\sigma^2 d_b[n]^\alpha} = \frac{P_a\rho_0 M}{\sigma^2 d_b[n]^\alpha}. \tag{20}$$

Similar to the SNR at the BS, the SNR at the malicious eavesdropper can be described as

$$\gamma_e[n] = \frac{P_a\rho_0|\mathbf{h}_e[n]\mathbf{u}[n]|^2}{\sigma^2 d_e[n]^\alpha}. \tag{21}$$

Similar to (8), the channel capacities from the UAV to both the BS and eavesdropper are smaller than the traditional infinite blocklength transmission. The maximum achievable transmission rate $R_b[n]$ of each slot can be expressed as

$$R_b[n] = \log_2\left(1 + \gamma_b[n]\right) - \sqrt{\frac{\gamma_b[n](\gamma_b[n]+2)}{N_u(\gamma_b[n]+1)^2}}\frac{Q^{-1}(\epsilon)}{\ln 2}, \tag{22}$$

where $n \in \{1, \cdots, N\}$. ϵ is the maximum allowed error decoding probability. The maximum achievable eavesdropping rate at the eavesdropper can be demonstrated as

$$R_e[n] = \log_2\left(1 + \gamma_e[n]\right) - \sqrt{\frac{\gamma_e[n](\gamma_e[n]+2)}{N_u(\gamma_e[n]+1)^2}}\frac{Q^{-1}(\delta_e)}{\ln 2}, \tag{23}$$

where $n \in \{1, \cdots, N\}$, and δ_e is the information leakage probability.

Based on [28], the lower bound to the secrecy rate $R_s[n]$ during each time slot can be described as (24), shown at the bottom of the next page.

The secure transmission outage occurs when the transmission rate $R_0[n]$ of the n-th slot is larger than the secrecy rate capacity. To guarantee the security, we define the secrecy outage probability $p_{out}[n]$ in each time slot as

$$p_{out}[n] = Pr\left\{R_s[n] \leq R_0[n]\right\}, \tag{25}$$

In the following, the EE maximization for data collection is investigated in Section III, while the secrecy rate in short-packet transmission is maximized in Section IV.

III. Energy Efficiency Maximization

Owning to the energy limitation, the maximum flying duration of UAV is limited. To balance between the flight duration of UAV and the amount of collected data, we optimize the trajectory of UAV and the scheduling variable of each sensor to achieve higher EE for data collection in this section.

$$P_{uav}[n] = P_{bld}\left(1 + \frac{3\Delta_{uav}[n]^2}{v_t^2\Delta t^2}\right) + \frac{1}{2}r_{drag}\rho_{air}h_{rtor}S_{rtor}\frac{\Delta_{uav}[n]^3}{\Delta t^3} + P_{ind}\left(\sqrt{1 + \frac{\Delta_{uav}[n]^4}{4\bar{v}^4\Delta t^4}} - \frac{\Delta_{uav}[n]^2}{2\bar{v}^2\Delta t^2}\right)^{\frac{1}{2}}. \tag{12}$$

A. Problem Formulation

The trajectory $\mathbf{w}$ of UAV and the scheduling vector $\mathbf{t} \triangleq \{t_i[n], \forall i = \{1, \cdots, S\}, \forall n = \{1, \cdots, N\}\}$ are optimized. In addition, we also optimize the total flight duration of UAV to achieve a higher EE. By optimizing the trajectory $\mathbf{w}$ of UAV, the scheduling vector $\mathbf{t}$, and the flight duration T, we aim at maximizing EE r_{tc}. The optimization problem can be formulated as

$$\begin{aligned}
\textbf{P1:} \quad & \max_{\mathbf{w},\mathbf{t},T} \; r_{tc} && \text{(26a)}\\
& s.t. \; w[1] = w[N], && \text{(26b)}\\
& \quad \Delta_{uav}[n] \le \Delta t V_{max}, && \text{(26c)}\\
& \quad \Delta_{uav}[n] \le \theta H, && \text{(26d)}\\
& \quad \sum_{n=1}^{N} t_i[n] P_s \Delta t \le E_i, && \text{(26e)}\\
& \quad \sum_{n=1}^{N} R_i[n] \Delta t \ge B_i, && \text{(26f)}\\
& \quad \sum_{i=1}^{S} t_i[n] \le 1, && \text{(26g)}\\
& \quad 0 \le t_i[n] \le 1, && \text{(26h)}
\end{aligned}$$

which has a non-convex structure and is difficult to solve. Thus, we propose an iterative algorithm to solve the proposed problem via SCA. We first optimize the scheduling vector $\mathbf{t}$ and flight duration T with a given trajectory $\mathbf{w}$. Then, with the optimized $\mathbf{t}$ and T, the trajectory $\mathbf{w}$ can be updated.

B. Optimization of Scheduling and Flight Duration

According to the definition of Δt, we reformulate P1 as the optimization of Δt instead of T, since r_{tc} is the expression of Δt. Thus, for a given trajectory $\mathbf{w}$ of UAV, the problem P1 can be simplified as

$$\begin{aligned}
\textbf{P1.1:} \quad & \max_{\mathbf{t},\Delta t} \; \frac{\sum_{i=1}^{S} \sum_{n=1}^{N} R_i[n] \Delta t}{E_{ucvx}(\Delta t) + E_{uNcvx}(\Delta t)} && \text{(27a)}\\
& s.t. \; \Delta_{uav}[n] \le \Delta t V_{max}, && \text{(27b)}\\
& \quad \sum_{n=1}^{N} t_i[n] P_s \Delta t \le E_i, && \text{(27c)}\\
& \quad \sum_{n=1}^{N} R_i[n] \Delta t \ge B_i, && \text{(27d)}\\
& \quad \sum_{i=1}^{S} t_i[n] \le 1, && \text{(27e)}\\
& \quad 0 \le t_i[n] \le 1, && \text{(27f)}
\end{aligned}$$

where $E_{uav} = E_{ucvx}(\Delta t) + E_{uNcvx}(\Delta t)$. $E_{ucvx}(\Delta t)$ is the convex component in E_{uav} with respect to Δt, and can be described as

$$\begin{aligned}
E_{ucvx}(\Delta t) = & \sum_{n=1}^{N} P_{bld} \left(\Delta t + \frac{3\Delta_{uav}[n]^2}{v_t^2 \Delta t} \right)\\
& + \frac{1}{2} r_{drag} \rho_{air} h_{rtor} S_{rtor} \sum_{n=1}^{N} \frac{\Delta_{uav}[n]^3}{\Delta t^2}. \qquad (28)
\end{aligned}$$

$E_{uNcvx}(\Delta t)$ is the non-convex component in E_{uav} with respect to Δt, and can be described as

$$E_{uNcvx}(\Delta t) = P_{ind} \sum_{n=1}^{N} \left(\sqrt{\Delta t^4 + \frac{\Delta_{uav}[n]^4}{4\bar{v}^4}} - \frac{\Delta_{uav}[n]^2}{2\bar{v}^2} \right)^{\frac{1}{2}}. \qquad (29)$$

From (27), we can see that $\sum_{i=1}^{S} \sum_{n=1}^{N} R_i[n] \Delta t$ is non-concave and $E_{uNcvx}(\Delta t)$ is non-convex, which makes P1.1 mathematically unsolvable. Therefore, we introduce an auxiliary parameter $R_N[i]$ as

$$R_N[i]^2 = \sum_{n=1}^{N} R_i[n] \Delta t, \qquad (30)$$

to transfer the non-concave (27a) into a different version, the numerator part of which can be changed into

$$D_{sen} = \sum_{i=1}^{S} R_N[i]^2. \qquad (31)$$

In addition, we introduce another auxiliary parameter $z[n]$ to upper bound a complex component in E_{uNcvx} as

$$z[n]^2 \ge \sqrt{\Delta t^4 + \frac{\Delta_{uav}[n]^4}{4\bar{v}^4}} - \frac{\Delta_{uav}^2}{2\bar{v}^2}. \qquad (32)$$

By performing the simple algebra transformation on (32), we have

$$\Delta t^4 \le z[n]^4 + \frac{\Delta_{uav}[n]^2}{\bar{v}^2} z[n]^2, \qquad (33)$$

which changes $E_{uNcvx}(\Delta t)$ in (29) into

$$E_{uNcvx}(\Delta t) \le P_{ind} \sum_{n=1}^{N} z[n]. \qquad (34)$$

Then, P1.1 can be transformed as

$$\begin{aligned}
\textbf{P1.1.a:} \quad & \max_{\mathbf{t},\Delta t, R_N[i], z[n]} \; \frac{\sum_{i=1}^{S} R_N[i]^2}{E_{ucvx}(\Delta t) + P_{ind} \sum_{n=1}^{N} z[n]} && \text{(35a)}\\
& s.t. \; (27b), (27e), (27f), && \text{(35b)}\\
& \quad \sum_{n=1}^{N} t_i[n] P_s \le \frac{E_i}{\Delta t}, && \text{(35c)}\\
& \quad R_N[i]^2 \ge B_i, && \text{(35d)}
\end{aligned}$$

$$R_s[n] = \log_2(1 + \gamma_b[n]) - \log_2(1 + \gamma_e[n]) - \sqrt{\frac{\gamma_b[n](\gamma_b[n] + 2)}{(\gamma_b[n] + 1)^2}} \frac{Q^{-1}(\epsilon)}{\ln 2 \sqrt{N_u}} - \sqrt{\frac{\gamma_e[n](\gamma_e[n] + 2)}{(\gamma_e[n] + 1)^2}} \frac{Q^{-1}(\delta_e)}{\ln 2 \sqrt{N_u}}. \qquad (24)$$

$$R_N[i]^2 \leq \sum_{n=1}^{N} R_i[n]\Delta t, \tag{35e}$$

$$\Delta t^4 \leq z[n]^4 + \frac{\Delta_{uav}[n]^2}{\bar{v}^2} z[n]^2. \tag{35f}$$

To ensure that (35) is mathematically solvable, we need to change (35c) and (35e) into concave ones with respect to Δt. Also, (35d) and (35f) need to be changed into concave ones with respect to $R_N[i]$ and $z[n]$, respectively.

We apply the first-order Taylor expansion to change the above-mentioned functions into their concave versions. Then, iteratively performing SCA, the optimal values of $\mathbf{t}$, Δt, $R_N[i]$, $z[n]$ can be achieved.

The first-order Taylor expansion of (35c) with a given point $\Delta t^{(r)}$can be expressed as

$$\frac{E_i}{\Delta t} \geq E_i \left(\frac{1}{\Delta t^{(r)}} - \left(\frac{1}{\Delta t^{(r)}} \right)^2 \left(\Delta t - \Delta t^{(r)} \right) \right) \geq \sum_{n=1}^{N} t_i[n] P_s, \tag{36}$$

where $\Delta t^{(r)}$ is assumed to be the optimal value of Δt in (35) from the r-th iteration.

Similarly, (35d) can be expanded at a given point $R_N^{(r)}[i]$ as

$$R_N[i]^2 \geq R_N^{(r)}[i]^2 + 2R_N^{(r)}[i] \left(R_N[i] - R_N^{(r)}[i] \right) \geq B_i, \tag{37}$$

where $R_N^{(r)}[i]$ is assumed to be the optimal value of $R_N[i]$ in (35) from the r-th iteration.

Also, according to the hyperbolic constraint [29], we have (35e) if and only if

$$\left\| \begin{bmatrix} 2R_N[i]^2 \\ \sum_{n=1}^{N} (R_i[n] - \Delta t) \end{bmatrix} \right\| \leq \sum_{n=1}^{N} (R_i[n] - \Delta t). \tag{38}$$

We can replace (35e) with (38). The expansion of (35f) at a given point $z^{(r)}[n]$ can be changed to

$$\begin{aligned} & z[n]^4 + \frac{\Delta_{uav}[n]^2}{\bar{v}^2} z[n]^2 \\ & \geq z^{(r)}[n]^4 + 4z^{(r)}[n]^3 \left(z[n] - z^{(r)}[n] \right) \\ & \quad + \frac{\Delta_{uav}[n]^2}{\bar{v}^2} \left[z^{(r)}[n]^2 + 2\ z^{(r)}[n] \left(z[n] - z^{(r)}[n] \right) \right] \geq \Delta t^4, \end{aligned} \tag{39}$$

where $z^{(r)}[n]$ is assumed to be the optimal value of $z[n]$ in (35) from the r-th iteration.

Thus, P1.1.a can be changed into a mathematically solvable problem as

$$\textbf{P1.1.b:} \quad \max_{\mathbf{t}, \Delta t, R_N[i], z[n]} \frac{R_N^{(r)}[i]^2 + 2R_N^{(r)}[i] \left(R_N[i] - R_N^{(r)}[i] \right)}{E_{ucvx}(\Delta t) + P_{ind} \sum_{n=1}^{N} z[n]} \tag{40a}$$

$$s.t. \ (27b), (27e), (27f), \tag{40b}$$

$$E_i \left(\frac{1}{\Delta t^{(r)}} - \left(\frac{1}{\Delta t^{(r)}} \right)^2 \left(\Delta t - \Delta t^{(r)} \right) \right) \geq \sum_{n=1}^{N} t_i[n] P_s, \tag{40c}$$

$$R_N^{(r)}[i]^2 + 2R_N^{(r)}[i] \left(R_N[i] - R_N^{(r)}[i] \right) \geq B_i, \tag{40d}$$

$$R_N[i]^2 \leq \sum_{n=1}^{N} R_i[n]\Delta t, \tag{40e}$$

$$\frac{\Delta_{uav}[n]^2}{\bar{v}^2} \left[z^{(r)}[n]^2 + 2\ z^{(r)}[n] \left(z[n] - z^{(r)}[n] \right) \right] \tag{40f}$$

$$\begin{aligned} & z^{(r)}[n]^4 + 4z^{(r)}[n]^3 \left(z[n] - z^{(r)}[n] \right) \geq \Delta t^4, \\ & \left\| \begin{bmatrix} 2R_N[i]^2 \\ \sum_{n=1}^{N} (R_i[n] - \Delta t) \end{bmatrix} \right\| \leq \sum_{n=1}^{N} (R_i[n] - \Delta t), \end{aligned} \tag{40g}$$

which is convex, and can be solved by existing convex programming tools such as CVX.

C. Optimization of UAV Trajectory

Then, we optimize the trajectory $\mathbf{w}$ of UAV with the given scheduling vector $\mathbf{t}$ and flight duration T. The optimization problem can be reformulated as

$$\textbf{P1.2:} \quad \max_{\mathbf{w}} \frac{\sum_{i=1}^{S} \sum_{n=1}^{N} R_i[n]\Delta t}{E_{ucvx}(\Delta t) + E_{uNcvx}(\Delta t)} \tag{41a}$$

$$s.t. \ w[1] = w[N], \tag{41b}$$

$$\Delta_{uav}[n] \leq \Delta t V_{max}, \tag{41c}$$

$$\Delta_{uav}[n] \leq \theta H, \tag{41d}$$

$$\sum_{n=1}^{N} R_i[n]\Delta t \geq B_i, \tag{41e}$$

where the numerator of (41a) is non-concave, $E_{uNcvx}(\Delta t)$ is non-convex, and (41e) is non-concave with respect to $\mathbf{w}$. Thus, we need to transform them into a mathematically solvable problem. The first-order Taylor expansion is utilized to change them into a mathematically solvable convex expression.

First, $R_i[n]$ can be expanded at a given point $w^{(r)}[n]$ to

$$R_i[n] \geq R_i^{lb}[n], \tag{42}$$

where

$$\begin{aligned} R_i^{lb}[n] = R_i^{(0)}[n] + R_i^{(1)}[n] \Big(& \|w[n] - L_i\|^{\alpha} \\ & - \|w^{(r)}[n] - L_i\|^{\alpha} \Big). \end{aligned} \tag{43}$$

$w^{(r)}[n]$ is assumed to be the optimal value of $w[n]$ in (41) from the r-th iteration, and $R_i^{(0)}[n] = R_i[n](w^{(r)}[n])$. $R_i^{(1)}[n]$ is the first-order derivative of $R_i[n]$ with respect to $\||w[n] - Li\||^{\alpha}$, which can be derived as

$$\begin{aligned} R_i^{(1)}[n] &= \frac{\partial R_i[n]}{\partial \|w^{(r)}[n] - L_i\|^{\alpha}} \\ &= t_i[n] \left[\frac{\frac{\partial \gamma_i^{(r)}[n]}{\partial \left(\|w^{(r)}[n] - L_i\|^{\alpha} \right)}}{(1 + \gamma_i^{(r)}[n]) \ln 2} - \frac{\frac{Q^{-1}(\epsilon) \partial V_i^{(r)}[n]}{\partial \left(\|w^{(r)}[n] - L_i\|^{\alpha} \right)}}{2 \ln 2 \sqrt{M V_i^{(r)}[n]}} \right], \end{aligned} \tag{44}$$

where

$$\frac{\partial \gamma_i^{(r)}[n]}{\partial\left(\|w^{(r)}[n]-L_i\|^{\alpha}\right)}=\frac{-P_s\rho_0}{\sigma^2\left(\|w^{(r)}[n]-L_i\|^{\alpha}\right)},\tag{45}$$

and

$$\frac{\partial V_i^{(r)}[n]}{\partial\left(\|w^{(r)}[n]-L_i\|^{\alpha}\right)}=\frac{-2P_s\rho_0}{\sigma^2(1+\gamma_i^{(r)}[n])^3\left(\|w^{(r)}[n]-L_i\|^{\alpha}\right)}.\tag{46}$$

Then, (41e) can be changed into

$$\sum_{n=1}^{N}R_i[n]\Delta t\geq\sum_{n=1}^{N}R_i^{lb}[n]\Delta t\geq B_i,\tag{47}$$

Similar to (32), we have

$$\frac{\Delta t^4}{z[n]^2}\leq z[n]^2+\frac{\Delta_{uav}[n]^2}{\bar{v}^2},\tag{48}$$

where the right hand is non-concave with respect to $z[n]$, which can be expanded into

$$\begin{aligned}&z[n]^2+\frac{\Delta_{uav}[n]^2}{\bar{v}^2}\\&\quad\geq\left(z^{(r)}[n]\right)^2+2\,z^{(r)}[n]\left(z[n]-z^{(r)}[n]\right)\\&\qquad+\frac{2}{\bar{v}^2}\left(w^{(r)}[n]-w^{(r)}[n-1]\right)^T(w[n]-w[n-1])\\&\qquad-\frac{\|w^{(r)}[n]-w^{(r)}[n-1]\|^2}{\bar{v}^2}\geq\frac{\Delta t^4}{\bar{v}^2}.\end{aligned}\tag{49}$$

In (49), $z^{(r)}[n]$ is assumed to be the optimal value of $z[n]$ in (41) from the r-th iteration.

Finally, (41) can be changed into a mathematically solvable problem as

$$\textbf{P1.2.a:}\quad\max_{\mathbf{w},z[n]}\ \frac{\sum_{i=1}^{S}\sum_{n=1}^{N}R_i^{lb}[n]\Delta t}{E_{ucvx}(\Delta t)+P_{ind}\sum_{n=1}^{N}z[n]}\tag{50a}$$

$$s.t.\ w[1]=w[N],\tag{50b}$$

$$\Delta_{uav}[n]\leq\Delta tV_{max},\tag{50c}$$

$$\Delta_{uav}[n]\leq\theta H,\tag{50d}$$

$$\sum_{s=1}^{S}\sum_{n=1}^{N}R_i^{lb}[n]\Delta t\geq B_i,\tag{50e}$$

$$\begin{aligned}&\frac{2}{\bar{v}^2}\left(w^{(r)}[n]-w^{(r)}[n-1]\right)^T(w[n]-w[n-1])\\&\quad+\left(z^{(r)}[n]\right)^2+2\,z^{(r)}[n]\left(z[n]-z^{(r)}[n]\right)\\&\quad-\frac{\|w^{(r)}[n]-w^{(r)}[n-1]\|^2}{\bar{v}^2}\geq\frac{\Delta t^4}{\bar{v}^2},\end{aligned}\tag{50f}$$

which can be solved by existing convex programming tools such as CVX.

Then, the optimal trajectory $\mathbf{w}^*$, flight duration T^*, and scheduling vector $\mathbf{t}^*$ can be obtained by iteratively solving P1.1.b and P1.2.a.

Accordingly, Algorithm 1 is summarized to solve P1.

The computational complexity of the proposed scheme can be concluded as follows. There are $N-1$ linear matrix inequalities (LMI) of dimension 1, N LMI of dimension 1, $2S$ LMI of dimension N, I LMI of dimension 1, I LMI of dimension 1, N LMI of dimension 1, S second-order cones (SOC) of dimension 3, and S SOC of dimension 2 in Step 4. In addition, the total number of variables is $2S+N+1$. Then, the number of iterations is $\mathcal{O}(SN)$, and the complexity of each is $\mathcal{O}\left(N^2S(N^2+S^2+SN)\right)$. Accordingly, the total computational complexity of Step 4 is $\mathcal{O}\left(N^{4.5}S^{1.5}+N^{2.5}S^{3.5}+N^{3.5}S^{2.5}\right)$. Similarly, the computational complexity of Step 5 can be calculated as $\mathcal{O}\left(\sqrt{N+S}(N^3+SN^2)\right)$. Thus, the overall computational complexity of Algorithm 1 can be expressed as $\mathcal{O}\left(N^{4.5}S^{1.5}+N^{2.5}S^{3.5}+N^{3.5}S^{2.5}\right)$.

Algorithm 1 Iterative Algorithm to Solve P1

```
1: Initialization Initialize $\mathbf{w}^{(0)}, \mathbf{t}^{(0)}, \Delta t^{(0)}$.
2: Set iteration index $r = 0$.
3: repeat
4:     Obtain $\mathbf{t}^{(r+1)}$ and $\Delta t^{(r+1)}$ from (40), under the given $\mathbf{w}^{(r)}$.
5:     Obtain $\mathbf{w}^{(r+1)}$ from (50), under the given $\mathbf{t}^{(r+1)}$ and $\Delta t^{(r+1)}$.
6:     Set $r = r + 1$.
7: until Convergence
8: Set $\mathbf{t}^* = \mathbf{t}^{(r)}$, $\Delta t^* = \Delta t^{(r)}$, and $\mathbf{w}^* = \mathbf{w}^{(r)}$.
```

IV. Secrecy Rate Maximization

During the data collection, the UAV also transfers the received data from the sensors together with its own data to the BS. Meanwhile, it should prevent the adversarial eavesdropping, with the secrecy outage probability requirement satisfied. Therefore, we should optimize the transmit power P_a and the information blocklength N_u to maximize the secrecy rate, while keeping the secrecy outage probability and the eavesdropping rate lower than the constraints.

Thus, the optimization can be formulated as

$$\textbf{P2:}\quad\max_{P_a,N_u}\ \sum_{n=1}^{N}R_s[n]\tag{51a}$$

$$s.t.\ P_a\leq P_{a_{max}},\tag{51b}$$

$$N_u\leq N_{u_{max}},\tag{51c}$$

$$R_e[n]\leq r,\tag{51d}$$

$$p_{out}[n]\leq\xi,\tag{51e}$$

where $P_{a_{max}}$ is the maximum allowed transmit power of UAV, $N_{u_{max}}$ represents the maximum allowed information blocklength, and r and ξ denote the thresholds of eavesdropping rate and outage probability, respectively.

The environmental noise is usually smaller than the signal power. In the rest of this paper, we consider the large SNR situation, where both $\sqrt{\frac{\gamma_b[n](\gamma_b[n]+2)}{(\gamma_b[n]+1)^2}}$ and $\sqrt{\frac{\gamma_e[n](\gamma_e[n]+2)}{(\gamma_e[n]+1)^2}}$ approach to 1. Thus, we have

$$R_s[n]\geq\log_2\left(\frac{1+\gamma_b[n]}{1+\gamma_e[n]}\right)-\frac{Q^{-1}(\epsilon)+Q^{-1}(\delta_e)}{\ln 2\sqrt{N_u}}=\tilde{R}_s[n].\tag{52}$$

Then, the expression of $p_{out}[n]$ is derived in Proposition 1.

Proposition 1: The detailed expression of $p_{out}[n]$ in (25) follows

$$p_{out}[n] = \int_{f(P_a)}^{+\infty} \frac{1}{a^2} \mathrm{e}^{-\frac{q[n]+b^2}{a^2}} I_0\left(\frac{b\sqrt{q[n]}}{a^2}\right) dq[n]. \tag{53}$$

Proof: The $p_{out}[n]$ defined in (25) can be changed into (54), as shown at the bottom of the next page, where $q[n] = |\mathbf{h}_e[n]\mathbf{u}[n]|^2$, and $f\left(P_a\right)$ can be expressed as

$$\begin{aligned} & f\left(P_a\right) \\ & = \frac{\sigma^2 d_e[n]^\alpha \left(2^{\log_2\left(1+\frac{MP_a\rho_0}{\sigma^2 d_b[n]^\alpha}\right)-\frac{Q^{-1}(\epsilon)+Q^{-1}(\delta_e)}{\ln 2\sqrt{N_u}}-R_0[n]}-1\right)}{P_a\rho_0}. \end{aligned} \tag{55}$$

Since $c_L\mathbf{h}_{eL}[n]\mathbf{u}[n]$ in $q[n]$ is a constant while $c_N\mathbf{h}_{eN}[n]\mathbf{u}[n]$ is a random variable, we transform $q[n]$ for analysis simplicity as

$$q[n] = |ax+b]|^2, \tag{56}$$

where $b = c_L\mathbf{h}_{eL}[n]\mathbf{u}[n]$, $a = c_N$, and $x = \mathbf{h}_{eN}[n]\mathbf{u}[n]$. It is proved in [30] that $\mathbf{h}_{eN}[n]\mathbf{u}[n] \sim \mathcal{CN}(0,1)$. According to [31], $q[n] \sim \chi^2(2, b^2)$ and the probability density function of $q[n]$ can be expressed as

$$f_q(q[n]) = \frac{1}{a^2} \mathrm{e}^{-\frac{q[n]+b^2}{a^2}} I_0\left(\frac{b\sqrt{q[n]}}{a^2}\right). \tag{57}$$

Therefore, $p_{out}[n]$ in (54) can be changed into (53). Proposition 1 is proved. ■

Then, since the trajectory is optimized in P1, the maximization of $\sum_{n=1}^{N} R_s[n]$ is equivalent to maximizing each $\tilde{R}_s[n]$. Thus, P2 can be reformulated into

$$\begin{aligned} \textbf{P2.1:} \quad & \max_{P_a, N_u} \quad \tilde{R}_s[n] && \text{(58a)} \\ & s.t. \; P_a \le P_{a_{max}}, && \text{(58b)} \\ & \qquad N_u \le N_{u_{max}}, && \text{(58c)} \\ & \qquad R_e[n] \le r, && \text{(58d)} \\ & \qquad p_{out}[n] \le \xi. && \text{(58e)} \end{aligned}$$

To derive the optimal transmit power P_a^* of UAV and the optimal blocklength N_u^*, we analyze the monotonicity of $\tilde{R}_s[n]$, $R_e[n]$, and $p_{out}[n]$ with respect to P_a and N_u in the following propositions.

Proposition 2: $\tilde{R}_s[n]$ monotonically increases with respect to P_a and N_u.

Proof: From the expression in (52), we have the first-order derivative of $\tilde{R}_s[n]$ with respect to P_a as

$$\begin{aligned} \frac{\partial \tilde{R}_s[n]}{\partial P_a} &= \frac{M\rho_0/\ln 2}{(d_b[n]^\alpha\sigma^2 + MP_a\rho_0)} - \frac{|\mathbf{h}_e\mathbf{u}|^2\rho_0/\ln 2}{(d_e[n]^\alpha\sigma^2 + |\mathbf{h}_e\mathbf{u}|^2P_a\rho_0)} \\ &= \frac{\rho_0\sigma^2\left(d_e[n]^\alpha M - |\mathbf{h}_e\mathbf{u}|^2 d_b[n]^\alpha\right)/\ln 2}{(d_b[n]^\alpha\sigma^2 + MP_a\rho_0)\left(d_e[n]^\alpha\sigma^2 + |\mathbf{h}_e\mathbf{u}|^2P_a\rho_0\right)}. \end{aligned} \tag{59}$$

With the definition of each parameter in (59), it is easy to conclude $\frac{\partial \tilde{R}_s[n]}{\partial P_a} > 0$, which indicates that $\tilde{R}_s[n]$ monotonically increases with the transmit power P_a at the UAV.

In addition, we have the first-order derivative of $\tilde{R}_s[n]$ with respect to N_u as

$$\frac{\partial \tilde{R}_s[n]}{\partial N_u} = \frac{Q^{-1}(\epsilon) + Q^{-1}(\delta)N^{-\frac{3}{2}}}{2\ln 2} > 0, \tag{60}$$

from which, we can conclude that $\tilde{R}_s[n]$ monotonically increases with N_u.

Proposition 2 is proved. ■

Therefore, to achieve higher $\tilde{R}_s[n]$, we need to set larger N_u and P_a. Then, the first-order derivative of eavesdropping rate $R_e[n]$ with respect to P_a and N_u is analyzed in Proposition 3.

Proposition 3: $R_e[n]$ monotonically increases with P_a and N_u.

Proof: First, in the large SNR scenario, the first-order derivative of eavesdropping rate $R_e[n]$ with respect to P_a can be derived as

$$\frac{\partial R_e[n]}{\partial P_a} = \frac{\rho_0|\mathbf{h}_e[n]\mathbf{u}[n]|^2}{(1+\gamma_e[n])\ln 2 \; d_e[n]^\alpha} > 0. \tag{61}$$

Then, the first-order derivative of eavesdropping rate $R_e[n]$ with respect to N_u can be derived as

$$\frac{\partial R_e[n]}{\partial N_u} = \frac{Q^{-1}(\delta)}{2\ln 2} N_u^{-\frac{3}{2}} > 0. \tag{62}$$

Thus, we can conclude that the increase of P_a and N_u will both result in a larger $R_e[n]$.

Proposition 3 is proved. ■

Furthermore, we have the first-order derivative of $p_{out}[n]$ with respect to P_a and N_u in Proposition 4.

Proposition 4: $p_{out}[n]$ monotonicially decreases with P_a and N_u.

Proof: The first-order derivative of $R_e[n]$ with respect to P_a can be described as

$$\frac{\partial p_{out}[n]}{\partial P_a} = -\frac{\mathrm{e}^{-\frac{f(P_a)+b^2}{a^2}} I_0 \frac{b\sqrt{f(P_a)}}{a^2}}{a^2} \frac{\partial f\left(P_a\right)}{\partial P_a}, \tag{63}$$

where we can derive the first-order derivative of $f\left(P_a\right)$ with respect to P_a from (55) as

$$\begin{aligned} \frac{\partial f\left(P_a\right)}{\partial P_a} &= \frac{\left(2^{c[n]}\left[\frac{\ln c[n]MP_a\rho_0}{(d_b[n]^\alpha\sigma^2+MP_a\rho_0)\ln 2} - 1\right] + 1\right)\sigma^2 d_e[n]^\alpha}{P_a^2\rho_0} \\ &\ge \frac{\frac{\ln c[n]MP_a\rho_0}{(d_b[n]^\alpha\sigma^2+MP_a\rho_0)\ln 2}\sigma^2 d_e[n]^\alpha}{P_a^2\rho_0} > 0, \end{aligned} \tag{64}$$

where

$$c[n] = \log_2\left(1 + \frac{MP_a\rho_0}{\sigma^2 d_b[n]^\alpha}\right) - \frac{Q^{-1}(\epsilon)+Q^{-1}(\delta_e)}{\ln 2\sqrt{N_u}} - R_0[n]. \tag{65}$$

From (63) and (64), we can see that $\frac{\partial p_{out}[n]}{\partial P_a} < 0$, which indicates that $p_{out}[n]$ monotonically decreases with P_a. Thus, to achieve a smaller $p_{out}[n]$, we need to increase the transmit power at the UAV.

Besides, we have the first-order derivative of $p_{out}[n]$ with respect to N_u as

$$\frac{\partial p_{out}[n]}{\partial N_u} = -\frac{\mathrm{e}^{-\frac{g(N_u)+b^2}{a^2}} I_0\left(\frac{b\sqrt{g(N_u)}}{\sigma^2}\right)}{a^2} \frac{\partial g(N_u)}{\partial N_u}, \tag{66}$$

where we set $g(N_u) = f(P_a)$. $\frac{\partial g(N_u)}{\partial N_u}$ can be derived as

$$\frac{\partial g(N_u)}{\partial N_u} = 2^{c[n]} \ln 2 \frac{Q^{-1}(\epsilon) + Q^{-1}(\delta_e)}{2 \ln 2} N_u^{-\frac{3}{2}} > 0. \quad (67)$$

Thus, we can conclude that $\frac{\partial p_{out}[n]}{\partial N_u} < 0$, which indicates that we should increase N_u to achieve a smaller secrecy outage probability $p_{out}[n]$.

Proposition 4 is proved. ■

Then, the solution to P2.1 can be derived in Proposition 5.

Proposition 5: The optimal transmit power P_a^* and blocklength N_u^* at the UAV for P2.1 can be derived as

$$P_a^* = \min\left\{P_{a_{max}}, \bar{R}_e[n]^{-1}(N_u^*, r)\right\}, \quad (68)$$

where N_u^* can be derived via the traversal algorithm to maximize $\tilde{R}_s[n](P_a^{N_u}, N_u)$.

Proof: To satisfy (58d), we need to keep the transmit power P_a and the blocklength N_u small. However, the decrease of both P_a and N_u will result in the decrease of $\tilde{R}_s[n]$ and the increase of $p_{out}[n]$. Therefore, we set P_a and N_u as large as possible with (58d) satisfied.

We first derive the upper bounds of P_a and N_u with (58d) taking the equality, and then figure out the optimal pair of (P_a^*, N_u^*) to maximize $\tilde{R}_s[n]$ while guaranteeing (58e). However, there exists a trade-off between P_a and N_u owing to that both of their increase can improve the performance. Since N_u is an integer, we derive the expression of the upper bound of P_a from $R_e[n] = r$ as $P_a^{N_u} = R_e[n]^{-1}(N_u, r)$, where $R_e[n]^{-1}(*)$ is the inverse function of $R_e[n]$. However, since we cannot obtain $\mathbf{h}_e[n]$ in $R_e[n]$, we replace $R_e[n]$ with its mean value of $\bar{R}_e[n]$. Thus, $P_a^{N_u}$ can be derived as

$$P_a^{N_u} = \bar{R}_e[n]^{-1}(N_u, r). \quad (69)$$

Proposition 5 is proved. ■

Remark: According to (68), P_a should be reduced to $P_{a_{max}}$ when $\bar{R}_e[n]^{-1}(N_u^*, r) > P_{a_{max}}$. Then, N_u^* should also be adjusted accordingly by maximizing $\tilde{R}_s[n](P_{a_{max}}, N_u)$.

V. Simulation Results and Discussion

Simulation results are provided to demonstrate the effectiveness of the proposed scheme. There are six sensors randomly distributed within a square ground with each side of 1500 m. The UAV is flying above the square area with a fixed altitude $H = 100$ m. The maximum velocity of UAV is set as $V_{max} =$ 50 m/s, and the flight duration T is divided into $N = 60$ time slots. For the aerodynamic propulsion parameters of UAV, the profile power of blades $P_{bld} = 79.86$ W, the tip speed of rotor blades $v_t = 120$ m/s, the fuselage drag ratio $r_{drag} = 0.6$, the density of air $\rho_{air} = 1.225$ kg/m^3, the solidity of rotor $h_{rtor} = 0.05$, the disc area of rotor $S_{rtor} = 0.50$ m^2, the induced power $P_{ind} = 88.61$ W when $\frac{\Delta uav[n]}{\Delta t} = 0$, and the mean induced speed of motor $\bar{v} = 4.03$ m/s according to [32]. The number of antennas at the UAV is set to $M = 8$. Assume that the BS locates at $L_b(7000, 0, 100)$ and the estimated closest location of eavesdropper is at $L_e(7500, 0, 0)$ in meters. In addition, the environmental noise power variance is set as $\sigma^2 = -110$ dBm. The large-scale channel fading reference at 1 m can be set to $\rho_0 = 10^{-6}$. The channel fading parameters are assumed as $K = 5$ and $\alpha = 2$. According to [33], $N_u > 100$ is usually set. In the simulation, we also examine the case when $N_u < 100$ to show the influence of blocklength.

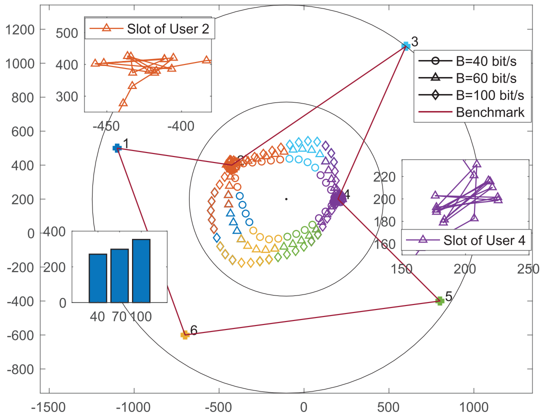


Fig. 2. Comparison of trajectories under different minimum collected data B_i of the proposed scheme and the benchmark.

A. Data Collection Phase

The trajectories of UAV are compared in Fig. 2, when the lower bound of collected data for each sensor is set to $B_i =$ 40 bit/Hz, $B_i = 60$ bit/Hz, $B_i = 80$ bit/Hz in the proposed EE algorithm, and $B_i = 40$ bit/Hz for the benchmark, respectively. The transmit power P_s at each sensor is set to 0.1 W. The proposed scheme focuses more on the EE. In the benchmark, the UAV boosts to its maximum velocity V_{max} to fly to each sensor and then hovers above it to collect 40 bit/Hz data in each round. We use different colors to represent the time slots assigned to different users during the collection. From the results, we can see that the trajectories of the proposed scheme in different settings tend to be shorter, and the UAV tends to hover above the two central users for a longer time. This is because a shorter path can reduce the energy consumption of UAV and thus increase EE. Hovering around the centered users can also save energy. In addition, we can see that the UAV tends to fly closer to other edge users when B_i increases.

In Fig. 3, the EE r_{tc} and sum collected data are compared between the proposed EE scheme and the benchmark with different B_i. The transmit power P_s in each scheme is set as 0.1 W. From the results, we can see that the proposed scheme is superior in both EE and collected data. Specifically, the collected data of both schemes increase with B_i. On the other hand, the EE of the proposed scheme decreases with B_i while that of the benchmark monotonically increases with B_i. This is because higher data requirement results in a longer flight duration for the proposed scheme, which increases the energy consumption of UAV and thus reduces the EE.

$$p_{out}[n] = Pr\left(\log_2\left(1 + \frac{M P_a \rho_0}{\sigma^2 d_b[n]^\alpha}\right) - \frac{Q^{-1}(\epsilon) + Q^{-1}(\delta_e)}{\ln 2 \sqrt{N_u}} - \log_2\left(1 + \frac{P_a \rho_0}{\sigma^2 d_e[n]^\alpha} q[n]\right) \le R_0[n]\right) = Pr\left(q[n] \ge f(P_a)\right). \quad (54)$$

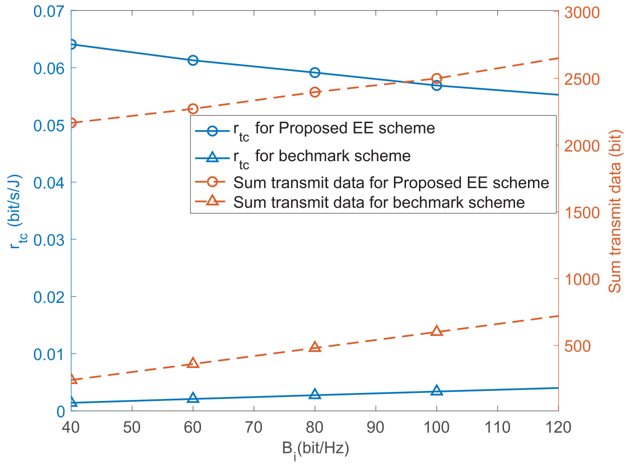


Fig. 3. Comparison of EE and sum collected data between the proposed scheme and the benchmark with different B_i.

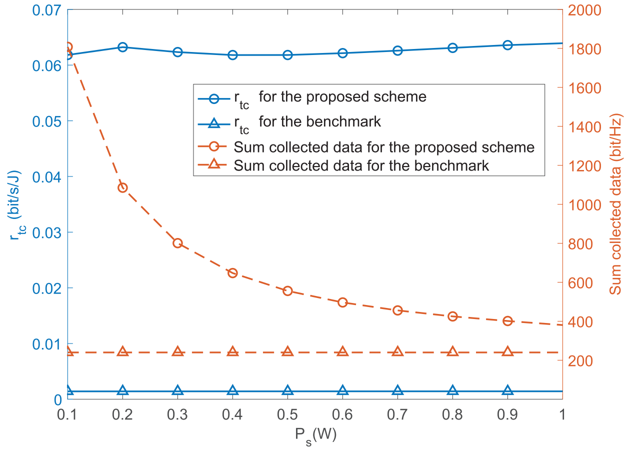


Fig. 4. Comparison of EE and sum collected data between the proposed scheme and the benchmark with different transmit power P_s at the sensors.

The impacts of the transmit power P_s at each sensor on the EE and collected data are plotted in Fig. 4, where the proposed scheme is compared to the benchmark. The minimum collected data in both schemes is set as $B_i = 40$ bit/Hz. From the results, we can observe that regardless of the values of transmit power P_s, the proposed scheme can achieve better performance of both EE and collected data. Moreover, the collected data of the proposed scheme decreases with the incremental of the transmit power P_s. This is due to the fact that the increase of P_s of each sensor results in a higher transmission rate, which can satisfy the minimum collected data B_i with a shorter flight duration.

B. Short-Packet Transmission Phase

Fig. 5 shows the impact of P_a on the average achievable eavesdropping rate R_e, transmission rate R_b and secrecy rate R_s. We set $B_i = 40$ bit/s, $P_s = 0.1$ W and $N_u = 20$. From the results, we can see that although the eavesdropping rate R_e increases with P_a, the transmission rate R_b towards the BS increases more rapidly, which enables the secrecy rate R_s to increase with P_a. This is because the MRT can result in higher SINR at the legitimate receiver.

The impacts of the blocklength N_u on R_b, R_e, and R_s are investigated in Fig. 6. We have $P_s = 0.1$ W, $B_i = 40$ bit/Hz and $P_a = 0.1$ W. From the results, we can see that R_e, R_b, and R_s all increase with the blocklength N_u. This is because the MRT can bring a higher SINR at BS, which enables R_b to increase faster than R_e.

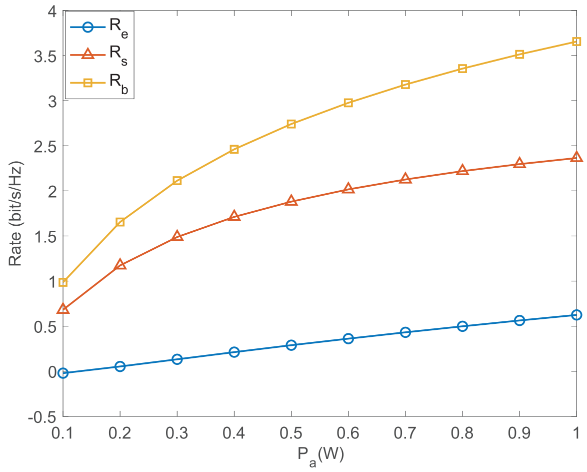


Fig. 5. Comparison of the average achievable eavesdropping rate R_e, transmission rate R_b and secrecy rate R_s with different transmit power P_a of UAV.

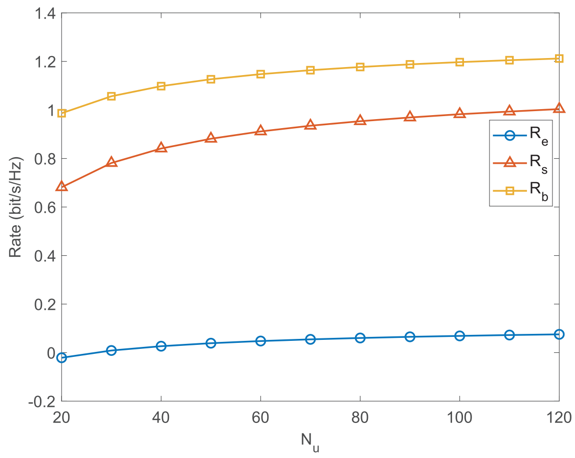


Fig. 6. Comparison of the average achievable eavesdropping rate R_e, transmission rate R_b and secrecy rate R_s with different blocklength N_u.

Then, the impact of P_a and N_u on the secrecy outage propability p_{out} is shown in Fig. 7. We have $P_s = 0.1$ W, $B_i = 40$ bit/Hz and $R_0[n] = 1.8$ bit/s/Hz. From the results, we can see that the secrecy outage probability p_{out} decreases with P_a. In addition, the increase of N_u can also lead to the reduction of p_{out}. Thus, a smaller p_{out} can be achieved by either a higher P_a or a larger N_u.

Finally, the impacts of the blocklength N_u and eavesdropping rate threshold r on the maximum achievable secrecy rate R_s and R_b are investigated in Fig. 8. We have $B_i = 40$ bit/s and $P_s = 0.1$ W. The transmit power P_a^* is derived from (68). From the results, we can see that R_b decreases with N_u with a given r, which indicates that the optimal transmit power P_a also decreases with N_u. This is because there is a trade-off between the maximum allowed transmit power P_a and the blocklength N_u under a given threshold r. In addition, the maximum achievable R_s first increases with N_u sharply, and then reaches a saturation level. This is because increasing the blocklength can enlarge the achievable secrecy rate, however, bounded by Shannon capacity. To evaluate the effectiveness

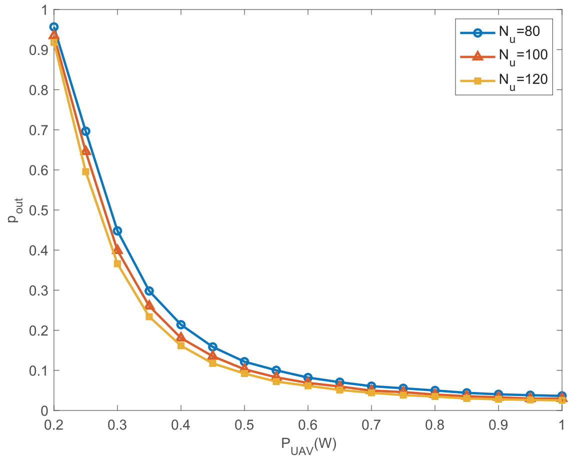


Fig. 7. Comparison of the secrecy outage probability p_{out} with different transmit power P_a. Different values of blocklength $N_u = 80$, $N_u = 100$, $N_u = 120$ are considered.

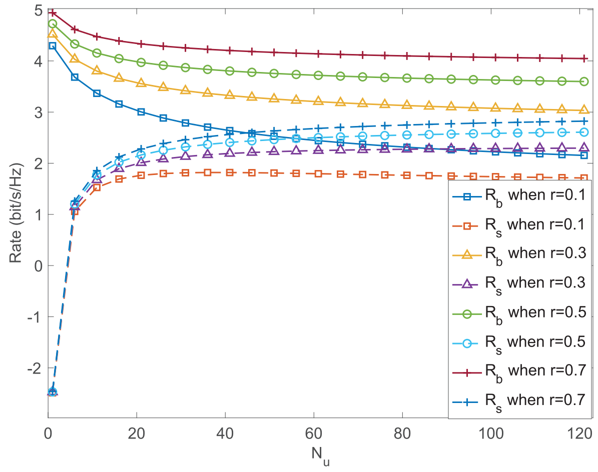


Fig. 8. Comparison of the maximum achievable R_s and R_b with different blocklength N_u. Four cases of $r = 0.1$ bit/s/Hz, $r = 0.3$ bit/s/Hz, $r = 0.5$ bit/s/Hz, $r = 0.7$ bit/s/Hz are considered.

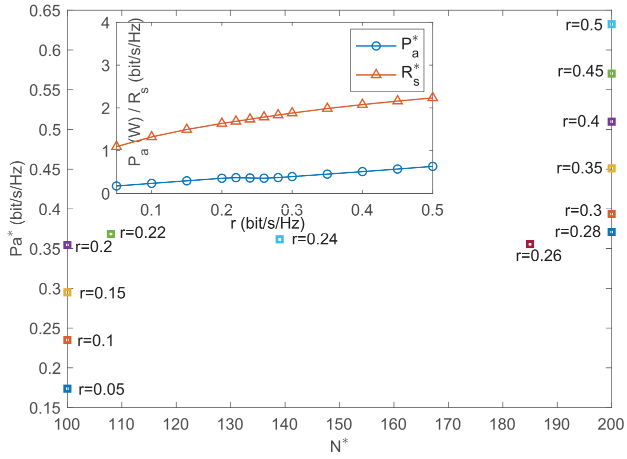


Fig. 9. Comparison of the maximum achievable R_s and the corresponding P_a^* and N_u^* under different values of r.

of the proposed scheme, we investigate the optimized P_a^* and N_u^* under different values of the eavesdropping rate threshold r in Fig. 9, where $100 \leq N_u \leq 200$. From the results, we can see that P_a^* increases as r, while N_u^* equaling to the smallest value when r is small but increases when r gets bigger. This indicates that N_u has more impact on R_e compared with R_b when r is small, and smaller N_u can achieve larger R_s. However, larger N_u is preferred when r increases.

VI. Conclusion

A secure short-packet data collection and transmission scheme for UAV-assisted wireless networks has been proposed in this paper. First, the trajectory together with the flight duration of UAV and the user scheduling are jointly designed to maximize the EE in the data collection phase. The formulated optimization problem is non-convex and mathematically unsolvable. We utilize the first-order Taylor expansion to convert it to two convex subproblems, which are solved via SCA. Then, in the data transmission phase, with the derived optimal trajectory of UAV, we optimize the transmit power and the blocklength of the secure short-packet transmission from the UAV to BS against the malicious eavesdropping to achieve a maximum secrecy rate while guaranteeing the reliability. Finally, simulation results are presented to evaluate the effectiveness of the proposed scheme.

References

[1] X. Chen, Z. Chang, N. Zhao, T. Hamalainen, and X. Wang, "Energy-efficient secure data collection and transmission via UAV," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2022, pp. 1–6.

[2] K. David and H. Berndt, "6G vision and requirements: Is there any need for beyond 5G?" *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 72–80, Sep. 2018.

[3] J. Liu, Y. Shi, Z. M. Fadlullah, and N. Kato, "Space-air-ground integrated network: A survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2714–2741, 4th Quart., 2018.

[4] 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.

[5] 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.

[6] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, 2nd Quart. 2016.

[7] B. Mao, F. Tang, Y. Kawamoto, and N. Kato, "Optimizing computation offloading in satellite-UAV-Served 6G IoT: A deep learning approach," *IEEE Netw.*, vol. 35, no. 4, pp. 102–108, Aug. 2021.

[8] L. Zhang, Y.-C. Liang, and D. Niyato, "6G visions: Mobile ultra-broadband, super Internet-of-Things, and artificial intelligence," *China Commun.*, vol. 16, no. 8, pp. 1–14, Aug. 2019.

[9] H. Guo and J. Liu, "UAV-enhanced intelligent offloading for Internet of Things at the edge," *IEEE Trans. Ind. Informat.*, vol. 16, no. 4, pp. 2737–2746, Apr. 2020.

[10] W. Wang, N. Zhao, L. Chen, X. Liu, Y. Chen, and D. Niyato, "UAV-assisted time-efficient data collection via uplink NOMA," *IEEE Trans. Commun.*, vol. 69, no. 11, pp. 7851–7863, Nov. 2021.

[11] J. Liu, P. Tong, X. Wang, B. Bai, and H. Dai, "UAV-aided data collection for information freshness in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 20, no. 4, pp. 2368–2382, Apr. 2021.

[12] Y. Liu, K. Xiong, Y. Lu, Q. Ni, P. Fan, and K. B. Letaief, "UAV-aided wireless power transfer and data collection in Rician fading," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 10, pp. 3097–3113, Oct. 2021.

[13] R. Zhang, X. Pang, W. Lu, N. Zhao, Y. Chen, and D. Niyato, "Dual-UAV enabled secure data collection with propulsion limitation," *IEEE Trans. Wireless Commun.*, vol. 20, no. 11, pp. 7445–7459, Nov. 2021.

[14] H. Yang, J. Zhao, Z. Xiong, K.-Y. Lam, S. Sun, and L. Xiao, "Privacy-preserving federated learning for UAV-enabled networks: Learning-based joint scheduling and resource management," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 10, pp. 3144–3159, Oct. 2021.

[15] X. Xu, H. Zhao, H. Yao, and S. Wang, "A blockchain-enabled energy-efficient data collection system for UAV-assisted IoT," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2431–2443, Feb. 2021.

[16] Y. Xu, T. Zhang, D. Yang, Y. Liu, and M. Tao, "Joint resource and trajectory optimization for security in UAV-assisted MEC systems," *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 573–588, Jan. 2021.

[17] X. Chen et al., "Secure transmission via power allocation in NOMA-UAV networks with circular trajectory," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 10033–10045, Sep. 2020.

[18] W. Wang et al., "Joint precoding optimization for secure SWIPT in UAV-aided NOMA networks," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 5028–5040, Aug. 2020.

[19] C. Zhong, J. Yao, and J. Xu, "Secure UAV communication with cooperative jamming and trajectory control," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 286–289, Feb. 2019.

[20] J. Kang, Z. Xiong, D. Niyato, S. Xie, and D. I. Kim, "Securing data sharing from the sky: Integrating blockchains into drones in 5G and beyond," *IEEE Netw.*, vol. 35, no. 1, pp. 78–85, Jan. 2021.

[21] D. Xu and P. Ren, "Quantum learning based nonrandom superimposed coding for secure wireless access in 5G URLLC," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2429–2444, 2021.

[22] H. Ji, S. Park, J. Yeo, Y. Kim, J. Lee, and B. Shim, "Ultra-reliable and low-latency communications in 5G downlink: Physical layer aspects," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 124–130, Jun. 2018.

[23] Z. Zhu et al., "Research and analysis of URLLC technology based on artificial intelligence," *IEEE Commun. Standards Mag.*, vol. 5, no. 2, pp. 37–43, Jun. 2021.

[24] X. Yang, Z. Zho, and B. Huang, "URLLC key technologies and standardization for 6G power Internet of Things," *IEEE Commun. Standards Mag.*, vol. 5, no. 2, pp. 52–59, Jun. 2021.

[25] A. Ranjha and G. Kaddoum, "URLLC facilitated by mobile UAV relay and RIS: A joint design of passive beamforming, blocklength, and UAV positioning," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4618–4627, Mar. 2021.

[26] H. Ren, C. Pan, K. Wang, Y. Deng, M. Elkashlan, and A. Nallanathan, "Achievable data rate for URLLC-enabled UAV systems with 3-D channel model," *IEEE Wireless Commun. Lett.*, vol. 8, no. 6, pp. 1587–1590, Jul. 2019.

[27] C. Pan, H. Ren, Y. Deng, M. Elkashlan, and A. Nallanathan, "Joint blocklength and location optimization for URLLC-enabled UAV relay systems," *IEEE Commun. Lett.*, vol. 23, no. 3, pp. 498–501, Mar. 2019.

[28] W. Yang, R. F. Schaefer, and H. V. Poor, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, Jul. 2019.

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

[30] X. Chen et al., "Multi-antenna covert communication via full-duplex jamming against a warden with uncertain locations," *IEEE Trans. Wireless Commun.*, vol. 20, no. 8, pp. 5467–5480, Aug. 2021.

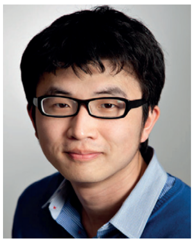
[31] S. I. Resnick, *Adventures in Stochastic Processes*. New York, NY, USA: Springer, 1992.

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

[33] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

Xinying Chen received the B.E. degree in electronic information engineering from the Dalian University of Technology, China, in 2015, and the M.S. degree in communication engineering from the Beijing University of Posts and Telecommunications in 2018. She is currently working toward a Ph.D. degree in software and communication engineering with the University of Jyväskylä, Finland. She also works on a Ph.D. degree in information and telecommunication engineering with the Dalian University of Technology. Her research interests include covert communications, physical-layer security in NOMA, and URLLC security.

Nan Zhao (Senior Member, IEEE) received the Ph.D. degree in information and communication engineering from the Harbin Institute of Technology, Harbin, China, in 2011. He is currently a Professor with the Dalian University of Technology, China. He won the Best Paper Awards in IEEE VTC 2017 Spring, ICNC 2018, WCSP 2018, and WCSP 2019. He also received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018. He is serving on the Editorial Boards for IEEE Wireless Communications and IEEE Wireless Communications Letters.



Zheng Chang (Senior Member, IEEE) received the Ph.D. degree from the University of Jyväskylä, Jyväskylä, Finland, in 2013. He has published over 140 papers in journals and conferences. His research interests include the IoT, cloud/edge computing, security and privacy, vehicular networks, and green communications. He received the Best Paper Awards from IEEE TCGCC and APCC in 2017 and has been awarded as the 2018 IEEE Best Young Research Professional for EMEA and the 2021 IEEE MMTC Outstanding Young Researcher. He serves as an Editor for IEEE Wireless Communications Letters, *Wireless Networks* (Springer), and *International Journal of Distributed Sensor Networks*, and a Guest Editor for *IEEE Network*, IEEE Wireless Communications, *IEEE Communications Magazine*, IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, *Physical Communications*, *EURASIP Journal on Wireless Communications and Networking*, and *Wireless Communications and Mobile Computing*. He was the Exemplary Reviewer of IEEE Wireless Communication Letters in 2018. He has participated in organizing workshops and special sessions in GLOBECOM 2019, WCNC 2018–2022, SPAWC 2019, and ISWCS 2018. He also serves as the Symposium Co-Chair for IEEE ICC 2020 and IEEE GLOBECOM 2023, the Publicity Co-Chair for IEEE Infocom 2022, the Workshop Co-Chair for ICCC 2022, the TPC Co-Chair of IEEE iThing 2022, and a TPC Member for many IEEE major conferences, such as INFOCOM, ICC, and GLOBECOM.

Timo Hämäläinen (Senior Member, IEEE) has over 30 years of research and teaching experience in computer networks and networking security. He has led tens of external funded network management related projects. He has launched and led a Master's Program with the University of Jyväskylä (software and communications engineering) and teaches network management and security related courses. He has more than 220 internationally peer-reviewed publications and he has supervised over 40 Ph.D. theses. His research interests include network resource management, the IoT, and networking security.

Xianbin Wang (Fellow, IEEE) received the Ph.D. degree in electrical and computer engineering from the National University of Singapore in 2001.

He is currently a Professor and a Tier-1 Canada Research Chair with Western University, Canada. Prior to joining Western University, he was with the Communications Research Centre Canada as a Research Scientist/Senior Research Scientist from July 2002 to December 2007. From January 2001 to July 2002, he was a System Designer at STMicroelectronics. He has over 500 highly cited journals and conference papers, in addition to 30 granted and pending patents and several standard contributions. His current research interests include 5G/6G technologies, the Internet of Things, communications security, machine learning, and intelligent communications.

Dr. Wang is a fellow of the Canadian Academy of Engineering and a fellow of the Engineering Institute of Canada. He has received many prestigious awards and recognitions, including the IEEE Canada R. A. Fessenden Award, the Canada Research Chair, the Engineering Research Excellence Award at Western University, the Canadian Federal Government Public Service Award, the Ontario Early Researcher Award, and six IEEE best paper awards. He was involved in many IEEE conferences, including GLOBECOM, ICC, VTC, PIMRC, WCNC, CCECE, and CWIT, in different roles, such as the General Chair, the Symposium Chair, a Tutorial Instructor, the Track Chair, the Session Chair, the TPC Co-Chair, and a Keynote Speaker. He was the Chair of the IEEE ComSoc Signal Processing and Computing for Communications (SPCC) Technical Committee and is also serving as the Central Area Chair for IEEE Canada. He also serves/has served as the Editor-in-Chief, an Associate Editor-in-Chief, and an editor/associate editor for over ten journals. He has been nominated as an IEEE Distinguished Lecturer several times during the last ten years. He is an IEEE Distinguished Lecturer.

II

SECURE TRANSMISSION FOR IRS-ON-UAV-ASSISTED WIRELESS NETWORKS

by

Xinying Chen, Zheng Chang, and Timo Hämäläinen 2024

IEEE Transactions on Communications, submitted

Secure Transmission for IRS-on-UAV-assisted Wireless Networks

Xinying Chen, Zheng Chang, *Senior Member, IEEE,* and Timo Hämäläinen, *Senior Member, IEEE*

Abstract—**Combined with the unmanned aerial vehicle (UAV), intelligent reflecting surface (IRS) can leverage the adjustable mobility and flexible deployment, thus enhancing the quality of wireless transmission via line-of-sight (LoS) links. However, IRS-assisted UAV network may also encounter security issues in the physical layer. To realize the secure transmission and improve transmission performance, we investigate an IRS-assisted UAV network against an eavesdropper in this paper, where the IRS is mounted on the UAV to leverage its mobility. Our goal is to maximize the secrecy rate while improving overall transmission performance by jointly optimizing the transmit/jamming beamforming vectors, phase shifting matrix, and the hovering location of IRS. Owing to the non-convexity of the summarized optimization problem, we decompose the optimization problem into three subproblems and solve them alternately to derive the optimal beamforming vectors, UAV location and phase shifting matrix. First, transmit/jamming beamforming vectors are derived with given IRS location and phase shifting matrix. Then, we adopt the first-order Taylor expansion to change the non-convex location optimization subproblems into a mathematical solvable convex version, and then solve it through successive convex approximation (SCA) with given phase shifting matrix and beamforming vetors. Next, with given UAV hovering location and and beamforming vetors, the phase shifting matrix is optimized via semidefinite relaxation (SDR) and SCA. Simulation results are provided to evaluate the effectiveness of our proposed secure IRS-on-UAV transmission scheme.**

Index Terms—**Intelligent reflecting surface, location optimization, secure transmission, transmit/jamming power split, unmanned aerial vehicle.**

I. Introduction

The intelligent reflecting surface (IRS) has attracted tremendous intention owing to its flexible deployment, easy configuration, and channel capacity improvement [2]. Consisting of a number of two-dimensional artificial electromagnetic surfaces, IRS is able to change the channel electromagnetic properties through its scattering elements [3], [4]. Technically, IRS can realize the re-design of channel fading via programming the amplitude and phase shifting of the passive reconfigurable reflection elements without extra high power consumption [5], [6]. The total received signals can be enhanced or reduced with the directly transmitted signals at specific receivers by properly designing phase shifts of the IRS units [7]. In [8], You *et al.* investigated the effectiveness of active and passive IRS in wireless communications, where they concluded that the passive IRS can achieve better performance with a sufficiently large amount of elements. IRS is able to be leveraged to migrate interference in a wireless network as well. In [9], Pang *et al.* exploited IRSs in a cellular connected UAV network to migrate/eliminate the interference caused by line-of-sight (LoS) channels in both uplinks and downlinks. In addition, the utilization of the IRSs can also improve the transmission security through its reconfigurable channel property. Wang *et al.* utilized beamforming and jamming to realize the secure transmission in IRS-assisted non-orthogonal multiple access (NOMA) networks in [10]. They alternately solved the non-convex optimization to derive the optimal beamforming, jamming, and phase shifting vectors to maximize the sum rate of legitimate users while constraining the eavesdropping rate under the limit. Although IRS can leverage channel design to realize the enhancement of desired signals and suppressant of undesired signals, the deployment of IRS still confronts some critical problems [11]. First, IRS can occupy a large surface, which results in the difficulty of deployment practically because the IRS can block a considerable area if attached to the building surface. Then, the fixed attached-to-building IRS has some non-avoidable blind zone, which causes transmission inefficiency.

On the other hand, the unmanned aerial vehicle (UAV) emerges with the advantages of high mobility and flexible deployment [12]–[14], which can solve the deployment blocking problem of IRS. In the past few years, UAVs have been endowed with tremendous values in both academic and industry owing to their characteristics [15], [16]. Benefiting from flexible mobility, convenient deployment, and low-cost reusability, UAVs are widely utilized in emergency networking, data collection, and remote cargo delivery. In addition, the introduction of UAV-aided wireless communication improves the transmission performance via superior LoS channels. Thus, lots of research effort related to UAV-aided wireless networks utilizing mobility and perfect LoS channels have been done. In [17], Chen *et al.* applied UAVs as both the relay and the warden in a long-range covert communication network. The authors considered the mobility trade-off of both the warden and the relay to maximize the transmission rate of the transmitter while maintaining the covertness. In addition, Zhu *et al.* proposed a UAV trajectory design and cluster heads (CHs) assignment scheme to minimize the energy consumption for a wireless sensor network (WSN) in [18], where a

X. Chen is with the Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, FIN-40014 Jyväskylä, Finland (email: chenxx@jyu.fi).

Z. Chang is with School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China, and also with Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, FIN-40014 Jyväskylä, Finland. (email: zheng.chang@jyu.fi).

Timo Hämäläinen is with the Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, FIN-40014 Jyväskylä, Finland (e-mail: timo.t.hamalainen@jyu.fi).

Part of this work is presented at IEEE ICC Workshops’23 [1]. Corresponding Author: Xinying Chen.

novel deep reinforcement learning (DRL) was applied to solve the optimized problem. Chen *et al.* utilized the mobility of a UAV to achieve energy efficiency via data collection trajectory optimization and guaranteed security via properly designing the transmit parameters in [19].

Attaching the IRS to an UAV can solve the deployment bottleneck of IRSs and further utilize the potential of LoS channels [20], [21]. IRS can be deployed easily and be engaged with mobility during its service [22]. On the other hand, the phase reflection design can migrate the security issues in UAV LoS channels. Few works have been conducted concerning to secure IRS-mounted UAV communications. In [23], Jiao *et al.* jointly optimized location and phase shifts of the IRS-on-UAV to maximize the transmission rate of strong link users while maintaining the minimum required rate of other users in a NOMA network. The authors improved energy efficiency of the system by jointly designing phase shifting matrix of the IRS relay and beamforming vector at the base station in [24]. The secrecy performance of an IRS-aided UAV network was analyzed by Wang *et al.* in [25], where the signal-to-noise ratio was statistically derived for both the legitimate receiver and multiple cooperate or independent eavesdroppers. Indeed, security is still critical in IRS-on-UAV networks owing to the air-ground channel links. Pang *et al.* designed a secure IRS-assisted UAV network in [26], where the trajectory, the transmit beamforming of UAV base station, and the phase shifts of relay IRS were jointly optimized to achieve the maximum averaged secrecy rate against an eavesdropper. In [27], Wei *et al.* attached an IRS on a UAV to assist direct links blocked secure transmission against several eavesdroppers, where the transmit beamforming for each access point, the location of UAV, and phase shifts of IRS relay were jointly optimized to maximize the sum secrecy rate of legitimate users under the worst secure case.

Unlike most of the research works on IRS-on-UAV only focusing on transmission performance, this paper investigates secure transmission in an IRS-assisted UAV network. Although [25] analyzed secrecy outage probability (SOP) in an IRS-in-UAV network, it primarily focused on evaluating security performance rather than directly optimizing the secure metric. Different from [27], which considers the particular situation of direct link has been blocked, we consider a more general case where each receiver can receive signals from both the direct link and the reflection link. In addition, we further apply the transmit/jamming split and beamforming solution to improve the secrecy performance. Moreover, the location and phase shifting are also jointly designed to maximize the secrecy rate. The main contributions of this paper are summarized as follows.

- We investigate the secure transmission in an IRS-on-UAV wireless network, where the mobility of UAV and the reconfiguration of IRS channel links are combined to achieve better communication performance and security. In addition, the transmit/jamming power split and beamforming are also adopted to avoid eavesdropping and achieve better transmission performance within legitimate users.
- We also jointly considers beamforming, artificial jamming, IRS phase shifting, and UAV location to optimize the secrecy rate while avoiding eavesdropping. The summarized optimization problem is non-convex and mathematically difficult to solve. Therefore, we decompose it into three subproblems and solve them iteratively and alternately.
- First, the transmit/jamming power split and beamforming vectors are jointly optimized with given phase shifting matrix and location of IRS. With the optimized beamforming vectors and a given IRS location, the phase shifts can be optimized to achieve a more considerable secrecy rate. The location of the UAV is optimized with given phase shifts and beamforming vectors to maximize the secrecy rate under the constraints. Finally, the maximum secrecy rate can be achieved by iteratively optimizing the three above-mentioned subproblems.

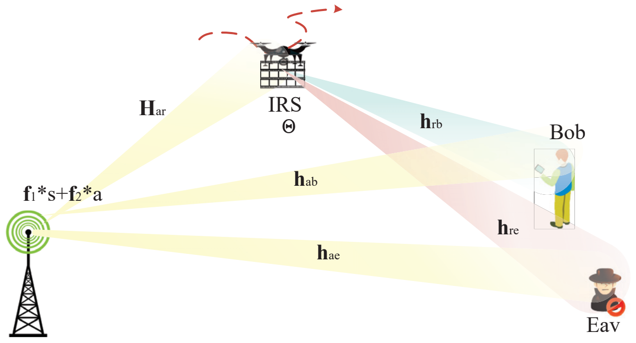


Fig. 1. IRS-on-UAV-assisted Wireless Network.

The rest of this paper is organized as follows. Section II depicts the system model and defines the key metrics used in the rest of this paper. In Section III, the secrecy rate maximization problem is formulated and alternately optimized. Simulation results are demonstrated in Section IV to evaluate the effectiveness of the proposed scheme. Section V summarized the conclusion of this work.

Notation: Boldface lowercase letter **a** and uppercase letter **A** identify vector and matrix, respectively. The $M \times N$ complex matrix can be represented by $\mathbb{C}^{M\times N}$. $|a|$ is the absolute Euclidean norm value of a complex variable a, and $||\mathbf{a}||$ stands the Euclidean norm value of vector $\mathbf{a}$. $\mathrm{diag}(\mathbf{a})$ denotes the diagonal matrix that stems the diagonal elements from vector $\boldsymbol{a}$. $\mathcal{CN}(0,1)$ stands for the complex Gaussian distribution with zero mean and unit variance. The Hermitian operation is denoted by $(*)^H$. $\mathrm{Tr}(\mathbf{A})$ represents the trace of a square matrix $\mathbf{A}$.

II. System Model

In our considered system a base station (BS) a transmits confidential information to a receiver Bob b with the assistance of an IRS r mounted on an UAV while avoiding eavesdropping from an Eav e. The BS performs precoding to optimize the power allocation between the transmit and jamming signals, enhancing both security and overall performance. Additionally, the phase shifting matrix and the location of the IRS are optimized to mitigate eavesdropping and improve the transmission rate for legitimate users. We assume that the BS is equipped with M antennas and the IRS has N reflection elements, Bob and Eav each has a single antenna. The locations of BS, IRS, Bob, and Eav are assumed at $L_a = (x_a, y_a, H)$, $L_r = (x_r, y_r, z_r)$, $L_b = (x_b, y_b, 0)$, $L_e = (x_e, y_e, 0)$, where the height of BS is set to H. The channel coefficients from the BS to Bob, and Eav are denoted as $\mathbf{h}_{ab} \in \mathbb{C}^{1\times M}$, and $\mathbf{h}_{ae} \in \mathbb{C}^{1\times M}$ and follow large-scale path loss and a small-scale Rician fading, which can be described as follows

$$\mathbf{h}_{ab} = \sqrt{\frac{\rho_0}{d_{ab}^{-\alpha}}}\mathbf{g}_{ab} = \sqrt{\frac{\rho_0}{d_{ab}^{-\alpha}}}\left(\sqrt{\frac{K_{bs}}{1+K_{bs}}}\mathbf{g}_{ab}^L + \sqrt{\frac{1}{1+K_{bs}}}\mathbf{g}_{ab}^N\right), \quad (1)$$

$$\mathbf{h}_{ae} = \sqrt{\frac{\rho_0}{d_{ae}^{-\alpha}}}\mathbf{g}_{ae} = \sqrt{\frac{\rho_0}{d_{ae}^{-\alpha}}}\left(\sqrt{\frac{K_{bs}}{1+K_{bs}}}\mathbf{g}_{ae}^L + \sqrt{\frac{1}{1+K_{bs}}}\mathbf{g}_{ae}^N\right), \quad (2)$$

where d_{ab} and d_{ae} are the distance from BS to Bob and Eav, and can be defined as

$$d_{ab} = ||L_a - L_b||, \quad (3)$$

$$d_{ae} = ||L_a - L_e||. \quad (4)$$

ρ_0 is the path loss reference at 1 m and α represents the large-scale path loss exponent. K_{bs} denotes the Rician factor between BS and terrestrial users. $\mathbf{g}_{ab}^L$, $\mathbf{g}_{ae}^L$ are the LoS components of Rician fading and follow $|g_{ab_i}^L| = 1$, and $|g_{ae_i}^L| = 1$. $\mathbf{g}_{ab}^N$, $\mathbf{g}_{ae}^N$ are the NLoS components of Rician fading, where $g_{ab_i}^N \in \mathbf{g}_{ab}^N$, and $g_{ae_i}^N \in \mathbf{g}_{ae}^N$ follow complex Gaussian distribution with zero mean and unit variance. For both LoS and NLoS components $i = \{1, \cdots, M\}$.

In addition, the channel coefficients from IRS to BS, Bob and Eav are denoted by $\mathbf{H}_{ar} \in \mathbb{C}^{N\times M}$, $\mathbf{h}_{rb} \in \mathbb{C}^{1\times N}$ and $\mathbf{h}_{re} \in \mathbb{C}^{1\times N}$, which also follow a large-scale path loss with a small-scale Rician fading, and can be described as

$$\mathbf{H}_{ar} = \sqrt{\frac{\rho_0}{d_{ar}^{-\alpha}}}\mathbf{G}_{ar} = \sqrt{\frac{\rho_0}{d_{ar}^{-\alpha}}}\left(\sqrt{\frac{K_{BI}}{1+K_{BI}}}\mathbf{G}_{ar}^L + \sqrt{\frac{1}{1+K_{BI}}}\mathbf{G}_{ar}^N\right), \quad (5)$$

$$\mathbf{h}_{rb} = \sqrt{\frac{\rho_0}{d_{rb}^{-\alpha}}}\mathbf{g}_{rb} = \sqrt{\frac{\rho_0}{d_{rb}^{-\alpha}}}\left(\sqrt{\frac{K_{IRS}}{1+K_{IRS}}}\mathbf{g}_{rb}^L + \sqrt{\frac{1}{1+K_{IRS}}}\mathbf{g}_{rb}^N\right), \quad (6)$$

$$\mathbf{h}_{re} = \sqrt{\frac{\rho_0}{d_{re}^{-\alpha}}}\mathbf{g}_{re} = \sqrt{\frac{\rho_0}{d_{re}^{-\alpha}}}\left(\sqrt{\frac{K_{IRS}}{1+K_{IRS}}}\mathbf{g}_{re}^L + \sqrt{\frac{1}{1+K_{IRS}}}\mathbf{g}_{re}^N\right), \quad (7)$$

where d_{ar}, d_{rb} and d_{re} are the distance from the IRS to BS, Bob and Eav, respectively. They can be defined as

$$d_{ar} = ||L_r - L_a||, \quad (8)$$

$$d_{rb} = ||L_r - L_b||, \quad (9)$$

$$d_{re} = ||L_r - L_e||. \quad (10)$$

In addition, K_{BI} and K_{IRS} represent the Rician factors for the IRS-BS and IRS-terrestrial user links, respectively. $\mathbf{G}_{ar}^L$, $\mathbf{g}_{rb}^L$, $\mathbf{g}_{re}^L$ are the LoS components of Rician fading and follow $|G_{ar_{ij}}^L| = 1$, $|g_{rb_i}^L| = 1$, and $|g_{re_i}^L| = 1$. $\mathbf{G}_{ar}^N$, $\mathbf{g}_{rb}^N$, $\mathbf{g}_{re}^N$ are the NLoS components of Rician fading, where $G_{ar_{ij}}^N \in \mathbf{G}_{ar}^N$, $g_{rb_i}^N \in \mathbf{g}_{rb}^N$, and $g_{re_i}^N \in \mathbf{g}_{re}^N$ follow complex Gaussian distribution with zero mean and unit variance.

We use $\mathbf{\Theta} = \mathrm{diag}(\mathrm{e}^{\mathrm{j}\theta_1}, \cdots, \mathrm{e}^{\mathrm{j}\theta_\mathrm{N}})$ to denote the diagonal phase shifting matrix of IRS, where $\theta_i \in [0, 2\pi), \forall i \in \{1, \cdots, N\}$, is the phase shift of the i-th element on the IRS. As for the IRS undergoing the passive reflection, we assume that IRS applys the time-division-duplexing (TDD) protocol. In addition, we also assume that the channel state information (CSI) within this network is known, which can be obtained through channel sounding, CSI feedback, and fast CSI reporting techniques[1]. The BS uses precoding vector $\mathbf{f}_1 \in \mathbb{C}^{M\times 1}$ and jamming vector $\mathbf{f}_2 \in \mathbb{C}^{M\times 1}$ for independent confidential signals $s[t] \sim \mathcal{CN}(0,1)$ and jamming signals $j[t] \sim \mathcal{CN}(0,1)$, where $\mathbf{f}_1^H\mathbf{f}_1 + \mathbf{f}_2^H\mathbf{f}_2 \le P_{amax}$, respectively. P_{amax} is the maximum allowed total transmit power at BS. Thus, the received signal at Bob and Eav can be respectively described as

$$y_b = (\mathbf{h}_{ab} + \mathbf{h}_{rb}\mathbf{\Theta}\mathbf{H}_{ar})(\mathbf{f}_1 s[t] + \mathbf{f}_2 j[t]) + n_b[t], \quad (11)$$

and

$$y_e = (\mathbf{h}_{ae} + \mathbf{h}_{re}\mathbf{\Theta}\mathbf{H}_{ar})(\mathbf{f}_1 s[t] + \mathbf{f}_2 j[t]) + n_e[t], \quad (12)$$

where $n_b[t]$ and $n_e[t]$ denote the noise received at Bob and Willie, respectively. Without loss of generality, we assume both $n_b[t]$ and $n_e[t]$ follow Gaussian distribution with zero mean and variance of σ^2. Therefore, the maximum achievable transmission rate at Bob and the eavesdropping rate at Eav can be described as

$$R_b = \log_2\left(1 + \frac{|(\mathbf{h}_{ab} + \mathbf{h}_{rb}\mathbf{\Theta}\mathbf{H}_{ar})\mathbf{f}_1|^2}{|(\mathbf{h}_{ab} + \mathbf{h}_{rb}\mathbf{\Theta}\mathbf{H}_{ar})\mathbf{f}_2|^2 + \sigma^2}\right), \quad (13)$$

and

$$R_e = \log_2\left(1 + \frac{|(\mathbf{h}_{ae} + \mathbf{h}_{re}\mathbf{\Theta}\mathbf{H}_{ar})\mathbf{f}_1|^2}{|(\mathbf{h}_{ae} + \mathbf{h}_{re}\mathbf{\Theta}\mathbf{H}_{ar})\mathbf{f}_2|^2 + \sigma^2}\right). \quad (14)$$

Then, the secrecy rate at Bob can be defined as

$$R_s = [R_b - R_e]^+, \quad (15)$$

where $[*]^+$ represents $\max(*, 0)$.

III. Problem Formulation

We aim to achieve a higher secrecy rate via jointly designing the precoding vector $\boldsymbol{f}_1$, jamming vector $\boldsymbol{f}_2$, phase shifting matrix $\mathbf{\Theta}$ of IRS, and the location L_r of UAV while constrained by the phase angles at IRS, and the total emit power P_{amax} at BS. Correspondingly, the optimization problem can be formulated as

$$\begin{aligned}
\textbf{P1:} \quad \max_{\boldsymbol{f}_1, \boldsymbol{f}_2, \mathbf{\Theta}, L_r} \quad & R_s & (16a)\\
s.t. \quad & R_b \ge R_{min}, & (16b)\\
& \theta_i \in [0, 2\pi), & (16c)\\
& \mathbf{f}_1^H\mathbf{f}_1 + \mathbf{f}_2^H\mathbf{f}_2 \le P_{amax}, & (16d)\\
& R_e \le r_e, & (16e)
\end{aligned}$$

[1] The results with perfect CSI provide an upper bound for scenarios with real, estimated CSI, highlighting the potential performance limits.

where (16b) guarantee the transmission performance of legitimate receiver, and (16e) provides an additional layer of security beyond R_s. (16) has a non-convex structure and is difficult to solve. Thus, we propose an iterative algorithm to solve the considered problem by alternately optimizing $\boldsymbol{f}_1$, $\boldsymbol{f}_2$, $\boldsymbol{\Theta}$, and L_r.

As observed from (16), L_r is constrained by (16b) and (16e), $\boldsymbol{\Theta}$ is only constrained by (16c) and $\boldsymbol{f}_1$, $\boldsymbol{f}_2$ are only constrained by (16d). Thus, we can solve the optimization problem via alternately optimizing L_r, $\boldsymbol{\Theta}$, $\boldsymbol{f}_1$, and $\boldsymbol{f}_2$. First, we optimize $\boldsymbol{f}_1$ and $\boldsymbol{f}_2$ with given L_r and $\boldsymbol{\Theta}$. Then, the optimized $\boldsymbol{\Theta}$ can be derived from P1 under given L_r, $\boldsymbol{f}_1$, and $\boldsymbol{f}_2$. Finally, we optimize L_r with given $\boldsymbol{\Theta}$, $\boldsymbol{f}_1$, and $\boldsymbol{f}_2$.

A. Optimization of $\boldsymbol{f}_1$ and $\boldsymbol{f}_2$ With Given L_r and $\boldsymbol{\Theta}$

First, we optimize $\boldsymbol{f}_1$ and $\boldsymbol{f}_2$ under the given L_r and $\boldsymbol{\Theta}$. To make the expression of R_s clearer, we change $\mathbf{h}_{rb}\boldsymbol{\Theta}\mathbf{H}_{ar}$ and $\mathbf{h}_{re}\boldsymbol{\Theta}\mathbf{H}_{ar}$ to

$$\mathbf{h}_{rb}\boldsymbol{\Theta}\mathbf{H}_{ar} = \boldsymbol{\theta}\mathrm{diag}(\mathbf{h}_{\mathrm{rb}})\mathbf{H}_{\mathrm{ar}} = \boldsymbol{\theta}\mathbf{H}_{\mathrm{arb}}, \tag{17}$$

$$\mathbf{h}_{re}\boldsymbol{\Theta}\mathbf{H}_{ar} = \boldsymbol{\theta}\mathrm{diag}(\mathbf{h}_{\mathrm{re}})\mathbf{H}_{\mathrm{ar}} = \boldsymbol{\theta}\mathbf{H}_{\mathrm{are}}, \tag{18}$$

where $\boldsymbol{\theta} = [\Theta_{11}, \Theta_{22}, \cdots, \Theta_{NN}]$, $\mathbf{H}_{arb} = \mathrm{diag}(\mathbf{h}_{\mathrm{rb}})\mathbf{H}_{\mathrm{ar}}$, and $\mathbf{H}_{are} = \mathrm{diag}(\mathbf{h}_{\mathrm{re}})\mathbf{H}_{\mathrm{ar}}$.

Furthermore, by setting $(\boldsymbol{\theta}\mathbf{H}_{arb}+\mathbf{h}_{ab})^H(\boldsymbol{\theta}\mathbf{H}_{arb}+\mathbf{h}_{ab}) = \mathbf{H}_b$ and $(\boldsymbol{\theta}\mathbf{H}_{are}+\mathbf{h}_{ae})^H(\boldsymbol{\theta}\mathbf{H}_{are}+\mathbf{h}_{ae}) = \mathbf{H}_e$, the expression of R_b and R_e can be altered into

$$R_b = \log_2\left(1 + \frac{\mathbf{f}_1^H\mathbf{H}_b\mathbf{f}_1}{\mathbf{f}_2^H\mathbf{H}_b\mathbf{f}_2 + \sigma^2}\right), \tag{19}$$

and

$$R_e = \log_2\left(1 + \frac{\mathbf{f}_1^H\mathbf{H}_e\mathbf{f}_1}{\mathbf{f}_2^H\mathbf{H}_e\mathbf{f}_2 + \sigma^2}\right). \tag{20}$$

By applying the semidefinite relaxation (SDR) on R_b, we have

$$\mathbf{f}_1^H\mathbf{H}_b\mathbf{f}_1 = \mathrm{Tr}(\mathbf{H}_{\mathrm{b}}\mathbf{f}_1\mathbf{f}_1^{\mathrm{H}}), \tag{21}$$

and

$$\mathbf{f}_2^H\mathbf{H}_b\mathbf{f}_2 = \mathrm{Tr}(\mathbf{H}_{\mathrm{b}}\mathbf{f}_2\mathbf{f}_2^{\mathrm{H}}). \tag{22}$$

This also applies to R_e. Therefore, with given L_r and $\boldsymbol{\Theta}$, P1 can be changed into

$$\textbf{P1.1:} \max_{\mathbf{F}_1,\mathbf{F}_2} \log_2\!\left(1+\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}\mathbf{F}_1)}{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}\mathbf{F}_2)+\sigma^2}\right) - \log_2\!\left(1+\frac{\mathrm{Tr}\left(\mathbf{H}_{\mathrm{e}}\mathbf{F}_2\right)}{\mathrm{Tr}(\mathbf{H}_{\mathrm{e}}\mathbf{F}_2)+\sigma^2}\right) \tag{23a}$$

$$s.t.\quad \log_2\!\left(1+\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}\mathbf{F}_1)}{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}\mathbf{F}_2)+\sigma^2}\right) \geq R_{min}, \tag{23b}$$

$$\mathrm{Tr}\left(\mathbf{F}_1 + \mathbf{F}_2\right) \leq \mathrm{P}_{\mathrm{amax}}, \tag{23c}$$

$$\log_2\!\left(1+\frac{\mathrm{Tr}\left(\mathbf{H}_{\mathrm{e}}\mathbf{F}_2\right)}{\mathrm{Tr}(\mathbf{H}_{\mathrm{e}}\mathbf{F}_2)+\sigma^2}\right) \leq r_e, \tag{23d}$$

where $\mathbf{F}_1 = \mathbf{f}_1\mathbf{f}_1^H$ and $\mathbf{F}_2 = \mathbf{f}_2\mathbf{f}_2^H$. Nonetheless, P1.1 is still non-convex and thus mathematical unsolvable. We utilize the following Lemma 1 to convert (23a) to a simpler version [28].

Lemma 1: For a given function $f(t) = -tx + \ln t + 1, \forall x > 0$, we have

$$\max_{t>0} f(t) = -\ln x, \tag{24}$$

where the optimal value is $t^* = \frac{1}{x}$.

Based on Lemma 1 and let $x = \frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}\mathbf{F}_2)}{\sigma^2} + 1$, R_b can be changed into

$$\begin{aligned} R_b =& \frac{\left(\ln\left(\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}(\mathbf{F}_1+\mathbf{F}_2))}{\sigma^2}+1\right) - \ln\left(\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}(\mathbf{F}_2))}{\sigma^2}+1\right)\right)}{\ln 2} \\ =& \max_{t_b} \frac{\ln\left(\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}(\mathbf{F}_1+\mathbf{F}_2))}{\sigma^2}+1\right) - t_b\left(\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}\mathbf{F}_2)}{\sigma^2}+1\right) + \ln t_b + 1}{\ln 2}. \end{aligned} \tag{25}$$

Similarly, by setting $x = \frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{e}}(\mathbf{F}_1+\mathbf{F}_2))}{\sigma^2} + 1$, $-R_e$ can be rewritten as

$$-R_e = \max_{t_e} \frac{-t_e\left(\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{e}}(\mathbf{F}_1+\mathbf{F}_2))}{\sigma^2}+1\right) + \ln t_e + 1 + \ln\left(\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{e}}\mathbf{F}_2)}{\sigma^2}+1\right)}{\ln 2}. \tag{26}$$

According to Lemma 1, the optimal t_b^* and t_e^* can be described as

$$t_b^* = \left[\frac{1}{\sigma^2}\mathrm{Tr}\left(\mathbf{H}_{\mathrm{b}}\mathbf{F}_2\right) + 1\right]^{-1}, \tag{27}$$

and

$$t_e^* = \left[\frac{1}{\sigma^2}\mathrm{Tr}\left(\mathbf{H}_{\mathrm{e}}\left(\mathbf{F}_1 + \mathbf{F}_2\right)\right) + 1\right]^{-1}, \tag{28}$$

Accordingly, the achievable maximum R_b and R_e can be expressed as

$$R_b^* = \frac{\ln\left(\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}(\mathbf{F}_1+\mathbf{F}_2))}{\sigma^2}+1\right) - t_b\left(\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{b}}\mathbf{F}_2)}{\sigma^2}+1\right) + \ln t_b + 1}{\ln 2}. \tag{29}$$

$$R_e^* = \frac{t_e^*\left(\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{e}}(\mathbf{F}_1+\mathbf{F}_2))}{\sigma^2}+1\right) - \ln t_e^* - 1 - \ln\left(\frac{\mathrm{Tr}(\mathbf{H}_{\mathrm{e}}\mathbf{F}_2)}{\sigma^2}+1\right)}{\ln 2}. \tag{30}$$

Then, **P1.1** can be changed into

$$\begin{aligned} \textbf{P1.1.1:} \max_{\mathbf{F}_1,\mathbf{F}_2}\ & \frac{1}{\ln 2}\Bigg\{\ln\left(\frac{1}{\sigma^2}\mathrm{Tr}\left(\mathbf{H}_{\mathrm{b}}\left(\mathbf{F}_1+\mathbf{F}_2\right)\right)+1\right) + \ln t_b^* + 1 \\ & - t_b^*\left(\frac{1}{\sigma^2}\mathrm{Tr}\left(\mathbf{H}_{\mathrm{b}}\mathbf{F}_2\right)+1\right) + \ln\left(\frac{1}{\sigma^2}\mathrm{Tr}\left(\mathbf{H}_{\mathrm{e}}\mathbf{F}_2\right)+1\right) \\ & - t_e^*\left(\frac{1}{\sigma^2}\mathrm{Tr}(\mathbf{H}_{\mathrm{e}}(\mathbf{F}_1+\mathbf{F}_2))+1\right) + \ln t_e^* + 1\Bigg\} \end{aligned} \tag{31a}$$

$$\begin{aligned} s.t.\ & \frac{1}{\ln 2}\Bigg\{\ln\left(\frac{1}{\sigma^2}\mathrm{Tr}\left(\mathbf{H}_{\mathrm{b}}\left(\mathbf{F}_1+\mathbf{F}_2\right)\right)+1\right) + \ln t_b^* + 1 \\ & - t_b^*\left(\frac{1}{\sigma^2}\mathrm{Tr}\left(\mathbf{H}_{\mathrm{b}}\mathbf{F}_2\right)\right)\Bigg\} \geq R_{min}, \end{aligned} \tag{31b}$$

$$\mathrm{Tr}\left(\mathbf{F}_1 + \mathbf{F}_2\right) \leq \mathrm{P}_{\mathrm{amax}}, \tag{31c}$$

$$\begin{aligned} & \frac{1}{\ln 2}\Bigg\{-\ln\left(\frac{1}{\sigma^2}\mathrm{Tr}\left(\mathbf{H}_{\mathrm{e}}\mathbf{F}_2\right)+1\right) - \ln t_e^* - 1 \\ & + t_e^*\left(\frac{1}{\sigma^2}\mathrm{Tr}\left(\mathbf{H}_{\mathrm{e}}\left(\mathbf{F}_1+\mathbf{F}_2\right)\right)+1\right)\Bigg\}. \end{aligned} \tag{31d}$$

P1.1.1 is a convex problem and mathematically solvable, and the optimal $\mathbf{F}_1$, $\mathbf{F}_2$ can be derived via toolbox, i.e., cvx. Then, $\mathbf{f}_1$ and $\mathbf{f}_2$ can be re-constructed from $\mathbf{F}_1$, $\mathbf{F}_2$.

$$R_s^* = \frac{\ln\left[\frac{\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{b1}}+\tilde{\mathbf{H}}_{\mathrm{b2}}\right)\tilde{\mathbf{\Theta}}}{\sigma^2}+1\right]+\ln S_b^*+1-S_b^*\left[\frac{\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{b2}}\tilde{\mathbf{\Theta}}\right)}{\sigma^2}+1\right]+\ln\left[\frac{\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{e2}}\tilde{\mathbf{\Theta}}\right)}{\sigma^2}+1\right]-S_e^*\left[\frac{\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{e1}}+\tilde{\mathbf{H}}_{\mathrm{e2}}\right)\tilde{\mathbf{\Theta}}}{\sigma^2}+1\right]+\ln S_e^*+1}{\ln 2} \tag{39}$$

B. Optimization of $\mathbf{\Theta}$ With Given L_r, $\boldsymbol{f}_1$, and $\boldsymbol{f}_2$

In this subsection, we derive the optimal $\mathbf{\Theta}$ with given $\mathbf{f}_1$, $\mathbf{f}_2$, and L_r for the optimization problem **P1**.

The channel gain from BS to IRS and then to Bob can be denoted as $\mathbf{h}_{rb}\mathbf{\Theta}\mathbf{H}_{ar}$ refering to (17). In addition, we further define $\tilde{\boldsymbol{\theta}}$ and $\tilde{\boldsymbol{H}}_b$ to simplify the expression of R_b as

$$\tilde{\boldsymbol{\theta}} = [\boldsymbol{\theta} \quad 1], \tag{32}$$

$$\tilde{\boldsymbol{H}}_b = \begin{pmatrix} \mathbf{H}_{arb} \\ \mathbf{h}_{ab} \end{pmatrix} \tag{33}$$

Then, R_b in (13) can be altered into a simpler expression as

$$R_b = \log_2\left(1+\frac{\left|\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_b\mathbf{f}_1\right|^2}{\left|\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_b\mathbf{f}_2\right|^2+\sigma^2}\right), \tag{34}$$

Let $\tilde{\boldsymbol{H}}_{b1} = \tilde{\boldsymbol{H}}_b\mathbf{f}_1\mathbf{f}_1^H\tilde{\boldsymbol{H}}_b^H$ and $\tilde{\boldsymbol{H}}_{b2} = \tilde{\boldsymbol{H}}_b\mathbf{f}_2\mathbf{f}_2^H\tilde{\boldsymbol{H}}_b^H$. Then, R_b in (34) can be changed into

$$R_b = \log_2\left(1+\frac{\frac{1}{\sigma^2}\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_{b1}\tilde{\boldsymbol{\theta}}^H}{\frac{1}{\sigma^2}\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_{b2}\tilde{\boldsymbol{\theta}}^H+1}\right), \tag{35}$$

Similarly, by letting $\mathbf{H}_{are} = \mathrm{diag}(\mathbf{h}_{\mathrm{re}})\mathbf{H}_{\mathrm{ar}}$, we can also define $\tilde{\boldsymbol{H}}_e$ as

$$\tilde{\boldsymbol{H}}_e = \begin{pmatrix} \mathbf{H}_{are} \\ \mathbf{h}_{ae}, \end{pmatrix} \tag{36}$$

Then, we also define $\tilde{\boldsymbol{H}}_{e1} = \tilde{\boldsymbol{H}}_e\mathbf{f}_1\mathbf{f}_1^H\tilde{\boldsymbol{H}}_e^H$ and $\tilde{\boldsymbol{H}}_{e2} = \tilde{\boldsymbol{H}}_e\mathbf{f}_2\mathbf{f}_2^H\tilde{\boldsymbol{H}}_e^H$. Thus, R_e in (14) can be changed into

$$R_e = \log_2\left(1+\frac{\frac{1}{\sigma^2}\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_{e1}\tilde{\boldsymbol{\theta}}^H}{\frac{1}{\sigma^2}\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_{e2}\tilde{\boldsymbol{\theta}}^H+1}\right), \tag{37}$$

However, the optimized problem is still non-convex. By applying SDR, R_s can be changed into

$$R_s = \frac{\ln\left(\frac{\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{b1}}\tilde{\mathbf{\Theta}}\right)}{\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{b2}}\tilde{\mathbf{\Theta}}\right)+1}+1\right)-\ln\left(\frac{\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{e1}}\tilde{\mathbf{\Theta}}\right)}{\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{e2}}\tilde{\mathbf{\Theta}}\right)+1}+1\right)}{\ln 2}. \tag{38}$$

Additionally, given $\mathbf{f}_1$, $\mathbf{f}_2$, and L_r, and following the expressions for R_b^* in (29) and R_e^* in (30), the achievable optimal secrecy rate R_s^* can be expressed as (39) at the top of this page. Then, **P1** can be turned into

$$\begin{aligned} \textbf{P1.2:} \max_{\tilde{\mathbf{\Theta}}} \quad & R_s^* && \text{(40a)} \\ s.t. \quad & \tilde{\mathbf{\Theta}} \succeq 0, && \text{(40b)} \\ & \tilde{\mathbf{\Theta}}_{nn} = 1, && \text{(40c)} \\ & \frac{1}{\ln 2}\ln\left(\frac{\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{e1}}\tilde{\mathbf{\Theta}}\right)}{\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{e2}}\tilde{\mathbf{\Theta}}\right)+1}+1\right) \leq r_e, && \text{(40d)} \end{aligned}$$

where $\tilde{\mathbf{\Theta}} = \tilde{\boldsymbol{\theta}}^H\tilde{\boldsymbol{\theta}} \in \mathbb{C}^{(N+1)\times(N+1)}$. S_b^* and S_e^* can be derived according to Lemma 1 as

$$S_b^* = \left[\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathbf{H}}_{\mathrm{b2}}\tilde{\mathbf{\Theta}}^{(\mathrm{r})}\right)+1\right]^{-1}, \tag{41}$$

and

$$S_e^* = \left[\frac{1}{\sigma^2}\mathrm{Tr}\left(\left(\tilde{\mathbf{H}}_{\mathrm{e1}}+\tilde{\mathbf{H}}_{\mathrm{e2}}\right)\tilde{\mathbf{\Theta}}^{(\mathrm{r})}\right)+1\right]^{-1}. \tag{42}$$

$\tilde{\mathbf{\Theta}}^{(r)}$ is the optimal value derived from the r-th iteration. To this end, **P1.2** is convex and mathematically solvable by alternately optimization via tool box, i.e., CVX. To obtain $\mathbf{\Theta}$ from $\tilde{\mathbf{\Theta}}$, we can apply eigenvalue decomposition via Gaussian randomizing.

C. Optimization of L_r With Given $\boldsymbol{f}_1$, $\boldsymbol{f}_2$, and $\mathbf{\Theta}$

With the given $\mathbf{f}_1$, $\mathbf{f}_2$, and $\mathbf{\Theta}$, the optimization problem **P1** can be changed into

$$\begin{aligned} \textbf{P1.3:} \max_{L_r,m,n,x,y} \; & \log_2\left(\frac{\left|\left(d_{ar}^{-\frac{\alpha}{2}}d_{rb}^{-\frac{\alpha}{2}}\tilde{\mathbf{g}}_{ab}^r+\mathbf{h}_{ab}\right)\mathbf{f}_1\right|^2}{\left|\left(d_{ar}^{-\frac{\alpha}{2}}d_{rb}^{-\frac{\alpha}{2}}\tilde{\mathbf{g}}_{ab}^r+\mathbf{h}_{ab}\right)\mathbf{f}_2\right|^2+\sigma^2}+1\right)- \\ & \log_2\left(\frac{\left|\left(d_{ar}^{-\frac{\alpha}{2}}d_{re}^{-\frac{\alpha}{2}}\tilde{\mathbf{g}}_{ae}^r+\mathbf{h}_{ae}\right)\mathbf{f}_1\right|^2}{\left|\left(d_{ar}^{-\frac{\alpha}{2}}d_{re}^{-\frac{\alpha}{2}}\tilde{\mathbf{g}}_{ae}^r+\mathbf{h}_{ae}\right)\mathbf{f}_2\right|^2+\sigma^2}+1\right) && \text{(43a)} \\ & s.t. R_b \geq R_{min}, && \text{(43b)} \\ & d_{ar}^2 \leq m, && \text{(43c)} \\ & d_{rb}^2 \leq n, && \text{(43d)} \\ & d_{ar}^2 \geq \mathrm{e}^{-\mathrm{x}}, && \text{(43e)} \\ & d_{re}^2 \geq \mathrm{e}^{-\mathrm{y}}, && \text{(43f)} \\ & R_e \leq r_e, && \text{(43g)} \end{aligned}$$

where R_{min} denotes the minimum required transmission rate. m, n, x, and y are four introduced auxiliary variables, which guarantee the convexity by (43c), (43d), (43e), (43f).

Furthermore, $\tilde{\mathbf{g}}_{ab}^r$ and $\tilde{\mathbf{g}}_{ae}^r$ are defined to simplify the expression of the optimization problem as

$$\tilde{\mathbf{g}}_{ab}^r = \rho_0\mathbf{g}_{rb}\mathbf{\Theta}\mathbf{G}_{ar}, \tag{44}$$

and

$$\tilde{\mathbf{g}}_{ae}^r = \rho_0\mathbf{g}_{re}\mathbf{\Theta}\mathbf{G}_{ar}. \tag{45}$$

However, (43a) and (43b) are still non-convex and mathematically intractable, both of which are required to alter into concave with respect to m, n, x, and y. We apply the first-order Taylor expansion on (43b) to change it into concave with

$$R_b^{m'}(m_k,n_k) = \frac{-\frac{\alpha}{2}m^{-\frac{\alpha}{2}-1}}{\Gamma_n^k \ln 2}\left\{\frac{\left[\left({R_1^m}^2+{I_1^m}^2\right)\left(R_3^m R_4+I_3^m I_4\right)-\left({R_3^m}^2+{I_3^m}^2\right)\left(R_1^m R_2+I_1^m I_2\right)\right]{B_k}^2}{\left({R_3^m}^2+{I_3^m}^2\right){B_k}^2+\left(R_3^m R_4+I_3^m I_4\right)B_k+{R_4}^2+{I_4}^2+\sigma^2}\right.$$
$$+\frac{\left[\left({R_1^m}^2+{I_1^m}^2\right)\left({R_4}^2+{I_4}^2+\sigma^2\right)-\left({R_3^m}^2+{I_3^m}^2\right)\left({R_2}^2+{I_2}^2\right)\right]B_k}{\left({R_3^m}^2+{I_3^m}^2\right){B_k}^2+\left(R_3^m R_4+I_3^m I_4\right)B_k+{R_4}^2+{I_4}^2+\sigma^2} \tag{47}$$
$$\left.+\frac{\left({R_1^m}^2+{I_1^m}^2\right)\left({R_4}^2+{I_4}^2+\sigma^2\right)-\left(R_3^m R_4+I_3^m I_4\right)\left({R_2}^2+{I_2}^2\right)}{\left({R_3^m}^2+{I_3^m}^2\right){B_k}^2+\left(R_3^m R_4+I_3^m I_4\right)B_k+{R_4}^2+{I_4}^2+\sigma^2}\right\}.$$

$$R_b^{n'}(m_k,n_k) = \frac{-\frac{\alpha}{2}m^{-\frac{\alpha}{2}-1}}{\Gamma_n^k \ln 2}\left\{\frac{\left[\left({R_1^n}^2+{I_1^n}^2\right)\left(R_3^n R_4+I_3^n I_4\right)-\left({R_3^n}^2+{I_3^n}^2\right)\left(R_1^n R_2+I_1^n I_2\right)\right]{A_k}^2}{\left({R_3^n}^2+{I_3^n}^2\right){A_k}^2+\left(R_3^n R_4+I_3^n I_4\right)A_k+{R_4}^2+{I_4}^2+\sigma^2}\right.$$
$$+\frac{\left[\left({R_1^n}^2+{I_1^n}^2\right)\left({R_4}^2+{I_4}^2+\sigma^2\right)-\left({R_3^n}^2+{I_3^n}^2\right)\left({R_2}^2+{I_2}^2\right)\right]A_k}{\left({R_3^n}^2+{I_3^n}^2\right){A_k}^2+\left(R_3^n R_4+I_3^n I_4\right)A_k+{R_4}^2+{I_4}^2+\sigma^2} \tag{53}$$
$$\left.+\frac{\left({R_1^n}^2+{I_1^n}^2\right)\left({R_4}^2+{I_4}^2+\sigma^2\right)-\left(R_3^n R_4+I_3^n I_4\right)\left({R_2}^2+{I_2}^2\right)}{\left({R_3^n}^2+{I_3^n}^2\right){A_k}^2+\left(R_3^n R_4+I_3^n I_4\right)A_k+{R_4}^2+{I_4}^2+\sigma^2}\right\}.$$

respect to m and n. The first-order Taylor expansion of R_b in (43b) at a given point (m_k, n_k) can be expressed as

$$\begin{aligned} R_b(m,n) =& R_b(m_k,n_k) + R_b^{m'}(m_k,n_k)(m-m_k) \\ &+ R_b^{n'}(m_k,n_k)(n-n_k) + o(m-m_k, n-n_k) \\ \geq& R_b(m_k,n_k) + R_b^{m'}(m_k,n_k)(m-m_k) \\ &+ R_b^{n'}(m_k,n_k)(n-n_k) = R_b^l(m,n), \end{aligned} \tag{46}$$

where $R_b^{m'}(m_k,n_k)$ and $R_b^{n'}(m_k,n_k)$ represent the first-order derivative of $R_b(m,n)$ with respect of m and n, respectively. $o(m-m_k, n-n_k)$ is the higher-order infinitesimal of $R_b(m,n)$. $R_b^{m'}(m_k,n_k)$ is demonstrated in (47) on the top of this page.

In (47), $B_k = {n_k}^{-\frac{\alpha}{4}}$. And Γ_n^k is defined as

$$\Gamma_n^k = \frac{\left|\left({m_k}^{-\frac{\alpha}{4}}{n_k}^{-\frac{\alpha}{4}}\tilde{\mathbf{g}}_{ab}^r + \mathbf{h}_{ab}\right)\mathbf{f}_1\right|^2}{\left|\left({m_k}^{-\frac{\alpha}{4}}{n_k}^{-\frac{\alpha}{4}}\tilde{\mathbf{g}}_{ab}^r + \mathbf{h}_{ab}\right)\mathbf{f}_2\right|^2 + \sigma^2} + 1. \tag{48}$$

In addition, R_1^m, I_1^m, R_2, I_2, R_3^m, I_3^m, R_4, and I_4 in (47) can be defined as

$$B_k\tilde{\mathbf{g}}_{ab}^r\mathbf{f}_1 = R_1^m + iI_1^m, \tag{49}$$

$$\mathbf{h}_{ab}\mathbf{f}_1 = R_2 + iI_2, \tag{50}$$

$$B_k\tilde{\mathbf{g}}_{ab}^r\mathbf{f}_2 = R_3^m + iI_3^m, \tag{51}$$

$$\mathbf{h}_{ab}\mathbf{f}_2 = R_4 + iI_4, \tag{52}$$

where i represents the imaginary unit in a complex number.

On the other hand, $R_b^{n'}(m_k,n_k)$ can be demonstrated in (53) at the top of this page, where $A_k = {m_k}^{-\frac{\alpha}{4}}$. We further define R_1^n, I_1^n, R_3^n, and I_3^n in (53) as

$$A_k\tilde{\mathbf{g}}_{ab}^r\mathbf{f}_1 = R_1^n + iI_1^n, \tag{54}$$

$$A_k\tilde{\mathbf{g}}_{ab}^r\mathbf{f}_2 = R_3^n + iI_3^n. \tag{55}$$

Thus, according to (46) and Taylor's theorem we can conclude

$$R_b(m,n) \geq R_b^l(m,n). \tag{56}$$

Then, the first part in (43a) turns to concave and mathematically solvable. With R_e further altered into a convex version, (43) becomes solvable.

By utilizing the first-order Taylor expansion, d_{ar}^2 and d_{re}^2 can be changed into

$$d_{ar}^2 \geq ||L_r^{(k)} - L_a||^2 + 2(L_r^{(k)} - L_a)(L_r - L_r^{(k)})^T \geq \mathrm{e}^{-\mathrm{x}}, \tag{57}$$

and

$$d_{re}^2 \geq ||L_r^{(k)} - L_e||^2 + 2(L_r^{(k)} - L_e)(L_r - L_r^{(k)})^T \geq \mathrm{e}^{-\mathrm{y}}, \tag{58}$$

which are convex. By defining

$$R_e(x,y) = \log_2\left(\frac{\left|\left((\mathrm{e}^{-\mathrm{x}})^{-\frac{\alpha}{4}}(\mathrm{e}^{-\mathrm{y}})^{-\frac{\alpha}{4}}\tilde{\mathbf{g}}_{ae}^r + \mathbf{h}_{ae}\right)\mathbf{f}_1\right|^2}{\left|\left((\mathrm{e}^{-\mathrm{x}})^{-\frac{\alpha}{4}}(\mathrm{e}^{-\mathrm{y}})^{-\frac{\alpha}{4}}\tilde{\mathbf{g}}_{ae}^r + \mathbf{h}_{ae}\right)\mathbf{f}_2\right|^2 + \sigma^2} + 1\right), \tag{59}$$

we can conclude $R_e \leq R_e(x,y)$. The first-order Taylor expansion of $R_e(x,y)$ can be demonstrated as

$$\tilde{R}_e(x,y) = R_e(x_k,y_k) + R_e^{x'}(x_k,y_k)(x-x_k) + R_e^{y'}(x_k,y_k)(y-y_k), \tag{60}$$

where $R_e^{x'}(x_k,y_k)$ represents the first-order derivative of R_e with respect to x at (x_k,y_k), and $R_e^{y'}(x_k,y_k)$ is the first-order derivative with respect to y at (x_k,y_k). Similar to (47), the detailed derivation can be referred to from Appendix A.

Thus, the optimization subproblem **P1.3** can be transformed to a convex version as follows.

P1.3.1:

$$\max_{L_r,m,n,x,y,R_e} \; R_b^l(m,n) - R_e \tag{61a}$$

$$s.t. \; R_b^l(m,n) \geq R_{min}, \tag{61b}$$

$$d_{ar}^2 \leq m, \tag{61c}$$

$$d_{rb}^2 \leq n, \tag{61d}$$

$$d_{ar}^2 \geq \mathrm{e}^{-\mathrm{x}}, \tag{61e}$$

$$d_{re}^2 \geq \mathrm{e}^{-\mathrm{y}}, \tag{61f}$$

$$R_e \geq \tilde{R}_e^{(}x,y), \tag{61g}$$

which can be solved easily via existing tool box, i.e., CVX.

D. *Overall Algorithm*

The proposed algorithm improves the secure performance effectively in an IRS-aided network via alternatively solving sub-problems alternatively until reaching convergence with another two parameters given. The overall algorithm can be summarized in Algorithm 1. In Algorithm 1, each subproblem is solved optimally at each iteration, ensuring that the overall R_s either increases or remains the same. Due to the convexity of the transformed sub-problems, this approach guarantees a non-decrease in the objective function value. As a result, the iterative process converges to at least a local optimal solution after a finite number of iterations. The time complexity of Algorithm 1 mainly results from outer iteration as well as the inner iteration of step 5, 11, and 17. For step 5, the complexity of solving P1.1.1 is $\mathcal{O}(\log(\frac{1}{\epsilon_f})M^{4.5})$, where ϵ_f is the solution accuracy for convergence [29]. For step 11, the complexity of solving P1.2 is $\mathcal{O}(\log(\frac{1}{\epsilon_I})N^{4.5})$, where ϵ_I is the solution accuracy. For step 17, the complexity of solving P1.3.1 is $\mathcal{O}(\log(\frac{1}{\epsilon_U}))$, where ϵ_U is the solution accuracy. Therefore, the overall computational complexity of Algorithm 1 is $\mathcal{O}\left(\log(\frac{1}{\epsilon})\left(\log(\frac{1}{\epsilon_f})M^{4.5}+\log(\frac{1}{\epsilon_I})N^{4.5}+\log(\frac{1}{\epsilon_U})\right)\right)$, where ϵ is the overall solution accuracy.

Algorithm 1 Proposed Algorithm

```
1:  **Initialization:** Initialize $\mathbf{f}_1^{(0)}, \mathbf{f}_2^{(0)}, \tilde{\mathbf{\Theta}}^{(0)}, L_r^{(0)}$ and set iteration index $i = 0$.
2:  **repeat**
3:      **Step 1: Optimize Beamforming Vectors**
4:      **repeat**
5:          Given $\mathbf{\Theta}^{(0)}$ and $L_r^{(0)}$, find the optimal $\mathbf{f}_1^{(j)}$ and $\mathbf{f}_2^{(j)}$ by solving P1.1.1.
6:          Update $j = j + 1$.
7:      **until** Convergence of P1.1.1 is reached.
8:      Set $\mathbf{f}_1^{(0)} \leftarrow \mathbf{f}_1^{(j)}$, $\mathbf{f}_2^{(0)} \leftarrow \mathbf{f}_2^{(j)}$.
9:      **Step 2: Optimize IRS Phase-Shifting Matrix**
10:     **repeat**
11:         Given $\mathbf{f}_1^{(0)}, \mathbf{f}_2^{(0)}$, and $L_r^{(0)}$, find the optimal $\tilde{\mathbf{\Theta}}^{(m)}$ by solving P1.2.
12:         Update $m = m + 1$.
13:     **until** Convergence of P1.2 is reached.
14:     Recover and update $\mathbf{\Theta}^{(0)} \leftarrow \tilde{\mathbf{\Theta}}^{(m)}$.
15:     **Step 3: Optimize UAV Location**
16:     **repeat**
17:         Given $\mathbf{f}_1^{(0)}, \mathbf{f}_2^{(0)}$, and $\mathbf{\Theta}^{(0)}$, find the optimal $L_r^{(n)}$ by solving P1.3.1.
18:         Update $n = n + 1$.
19:     **until** Convergence of P1.3.1 is reached.
20:     Set $L_r^{(0)} \leftarrow L_r^{(n)}$.
21:     Update $i = i + 1$.
22: **until** Convergence of P1 is reached.
23: **Output:** $\mathbf{f}_1^{(0)}$, $\mathbf{f}_2^{(0)}$, $\mathbf{\Theta}^{(0)}$, and $L_r^{(0)}$.
```

IV. Simulation

Simulation results are presented and discussed in this section to evaluate the effectiveness of the proposed scheme. Without further stated, simulation parameters are set as follows. The location coordinates of BS, Bob, and Eav are assumed at $L_a = (0, 0, 20)$, $L_b = (200, 0, 0)$, and $L_e = (200, 100, 0)$ in meters, respectively. The channel gain reference at 1 m is set to $\rho_0 = -30$ dB, and the large-scale path loss exponent is set to $\alpha = 3$. Rician factors are set to $K_{BS} = 2$, $K_{BI} = 4$, and $K_{IRS} = 4$. Then, the numbers of antennas on BS and the reflection elements on IRS are assumed to be $M = 8$ and $N = 25$, respectively. In addition, $\sigma^2 = -110$ dBm.

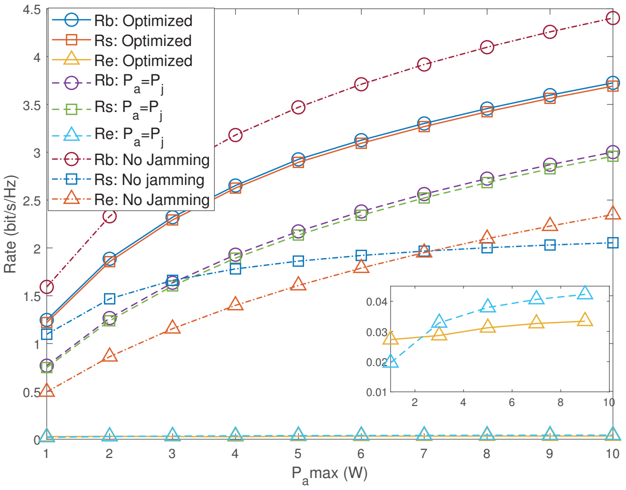


Fig. 2. Comparision of the R_b, R_e, R_s among the $\mathbf{f}_1$ $\mathbf{f}_2$ optimization, equal transmit-jamming power allocation, and no-jamming scheme.

In Fig. 2, the influence of the maximum transmit power P_{amax} on transmission rate, eavesdropping rate, and secrecy rate are presented. The experiment investigates R_b, R_e, and R_s under three cases, i.e., our proposed precoding and jamming vector and allocation optimization scheme, the transmit power equals to the jamming power, and no jamming scheme. From the results, we can see that R_b, R_e, and R_s all increase with the maximum allowed BS sum power P_{amax}. R_e slightly increase with P_{amax} in both our proposed scheme and equal transmit-jamming power scheme indicates the effectiveness of beamforming in suppressing R_e. Although R_b in the no-jamming scheme is higher than our proposed precoding and jamming vector optimization scheme, the R_s in our proposed scheme is much higher than the other two schemes. This is because all power budget at BS in the no-jamming scheme can be used to transmit signals, and there is no interference at the legitimate receiver. However, the high transmit power also results in a higher R_e without the protection of jamming. This, on the other hand, proves that our proposed scheme is optimized to balance the influence between transmit and jamming signals to achieve higher R_s.

Fig. 3 plots the transmission rate, eavesdropping rate, and secrecy rate under the influence of transmit antenna numbers at BS. The maximum allowed transmit power at BS is set to $P_{amax} = 10$ W. The reflection elements number is set to $N = 50$ during this experiment. It is observed that the eavesdropping rate R_e barely increases with transmit antenna

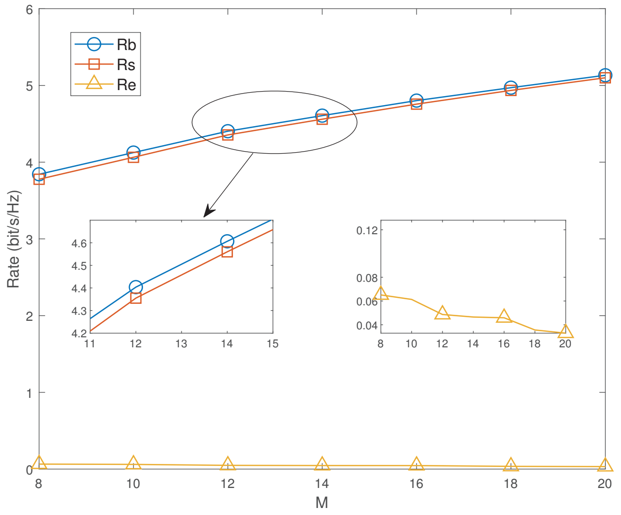


Fig. 3. Impact of antenna numbers on transmission, eavesdropping, and secrecy rates.

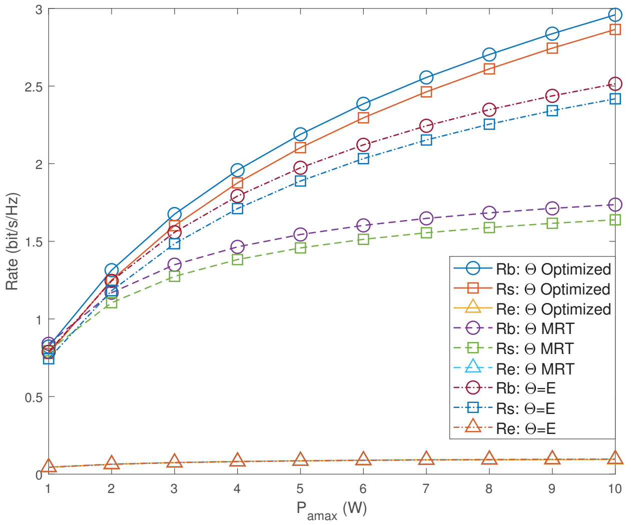


Fig. 4. Comparision of the achievable R_b, R_e, and R_s in our proposed $\boldsymbol{\Theta}$ optimization, MRT optimization, and reflection scheme.

number M, where the subtle changes indicate improved secure transmission as the number of antennas increase. However, the transmission rate R_b and secrecy rate R_s both increase with antenna numbers. This is consistent with our conclusion that properly designing precoding and jamming vectors can leverage the directional characteristic of antennas to achieve better transmission performance. Therefore, the network performance can be improved by increasing the antenna numbers at BS.

The achievable transmission rate R_b, eavesdropping rate R_e, and secrecy rate R_s are compared under our proposed phase shifting matrix optimization, the maximum ratio transmission (MRT) optimization, and the direct reflection scheme in Fig. 4. The transmit antenna number at BS is set to $M = 8$, and the reflection elements number of IRS is set to $N = 25$. We assume that UAV hovers at $L_r(200, 0, 50)$. It can be observed that all rates increase with the maximum allowed sum transmit power P_{amax}, which is consistent with common knowledge that higher transmit power leads to a higher achievable rate. In addition, we can also conclude from the results that our proposed phase shifting matrix can lead to a higher R_b and R_s than the other two benchmark schemes.

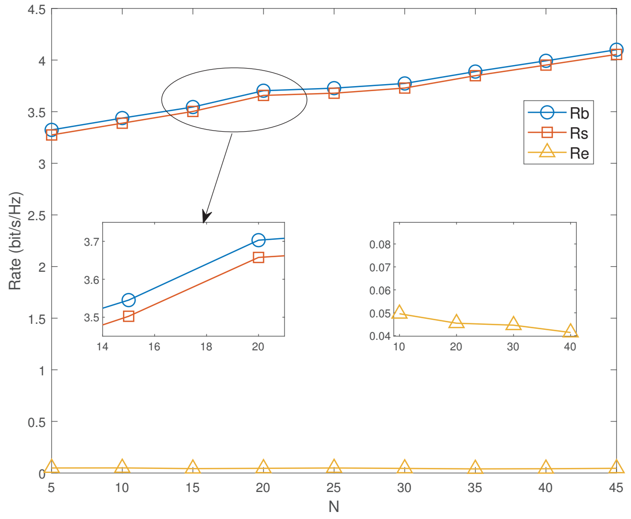


Fig. 5. Comparision of the achievable R_b, R_e, and R_s under different IRS reflection elements number N.

The impact of different IRS reflection elements number N on the achievable transmission rate R_b, eavesdropping rate R_e, and secrecy rate R_s are presented in Fig. 5. The transmit antenna number is set to $M = 8$, and the maximum power limit at BS is set to $P_{amax} = 10$ W. The phase shifting matrix is optimized according to Section III-B. The simulation results show that all of R_b, R_e, and R_s increase with N getting larger. R_e slightly changes with N increasing, which benefits from the successful eavesdropping suppression. R_b increases significantly and thus leads to a bigger R_s, which indicates that the increase of reflection elements N can improve the secrecy performance.

The impact of different IRS locations L_r and maximum total allowed transmit power P_{amax} on the secrecy rate R_s are investigated in Fig. 6. We have the IRS locating at the optimized location, $L_r = (160, 0, 100)$, $L_r = (50, 250, 50)$, and $L_r = (150, -50, 50)$ considered. The optimized IRS location is derived from Algorithm 1 listed in Table 1. The transmit antenna number is set to $M = 8$, and the reflection elements number is set to $N = 25$. From the results, we can see that the secrecy rate R_s with L_r derived by our proposed scheme is higher than other random locations. This proves the effectiveness of our proposed scheme in optimizing IRS location. In addition, the secrecy rate R_s also increases with the rising of P_{amax}.

In Fig. 7, the effectiveness of the proposed scheme is investigated. The achievable secrecy rate R_s is compared over the proposed scheme, no IRS optimization, and no location optimization. The transmit antenna number is set to $M = 8$ and the reflection elements number is set to $N = 25$. The

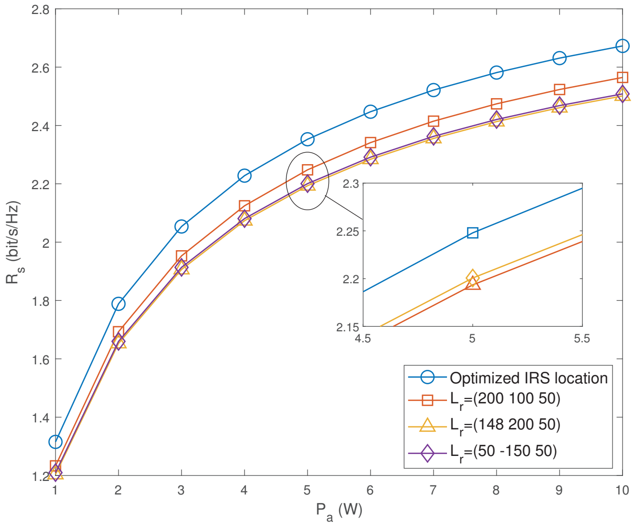


Fig. 6. Comparision of the achievable secrecy rate with different maximum allowed total transmit power P_{amax} when the IRS is at different locations.

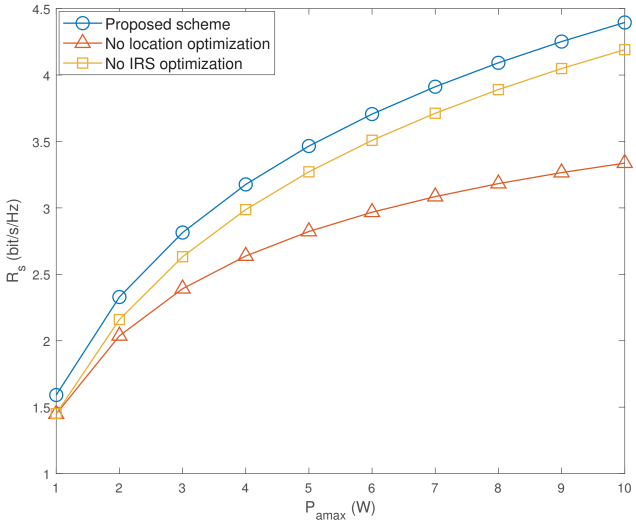


Fig. 7. Comparision of the achievable secrecy rate R_s among our proposed scheme, without IRS optimization, and without location optimization.

location of IRS is set to $L_r = (200, 100, 50)$ when there is no location optimization. We only consider the direct link when there is no optimization of $\mathbf{\Theta}$. From the results, we can see that the proposed scheme can achieve a higher R_s compared with when there is no $\mathbf{\Theta}$ optimization and no L_r optimization. This proves the effectiveness of our proposed scheme by optimizing the precoding and jamming vector $\mathbf{f}_1$ and $\mathbf{f}_2$, phase shifting matrix $\mathbf{\Theta}$, and IRS location L_r. In addition, we can see that the secrecy rate increases as the maximum allowed transmit power P_{amax} increases.

V. Conclusion

A secure IRS-on-UAV-assisted wireless network is investigated to maximize the secrecy rate against an eavesdropper in this paper. The beamforming vectors, transmit-jamming power split, reflection elements gain of IRS, and the mobility of UAV are simultaneously optimized to provide secure transmission. In the proposed scheme, we optimize the transmit-jamming power split ratio and beamforming vectors, the location of the UAV, and the phase shifting matrix of IRS to maximize the secrecy rate while avoiding eavesdropping, where the optimization problem is non-convex and mathematically intractable. We alternately optimize the beamforming vectors, UAV location, and IRS phase shifting matrix to solve the problem. Simulation results are demonstrated and discussed to evaluate the effectiveness of our proposed scheme. In our future work, we will focus on the secure and robust design of an IRS-on-UAV network serving more legitimate users and against multiple eavesdroppers.

Appendix A
Details of $\tilde{R}_e(x, y)$

Based on (60), the first-order derivative of R_e with respect to x can be illustrated as (59) on the top of this page, where $Y_k = \mathrm{e}^{\frac{\alpha}{4}\mathrm{y_k}}$ and $X_k = \mathrm{e}^{\frac{\alpha}{4}\mathrm{x_k}}$. Γ_e^k is defined as

$$\Gamma_e^k = \frac{\left|X_k Y_k \tilde{\mathbf{h}}_{ae}^{r} \mathbf{f}_1 + \mathbf{h}_{ae}\mathbf{f}_1\right|^2}{\left|X_k Y_k \tilde{\mathbf{h}}_{ae}^{r} \mathbf{f}_2 + \mathbf{h}_{ae}\mathbf{f}_2\right|^2 + \sigma^2} + 1. \tag{60}$$

In addition, we define R_1^x, I_1^x, R_2^e, I_2^e, R_3^x, I_3^x, R_4^e, and I_4^e in (59) as

$$Y_k \tilde{\mathbf{h}}_{ae}^{r} \mathbf{f}_1 = R_1^x + iI_1^x, \tag{61}$$

$$\mathbf{h}_{ae}\mathbf{f}_1 = R_2^e + iI_2^e, \tag{62}$$

$$Y_k \tilde{\mathbf{h}}_{ae}^{r} \mathbf{f}_2 = R_3^x + iI_3^x, \tag{63}$$

$$\mathbf{h}_{ae}\mathbf{f}_2 = R_4^e + iI_4^e, \tag{64}$$

On the other hand, $R_e^{y'}(x_k, y_k)$ can be expressed as (65) on the top of this page.

We further define R_1^y, I_1^y, R_3^y, and I_3^y in (65) as

$$X_k \tilde{\mathbf{h}}_{ae}^{r} \mathbf{f}_1 = R_1^y + iI_1^y, \tag{66}$$

$$X_k \tilde{\mathbf{h}}_{ae}^{r} \mathbf{f}_2 = R_3^y + iI_3^y. \tag{67}$$

Till now, the details of $R_e^{x'}(x_k, y_k)$ and $R_e^{y'}(x_k, y_k)$ of $\tilde{R}_e(x, y)$ in (60) are both demonstrated.

References

[1] X. Chen, Z. Chang, N. Zhao, and T. Hämäläinen, "IRS-based secure UAV-assisted transmission with location and phase shifting optimization," in *Proc. IEEE ICC Workshops'23*, pp. 1672–1677, Rome, Italy, May 2023.

[2] B. Zheng, C. You, W. Mei, and R. Zhang, "A survey on channel estimation and practical passive beamforming design for intelligent reflecting surface aided wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1035–1071, 2nd Quart. 2022.

[3] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Commun. Mag.*, vol. 58, no. 1, pp. 106–112, Jan. 2020.

[4] X. Pang, M. Sheng, N. Zhao, J. Tang, D. Niyato, and K.-K. Wong, "When UAV meets IRS: Expanding air-ground networks via passive reflection," *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 164–170, Oct. 2021.

[5] H. Hashida, Y. Kawamoto, and N. Kato, "Intelligent reflecting surface placement optimization in air-ground communication networks toward 6G," *IEEE Wireless Commun.*, vol. 27, no. 6, pp. 146–151, Dec. 2020.

$$
\begin{aligned}
R_e^{x'}(x_k,y_k) = & \frac{\alpha \mathrm{e}^{-\frac{\alpha}{2}\mathrm{x_k}}}{\ln 2\Gamma_e^k} \left\{ \frac{\left[\left({R_1^x}^2+{I_1^x}^2\right)\left(R_3^x R_4^e+I_3^x I_4^e\right)-\left({R_3^x}^2+{I_3^x}^2\right)\left(R_1^x R_2^e+I_1^x I_2^e\right)\right]{Y_k}^2}{\left({R_3^x}^2+{I_3^x}^2\right){Y_k}^2+\left(R_3^x R_4^e+I_3^x I_4^e\right)Y_k+{R_4^e}^2+{I_4^e}^2+\sigma^2} \right. \\
& + \frac{\left[\left({R_1^x}^2+{I_1^x}^2\right)\left({R_4^e}^2+{I_4^e}^2+\sigma^2\right)-\left({R_3^x}^2+{I_3^x}^2\right)\left({R_2^e}^2+{I_2^e}^2\right)\right]Y_k}{\left({R_3^x}^2+{I_3^x}^2\right){Y_k}^2+\left(R_3^x R_4^e+I_3^x I_4^e\right)Y_k+{R_4^e}^2+{I_4^e}^2+\sigma^2} \\
& \left. + \frac{\left({R_1^x}^2+{I_1^x}^2\right)\left({R_4^e}^2+{I_4^e}^2+\sigma^2\right)-\left(R_3^x R_4^e+I_3^x I_4^e\right)\left({R_2^e}^2+{I_2^e}^2\right)}{\left({R_3^x}^2+{I_3^x}^2\right){Y_k}^2+\left(R_3^x R_4^e+I_3^x I_4^e\right)Y_k+{R_4^e}^2+{I_4^e}^2+\sigma^2} \right\},
\end{aligned}
\tag{59}
$$

$$
\begin{aligned}
R_e^{y'}(x_k,y_k) = & \frac{\alpha \mathrm{e}^{-\frac{\alpha}{2}\mathrm{y_k}}}{\ln 2\Gamma_e^k} \left\{ \frac{\left[\left({R_1^y}^2+{I_1^y}^2\right)\left(R_3^y R_4^e+I_3^y I_4^e\right)-\left({R_3^y}^2+{I_3^y}^2\right)\left(R_1^y R_2^e+I_1^y I_2^e\right)\right]{X_k}^2}{\left({R_3^y}^2+{I_3^y}^2\right){X_k}^2+\left(R_3^y R_4^e+I_3^y I_4^e\right)X_k+{R_4^e}^2+{I_4^e}^2+\sigma^2} \right. \\
& + \frac{\left[\left({R_1^y}^2+{I_1^y}^2\right)\left({R_4^e}^2+{I_4^e}^2+\sigma^2\right)-\left({R_3^y}^2+{I_3^y}^2\right)\left({R_2^e}^2+{I_2^e}^2\right)\right]X_k}{\left({R_3^y}^2+{I_3^y}^2\right){X_k}^2+\left(R_3^y R_4^e+I_3^x I_4^e\right)X_k+{R_4^e}^2+{I_4^e}^2+\sigma^2} \\
& \left. + \frac{\left({R_1^y}^2+{I_1^y}^2\right)\left({R_4^e}^2+{I_4^e}^2+\sigma^2\right)-\left(R_3^y R_4^e+I_3^y I_4^e\right)\left({R_2^e}^2+{I_2^e}^2\right)}{\left({R_3^y}^2+{I_3^y}^2\right){X_k}^2+\left(R_3^y R_4^e+I_3^y I_4^e\right)X_k+{R_4^e}^2+{I_4^e}^2+\sigma^2} \right\}.
\end{aligned}
\tag{65}
$$

[6] A. S. d. Sena, D. Carrillo, F. Fang, P. H. J. Nardelli, D. B. d. Costa, U. S. Dias, Z. Ding, C. B. Papadias, and W. Saad, “What role do intelligent reflecting surfaces play in multi-antenna non-orthogonal multiple access?,” *IEEE Wireless Commun.*, vol. 27, no. 5, pp. 24–31, Oct. 2020.

[7] C. You, Z. Kang, Y. Zeng, and R. Zhang, “Enabling smart reflection in integrated air-ground wireless network: IRS meets UAV,” *IEEE Wireless Commun.*, vol. 28, no. 6, pp. 138–144, Dec. 2021.

[8] C. You and R. Zhang, “Wireless communication aided by intelligent reflecting surface: Active or passive?,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2659–2663, Dec. 2021.

[9] X. Pang, W. Mei, N. Zhao, and R. Zhang, “Intelligent reflecting surface assisted interference mitigation for cellular-connected UAV,” *IEEE Wireless Commun. Lett.*, vol. 11, no. 8, pp. 1708–1712, Aug. 2022.

[10] W. Wang, X. Liu, J. Tang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, “Beamforming and jamming optimization for IRS-aided secure NOMA networks,” *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1557–1569, Mar. 2022.

[11] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, “Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey,” *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2283–2314, 4th Quart. 2020.

[12] L. Gupta, R. Jain, and G. Vaszkun, “Survey of important issues in UAV communication networks,” *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, 2nd Quart. 2016.

[13] X. Song, Y. Zhao, Z. Wu, Z. Yang, and J. Tang, “Joint trajectory and communication design for IRS-assisted UAV networks,” *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1538–1542, Jul. 2022.

[14] T. Shafique, H. Tabassum, and E. Hossain, “Optimization of wireless relaying with flexible UAV-borne reflecting surfaces,” *IEEE Trans. Commun.*, vol. 69, no. 1, pp. 309–325, Jan. 2021.

[15] D. Liu, Y. Xu, J. Wang, J. Chen, K. Yao, Q. Wu, and A. Anpalagan, “Opportunistic UAV utilization in wireless networks: Motivations, applications, and challenges,” *IEEE Commun. Mag.*, vol. 58, no. 5, pp. 62–68, May 2020.

[16] X. Jiang, X. Chen, J. Tang, N. Zhao, X. Y. Zhang, D. Niyato, and K.-K. Wong, “Covert communication in UAV-assisted air-ground networks,” *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 190–197, Aug. 2021.

[17] X. Chen, M. Sheng, N. Zhao, W. Xu, and D. Niyato, “UAV-relayed covert communication towards a flying warden,” *IEEE Trans. Commun.*, vol. 69, no. 11, pp. 7659–7672, Nov. 2021.

[18] B. Zhu, E. Bedeer, H. H. Nguyen, R. Barton, and J. Henry, “UAV trajectory planning in wireless sensor networks for energy consumption minimization by deep reinforcement learning,” *IEEE Trans. Vehi. Tech.*, vol. 70, no. 9, pp. 9540–9554, Sept. 2021.

[19] X. Chen, N. Zhao, Z. Chang, T. Hämäläinen, and X. Wang, “UAV-aided secure short-packet data collection and transmission,” *IEEE Trans. Commun.*, vol. 71, no. 4, pp. 2475–2486, 2023.

[20] W. U. Khan, E. Lagunas, Z. Ali, M. A. Javed, M. Ahmed, S. Chatzinotas, B. Ottersten, and P. Popovski, “Opportunities for physical layer security in UAV communication enhanced with intelligent reflective surfaces,” *IEEE Wireless Commun.*, vol. 29, no. 6, pp. 22–28, Dec. 2022.

[21] X. Zhang, J. Wang, and H. V. Poor, “Joint optimization of IRS and UAV-trajectory: For supporting statistical delay and error-rate bounded QoS over mURLLC-driven 6G mobile wireless networks using FBC,” *IEEE Veh. Tech. Mag.*, vol. 17, no. 2, pp. 55–63, Jun. 2022.

[22] Y. Ge, J. Fan, G. Y. Li, and L.-C. Wang, “Intelligent reflecting surface-enhanced UAV communications: Advances, challenges, and prospects,” *IEEE Wireless Commun.*, pp. 1–8, to appear.

[23] S. Jiao, F. Fang, X. Zhou, and H. Zhang, “Joint beamforming and phase shift design in downlink UAV networks with IRS-assisted NOMA,” *J. Commun. Inf. Networks*, vol. 5, no. 2, pp. 138–149, Jun. 2020.

[24] Z. Mohamed and S. Aissa, “Leveraging UAVs with intelligent reflecting surfaces for energy-efficient communications with cell-edge users,” in *Proc. IEEE ICC Workshops*, pp. 1–6, Dublin, Ireland, 2020.

[25] W. Wang, H. Tian, and W. Ni, “Secrecy performance analysis of IRS-aided UAV relay system,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2693–2697, Dec. 2021.

[26] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K.-K. Wong, “IRS-assisted secure UAV transmission via joint trajectory and beamforming design,” *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1140–1152, Feb. 2022.

[27] W. Wei, X. Pang, J. Tang, N. Zhao, X. Wang, and A. Nallanathan, “Secure transmission design for aerial IRS assisted wireless networks,” *IEEE Trans. Commun.*, vol. 71, no. 6, pp. 3528–3540, 2023.

[28] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, “Transmit solutions for MIMO wiretap channels using alternating optimization,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sept. 2013.

[29] Z.-q. Luo, W.-k. Ma, A. M.-c. So, Y. Ye, and S. Zhang, “Semidefinite relaxation of quadratic optimization problems,” *IEEE Signal Proc. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.

III

IRS-BASED SECURE UAV-ASSISTED TRANSMISSION WITH LOCATION AND PHASE SHIFTING OPTIMIZATION

by

Xinying Chen, Zheng Chang, Nan Zhao, and Timo Hämäläinen 2023

2023 IEEE International Conference on Communications Workshops
(ICC Workshops), pp. 1672–1677,
https://www.doi.org/10.1109/ICCWorkshops57953.2023.10283558

IRS-Based Secure UAV-Assisted Transmission with Location and Phase Shifting Optimization

Xinying Chen[∐†], Zheng Chang[∐], Nan Zhao[†], and Timo Hämäläinen[∐]
[∐]Faculty of Information Technology, University of Jyväskylä, P. O. Box 35, FIN-40014 Jyväskylä, Finland.
[†]School of Information and Communication Engineering, Dalian University of Technology, Dalian, 116024, P. R. China.

***Abstract*—An intelligent reflection surface (IRS) can actively design the propagation channel via designing the phase shifting matrix to provide more secure transmission. Being mounted on the unmanned aerial vehicle (UAV), IRS is able to further leverage the mobility and flexible advantages of UAV. In this paper, we investigate the secure transmission of an IRS-assisted UAV network against an eavesdropper, where the IRS is mounted on the UAV. The secrecy rate is maximized by jointly optimizing the phase shifting matrix and the hovering location of IRS. Owing to the non-convexity of the optimized problem, we decompose it to two subproblems and alternatively solve them to derive the optimal UAV location and phase shifting matrix. First, we adopt the first-order Taylor expansion to change the non-convex UAV location optimization subproblem into a mathematical solvable convex version, and solve it through successive convex approximation (SCA) with a given phase shifting matrix. Then, with a given UAV hovering location, the phase shifting matrix is optimized via semidefinite relaxation (SDR) and SCA. Finally, simulation results are provided to evaluate the effectiveness of our proposed secure IRS-assisted wireless transmission scheme.**

***Index Terms*—IRS, Location optimization, Secure transmission, UAV.**

I. Introduction

The intelligent reflecting surface (IRS) has attracted tremendous intention owing to its deployment flexibility, easy configuration, and link capacity improvement [1]. Consisting of many two-dimensional artificial electromagnetic surfaces, IRS can change the electromagnetic properties of signal through its scattering elements. Technically, IRS can realize the re-design of channel fading via programming the phase shifting of passive reconfigurable reflection elements without extra high power consumption. The total received signals can be enhanced or reduced with the directly transmitted signals at specific receivers by properly designing phase shifts of the IRS units. In [2], You *et al.* investigated the effectiveness of both active and passive IRS in wireless communications. They conclude that the passive IRS can achieve better performance with a sufficiently large amount of elements. In addition, the utilization of IRS can also improve the security of transmission owing to its reconfigurable channel property. Wang *et al.* utilized beamforming and jamming to realize the secure transmission in an IRS-assisted non-orthogonal multiple access (NOMA) networks in [3]. They alternatively solved the non-convex optimization to derive the optimal beamforming, jamming, and phase shifting vectors to maximize the sum rate of legitimate users while constraining the eavesdropping rate under a specific limit. Although IRS can leverage channel design to realize the enhancement of desired signals and suppressant of undesired signals, the deployment of IRS still faces some critical challenges [4]. First, IRS can occupy a large surface and may result in the difficulty of deployment authentification practically, which is because IRS will block a considerable area if attached to the building surface. Then, the fixed attached-to-building IRS has some non-avoidable blind zone, which will result in the inefficiency of transmission.

Meanwhile, the unmanned aerial vehicle (UAV)-aid network emerges with the features of high mobility and flexible deployment [5]. Thus, considerable works have been done to the UAV-aided networks, which utilize the advantages of mobility and good quality of line-of-sight (LoS) channels has been conducted. In [6], Chen *et al.* applied UAVs as both the relay and the warden to investigate long-range covert communications. The authors considered the mobility trade-off of both the warden and the relay to maximize the transmission rate of Alice while keeping the covertness. In addition, Zhu *et al.* proposed a UAV trajectory design and cluster heads (CHs) assignment scheme to minimize the energy consumption for a wireless sensor network (WSN) in [7], where a novel deep reinforcement learning (DRL) was applied to solve the problem optimization.

Being mounted IRS on UAV can solve the deployment of IRS and take further utilization of the LoS potentials [8]. On one hand, molding IRS on a UAV can omit the troubles caused by the occupation authority issues. IRS can be deployed easily and be engaged with mobility during work. On the other hand, the phase reflection design can make up for the lack of security in UAV LoS channels. Few works related to secure IRS-mounted-on-UAV communications have been conducted. In [9], Jiao *et al.* jointly optimized the location and phase shift of a UAV to maximize the transmission rate for strong link users while maintaining the minimum required transmission rate of other users in a NOMA network. The authors improved the energy efficiency of the system by jointly designing the phase shifting of the IRS relay and the beamforming vector at the base station in [10]. However, security is still critical in IRS-UAV networks. In this paper, we investigate the secure transmission in an IRS-mounted-on-UAV network. The location and phase shifting are jointly designed to maximize the secrecy rate. To achieve this purpose, we propose an alternative optimization algorithm to solve the non-convex optimization problem with low computational complexity.

Unlike most previous works, this paper investigates the secure transmission in an IRS-mounted-on-UAV network. We jointly optimize the location and phase shifting of IRS to

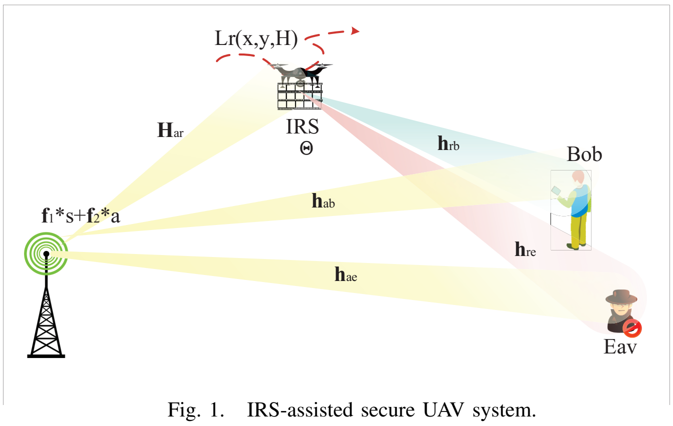


Fig. 1. IRS-assisted secure UAV system.

maximize the achievable secrecy rate while avoiding being eavesdropped. First, the location of the UAV is optimized with a given phase shifting of IRS to maximize the secrecy rate under the constraints. Then, with the optimized location, the phase shifting matrix will be optimized to achieve a bigger secrecy rate. Finally, by alternatively optimizing the location and phase shift of IRS, the maximum achievable secrecy rate can be obtained.

II. System Model

Consider a secure wireless communication system, where a base station (BS) a transmits confidential information to a terrestrial Bob b with the assistance of an IRS r mounted on a UAV while avoiding eavesdropping from a terrestrial Eav e. Assume that BS is equipped with M antennas and the IRS has N reflecting elements, while both Bob and Eav have a single antenna. The locations of the BS, IRS, Bob, and Eav are assumed at $L_a = (x_a, y_a, H)$, $L_r = (x_r, y_r, z_r)$, $L_b = (x_b, y_b, 0)$, $L_e = (x_e, y_e, 0)$, where the height of BS is set to H. Suppose that the channel fading coefficients from the BS to Bob, and Eav are denoted as $\mathbf{h}_{ab} \in \mathbb{C}^{1\times M}$, and $\mathbf{h}_{ae} \in \mathbb{C}^{1\times M}$. Both of $\mathbf{h}_{ab}$ and $\mathbf{h}_{ae}$ follow large-scale path loss and a small-scale Rayleigh fading, which can be described as follows

$$\mathbf{h}_{ab} = \sqrt{\frac{\rho_0}{D_{ab}^{-\alpha}}}\mathbf{g}_{ab}, \tag{1}$$

$$\mathbf{h}_{ae} = \sqrt{\frac{\rho_0}{D_{ae}^{-\alpha}}}\mathbf{g}_{ae}, \tag{2}$$

where D_{ab} and D_{ae} are the distances from BS to Bob and Eav. ρ_0 is the path loss reference at 1 m and α represents the large-scale path loss exponent. $g_{ab_i} \in \mathbf{g}_{ab}$ and $g_{ae_i} \in \mathbf{g}_{ae}$ denote the Rayleigh fading components with zero mean and unit variance. In addition, the air-to-ground channel coefficients from IRS to BS, Bob and Eav are denoted by $\mathbf{H}_{ar} \in \mathbb{C}^{N\times M}$, $\mathbf{h}_{rb} \in \mathbb{C}^{1\times N}$ and $\mathbf{h}_{re} \in \mathbb{C}^{1\times N}$, which follow a large-scale path loss with a small-scale Rician fading, and can be described as

$$\mathbf{H}_{ar}=\sqrt{\frac{\rho_0}{D_{ar}^{-\alpha}}}\mathbf{G}_{ar}=\sqrt{\frac{\rho_0}{D_{ar}^{-\alpha}}}\left(\sqrt{\frac{K}{1+K}}\mathbf{G}_{ar}^{L}+\sqrt{\frac{1}{1+K}}\mathbf{G}_{ar}^{N}\right), \tag{3}$$

$$\mathbf{g}_{rb}=\sqrt{\frac{\rho_0}{D_{rb}^{-\alpha}}}\mathbf{g}_{rb}=\sqrt{\frac{\rho_0}{D_{rb}^{-\alpha}}}\left(\sqrt{\frac{K}{1+K}}\mathbf{g}_{rb}^{L}+\sqrt{\frac{1}{1+K}}\mathbf{g}_{rb}^{N}\right), \tag{4}$$

$$\mathbf{g}_{re}=\sqrt{\frac{\rho_0}{D_{re}^{-\alpha}}}\mathbf{g}_{re}=\sqrt{\frac{\rho_0}{D_{re}^{-\alpha}}}\left(\sqrt{\frac{K}{1+K}}\mathbf{g}_{re}^{L}+\sqrt{\frac{1}{1+K}}\mathbf{g}_{re}^{N}\right), \tag{5}$$

where D_{ar}, D_{rb} and D_{re} are the distance from IRS to BS, Bob and Eav. K denotes the Rician factor. $\mathbf{G}_{ar}^{L}$, $\mathbf{g}_{rb}^{L}$, $\mathbf{g}_{re}^{L}$ are the LoS components of Rician fading and follow $|G_{ar_{ij}}^{L}| = 1$, $|g_{rb_i}^{L}| = 1$, and $|g_{re_i}^{L}| = 1$. $\mathbf{G}_{ar}^{N}$, $\mathbf{g}_{rb}^{N}$, $\mathbf{g}_{re}^{N}$ are the NLoS components of Rician fading, where $G_{ar_{ij}}^{N} \in \mathbf{G}_{ar}^{N}$, $g_{rb_i}^{N} \in \mathbf{g}_{rb}^{N}$, and $g_{re_i}^{N} \in \mathbf{g}_{re}^{N}$ follow complex Gaussian distribution with zero mean and unit variance.

Apply $\mathbf{\Theta} = \mathrm{diag}(\mathrm{e}^{\mathrm{j}\theta_1}, \cdots, \mathrm{e}^{\mathrm{j}\theta_N})$ to denote the diagonal phase-sifting matrix of IRS, where $\theta_i \in [0, 2\pi), \forall i \in \{1, \cdots, N\}$, is the phase-shifting of the i-th element on the IRS. As for the IRS undergoing the passive reflection, we assume that IRS is applying the time-division-duplexing (TDD) protocol. In addition, we also assume that the channel state information (CSI) within this network is obtainable. The BS applies precoding vector $\mathbf{f}_1 \in \mathbb{C}^{M\times 1}$ and $\mathbf{f}_2 \in \mathbb{C}^{M\times 1}$ for independent confidential signals $s \sim \mathcal{CN}(0,1)$ and jamming signals $j \sim \mathcal{CN}(0,1)$, where $\mathbf{f}_1^H\mathbf{f}_1 + \mathbf{f}_2^H\mathbf{f}_2 \leq P_{amax}$, respectively. P_{amax} is the maximum allowed total transmit power at BS. Thus, the received signal at Bob and Eav can be described as

$$y_b = (\mathbf{h}_{ab} + \mathbf{h}_{rb}\mathbf{\Theta}\mathbf{H}_{ar})(\mathbf{f}_1 s + \mathbf{f}_2 j) + n_b, \tag{6}$$

and

$$y_e = (\mathbf{h}_{ae} + \mathbf{h}_{re}\mathbf{\Theta}\mathbf{H}_{ar})(\mathbf{f}_1 s + \mathbf{f}_2 j) + n_e, \tag{7}$$

where n_b and n_e denote the noise received at Bob and the eavesdropper, respectively. Without loss of generality, we assume both n_b and n_e follow Gaussian distribution with zero mean and variance of σ^2. Therefore, the maximum achievable transmission rate at Bob and eavesdropping rate at Eav can be described as

$$R_b = \log_2\left(1 + \frac{|(\mathbf{h}_{ab} + \mathbf{h}_{rb}\mathbf{\Theta}\mathbf{H}_{ar})\mathbf{f}_1|^2}{|(\mathbf{h}_{ab} + \mathbf{h}_{rb}\mathbf{\Theta}\mathbf{H}_{ar})\mathbf{f}_2|^2 + \sigma^2}\right), \tag{8}$$

and

$$R_e = \log_2\left(1 + \frac{|(\mathbf{h}_{ae} + \mathbf{h}_{re}\mathbf{\Theta}\mathbf{H}_{ar})\mathbf{f}_1|^2}{|(\mathbf{h}_{ae} + \mathbf{h}_{re}\mathbf{\Theta}\mathbf{H}_{ar})\mathbf{f}_2|^2 + \sigma^2}\right). \tag{9}$$

Then, the secrecy rate at Bob can be defined as

$$R_s = [R_b - R_e]^+, \tag{10}$$

where $[*]^+$ represents $\max\{*, 0\}$.

III. Problem Formulation

We aim to achieve a higher secrecy rate via jointly designing the location L_r and phase shifting matrix $\mathbf{\Theta}$ of IRS while constrained by the phase angles at IRS. Thus, the optimization problem can be formulated as

$$\textbf{P1:} \max_{\boldsymbol{\Theta}, L_r} R_s \tag{11a}$$

$$s.t. \quad R_b \geq R_{min}, \tag{11b}$$

$$\theta_i \in [0, 2\pi), \tag{11c}$$

$$R_e \geq r_e, \tag{11d}$$

P1 has a non-convex structure and is difficult to be addressed. Thus, we propose an iterative algorithm to solve the proposed problem by alternatively optimizing $\boldsymbol{\Theta}$ and L_r with the other variable given.

Considering L_r and $\boldsymbol{\Theta}$ are not coupled with each other, we can solve the optimization problem via alternately optimizing L_r and $\boldsymbol{\Theta}$. First, we optimize L_r with a given $\boldsymbol{\Theta}$. Then, the optimized $\boldsymbol{\Theta}$ can be derived from P1 under a given L_r.

A. Optimization of L_r With A Given $\boldsymbol{\Theta}$

With a given $\boldsymbol{\Theta}$, the optimization problem P1 can can be changed into

$$\textbf{P2:} \max_{L_r} \log_2\left(\frac{\left|\left(D_{ar}^{-\frac{\alpha}{2}} D_{rb}^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{ab}^r + \mathbf{h}_{ab}\right)\mathbf{f}_1\right|^2}{\left|\left(D_{ar}^{-\frac{\alpha}{2}} D_{rb}^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{ab}^r + \mathbf{h}_{ab}\right)\mathbf{f}_2\right|^2 + \sigma^2} + 1\right) - \log_2\left(\frac{\left|\left(D_{ar}^{-\frac{\alpha}{2}} D_{re}^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{ae}^r + \mathbf{h}_{ae}\right)\mathbf{f}_1\right|^2}{\left|\left(D_{ar}^{-\frac{\alpha}{2}} D_{re}^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{ae}^r + \mathbf{h}_{ae}\right)\mathbf{f}_2\right|^2 + \sigma^2} + 1\right) \tag{12a}$$

$$s.t. \quad R_b \geq R_{min}, \tag{12b}$$

$$R_e \geq r_e, \tag{12c}$$

$$D_{ar} \leq m, \tag{12d}$$

$$D_{rb} \leq n, \tag{12e}$$

$$D_{ar} \geq \mathrm{e}^{-\mathrm{x}}, \tag{12f}$$

$$D_{re} \geq \mathrm{e}^{-\mathrm{y}}, \tag{12g}$$

where D_{ar}, D_{rb}, and D_{re} are defined as

$$D_{ar} = ||L_r - L_a||^2, \tag{13}$$

$$D_{rb} = ||L_r - L_b||^2, \tag{14}$$

$$D_{re} = ||L_r - L_e||^2, \tag{15}$$

In addition, in (12) R_{min} denotes the minimum required transmission rate. m, n, x, and y are four introduced auxiliary variables, where the convexity of (12d), (12e), (12f), (12g) can be guaranteed.

Furthermore, $\tilde{\mathbf{g}}_{ab}^r$ and $\tilde{\mathbf{g}}_{ae}^r$ are introduced to simplify the expression of the optimization problem, which can be expressed as

$$\tilde{\mathbf{g}}_{ab}^r = \sqrt{\rho_0}\mathbf{g}_{rb}\boldsymbol{\Theta}\mathbf{G}_{ar}, \tag{16}$$

and

$$\tilde{\mathbf{g}}_{ae}^r = \sqrt{\rho_0}\mathbf{g}_{re}\boldsymbol{\Theta}\mathbf{G}_{ar}. \tag{17}$$

However, (12b) and (12a) are still non-convex and mathematically unsolvable, both of which need to be altered into concave with respect to m, n, x, and y. We apply the first-order Taylor expansion to (12b) to change it into concave with respect to m and n. The first-order Taylor expansion of (12b) at a given (m_k, n_k) can be expressed as

$$R_b^l(m,n) = R_b(m_k, n_k) + R_b^{m'}(m_k, n_k)(m - m_k) + R_b^{n'}(m_k, n_k)(n - n_k). \tag{18}$$

$R_b^{m'}(m_k, n_k)$ and $R_b^{n'}(m_k, n_k)$ represent the first-order derivative of $R_b(m, n)$ with respect of m and n, respectively. Thus, according to Taylor's theorem we can conclude

$$R_b(m, n) \geq R_b^l(m, n). \tag{19}$$

$R_b^{m'}(m_k, n_k)$ can be described as (20) at the top of next page.

In (20) $B_k = {n_k}^{-\frac{\alpha}{2}}$ and Γ_m is defined as

$$\Gamma_m = \frac{\left|\left({m_k}^{-\frac{\alpha}{2}} {n_k}^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{ab}^r + \mathbf{h}_{ab}\right)\mathbf{f}_1\right|^2}{\left|\left({m_k}^{-\frac{\alpha}{2}} {n_k}^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{ab}^r + \mathbf{h}_{ab}\right)\mathbf{f}_2\right|^2 + \sigma^2} + 1, \tag{21}$$

In addition, R_1^m, I_1^m, R_2, I_2, R_3^m, I_3^m, R_4, and I_4 in (20) can be defined as

$$B_k \tilde{\mathbf{g}}_{ab}^r \mathbf{f}_1 = R_1^m + iI_1^m, \tag{22}$$

$$\mathbf{h}_{ab}\mathbf{f}_1 = R_2 + iI_2, \tag{23}$$

$$B_k \tilde{\mathbf{g}}_{ab}^r \mathbf{f}_2 = R_3^m + iI_3^m, \tag{24}$$

$$\mathbf{h}_{ab}\mathbf{f}_2 = R_4 + iI_4, \tag{25}$$

In addition, $R_b^{n'}(m_k, n_k)$ can be demonstrated in (26) at the top of next page.

where $A_k = {m_k}^{-\frac{\alpha}{2}}$. We further define R_1^n, I_1^n, R_3^n, and I_3^n in (26) as

$$A_k \tilde{\mathbf{g}}_{ab}^r \mathbf{f}_1 = R_1^n + iI_1^n, \tag{27}$$

$$A_k \tilde{\mathbf{g}}_{ab}^r \mathbf{f}_2 = R_3^n + iI_3^n, \tag{28}$$

Then, the first part in (12a) turns to concave and mathematically solvable. (12a) becomes solvable, if R_e altered to a convex version, .

By utilizing the first-order Taylor expansion, D_{ar} and D_{re} can be changed into

$$D_{ar} \geq ||L_r^{(k)} - L_a||^2 + 2(L_r^{(k)} - L_a)(L_r - L_r^{(k)})^T \geq \mathrm{e}^{-\mathrm{x}} \tag{29}$$

$$D_{re} \geq ||L_r^{(k)} - L_e||^2 + 2(L_r^{(k)} - L_e)(L_r - L_r^{(k)})^T \geq \mathrm{e}^{-\mathrm{y}} \tag{30}$$

Then we define $R_e(x, y)$ as

$$R_e(x,y) = \log_2\left(\frac{\left|\left((\mathrm{e}^{-\mathrm{x}})^{-\frac{\alpha}{2}} (\mathrm{e}^{-\mathrm{y}})^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{ae}^r + \mathbf{h}_{ae}\right)\mathbf{f}_1\right|^2}{\left|\left((\mathrm{e}^{-\mathrm{x}})^{-\frac{\alpha}{2}} (\mathrm{e}^{-\mathrm{y}})^{-\frac{\alpha}{2}} \tilde{\mathbf{g}}_{ae}^r + \mathbf{h}_{ae}\right)\mathbf{f}_2\right|^2 + \sigma^2} + 1\right). \tag{31}$$

We can have $R_e \leq R_e(x, y)$. The first-order Taylor expansion of $R_e(x, y)$ can be demonstrated as

$$\tilde{R}_e(x, y) = R_e(x_k, y_k) + R_e^{x'}(x_k, y_k)(x - x_k) + R_e^{y'}(x_k, y_k)(y - y_k), \tag{32}$$

where $R_e^{x'}(x_k, y_k)$ represents the first-order derivative of R_e with respect to x at (x_k, y_k) and $R_e^{y'}(x_k, y_k)$ is the first-order derivative with respect to y at (x_k, y_k). Similar to (20) and (26), the detailed derivation can be refered from Appendix A.

Thus, the optimization problem P2 can be changed to a

$$R_b^{m'}(m_k,n_k) = \frac{-\frac{\alpha}{2}m^{-\frac{\alpha}{2}-1}}{\ln 2\Gamma_a}\left\{\frac{\left[\left(R_1^{m2}+I_1^{m2}\right)\left(R_3^mR_4+I_3^mI_4\right)-\left(R_3^{m2}+I_3^{m2}\right)\left(R_1^mR_2+I_1^mI_2\right)\right]{B_k}^2}{\left(R_3^{m2}+I_3^{m2}\right){B_k}^2+\left(R_3^mR_4+I_3^mI_4\right)B_k+{R_4}^2+{I_4}^2+\sigma^2}\right.$$
$$+\frac{\left[\left(R_1^{m2}+I_1^{m2}\right)\left({R_4}^2+{I_4}^2+\sigma^2\right)-\left(R_3^{m2}+I_3^{m2}\right)\left({R_2}^2+{I_2}^2\right)\right]B_k}{\left(R_3^{m2}+I_3^{m2}\right){B_k}^2+\left(R_3^mR_4+I_3^mI_4\right)B_k+{R_4}^2+{I_4}^2+\sigma^2}$$
$$\left.+\frac{\left(R_1^{m2}+I_1^{a2}\right)\left({R_4}^2+{I_4}^2+\sigma^2\right)-\left(R_3^mR_4+I_3^mI_4\right)\left({R_2}^2+{I_2}^2\right)}{\left(R_3^{m2}+I_3^{m2}\right){B_k}^2+\left(R_3^mR_4+I_3^aI_4\right)B_k+{R_4}^2+{I_4}^2+\sigma^2}\right\}. \tag{20}$$

$$R_b^{n'}(m_k,n_k) = \frac{-\frac{\alpha}{2}m^{-\frac{\alpha}{2}-1}}{\ln 2\Gamma_m}\left\{\frac{\left[\left(R_1^{n2}+I_1^{n2}\right)\left(R_3^nR_4+I_3^nI_4\right)-\left(R_3^{n2}+I_3^{n2}\right)\left(R_1^nR_2+I_1^nI_2\right)\right]{A_k}^2}{\left(R_3^{n2}+I_3^{n2}\right){A_k}^2+\left(R_3^nR_4+I_3^nI_4\right)A_k+{R_4}^2+{I_4}^2+\sigma^2}\right.$$
$$+\frac{\left[\left(R_1^{n2}+I_1^{n2}\right)\left({R_4}^2+{I_4}^2+\sigma^2\right)-\left(R_3^{n2}+I_3^{n2}\right)\left({R_2}^2+{I_2}^2\right)\right]A_k}{\left(R_3^{n2}+I_3^{n2}\right){A_k}^2+\left(R_3^nR_4+I_3^nI_4\right)A_k+{R_4}^2+{I_4}^2+\sigma^2}$$
$$\left.+\frac{\left(R_1^{n2}+I_1^{n2}\right)\left({R_4}^2+{I_4}^2+\sigma^2\right)-\left(R_3^nR_4+I_3^nI_4\right)\left({R_2}^2+{I_2}^2\right)}{\left(R_3^{n2}+I_3^{n2}\right){A_k}^2+\left(R_3^nR_4+I_3^nI_4\right)A_k+{R_4}^2+{I_4}^2+\sigma^2}\right\}. \tag{26}$$

convex version as follows.

$$\textbf{P2.1:} \max_{L_r,m,n,x,y,R_e} \quad R_b^l(m,n)-R_e \tag{33a}$$
$$s.t. \quad R_b^l(m,n)\geq R_{min}, \tag{33b}$$
$$D_{ar}\leq m, \tag{33c}$$
$$D_{rb}\leq n, \tag{33d}$$
$$D_{ar}\geq \mathrm{e}^{-\mathrm{x}}, \tag{33e}$$
$$D_{re}\geq \mathrm{e}^{-\mathrm{y}}, \tag{33f}$$
$$R_e\leq \tilde{R}_e^{(}x,y), \tag{33g}$$

which is mathematically solvable, and can be solved easily via cvx.

B. Optimization of $\mathbf{\Theta}$ With A Given L_r

Then, we derive the optimal $\mathbf{\Theta}$ with a given L_r. The channel gain of BS-IRS-Bob link can be denoted as $\mathbf{h}_{rb}\mathbf{\Theta}\mathbf{H}_{ar}$, which can be changed into

$$\mathbf{h}_{rb}\mathbf{\Theta}\mathbf{H}_{ar}=[\mathbf{\Theta}_{11},\mathbf{\Theta}_{22},\cdots,\mathbf{\Theta}_{NN}]\mathrm{diag}(\mathbf{h}_{\mathrm{rb}})\mathbf{H}_{\mathrm{ar}}=\boldsymbol{\theta}\mathbf{H}_{\mathrm{arb}}, \tag{34}$$

where $\boldsymbol{\theta}=[\mathbf{\Theta}_{11},\mathbf{\Theta}_{22},\cdots,\mathbf{\Theta}_{NN}]$.

In addition, we further define $\tilde{\boldsymbol{\theta}}$ and $\tilde{\boldsymbol{H}}_b$ as

$$\tilde{\boldsymbol{\theta}}=[\boldsymbol{\theta}\quad 1], \tag{35}$$

and

$$\tilde{\boldsymbol{H}}_b=\begin{pmatrix}\mathbf{H}_{arb}\\ \mathbf{h}_{ab}\end{pmatrix}. \tag{36}$$

Then, R_b in (8) can be altered into

$$R_b=\log_2\left(1+\frac{\left|\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_b\mathbf{f}_1\right|^2}{\left|\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_b\mathbf{f}_2\right|^2+\sigma^2}\right). \tag{37}$$

Let $\tilde{\boldsymbol{H}}_{b1}=\tilde{\boldsymbol{H}}_b\mathbf{f}_1\mathbf{f}_1^H\tilde{\boldsymbol{H}}_b^H$ and $\tilde{\boldsymbol{H}}_{b2}=\tilde{\boldsymbol{H}}_b\mathbf{f}_2\mathbf{f}_2^H\tilde{\boldsymbol{H}}_b^H$, based on which R_b in (38) can be changed into

$$R_b=\log_2\left(1+\frac{\frac{1}{\sigma^2}\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_{b1}\tilde{\boldsymbol{\theta}}^H}{\frac{1}{\sigma^2}\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_{b2}\tilde{\boldsymbol{\theta}}^H+1}\right). \tag{38}$$

Similarly, by letting $\mathbf{H}_{are}=\mathrm{diag}(\mathbf{h}_{\mathrm{re}})\mathbf{H}_{\mathrm{ar}}$, we can also define $\tilde{\boldsymbol{H}}_e$ as

$$\tilde{\boldsymbol{H}}_e=\begin{pmatrix}\mathbf{H}_{are}\\ \mathbf{h}_{ae}\end{pmatrix}. \tag{39}$$

Then, we further define $\tilde{\boldsymbol{H}}_{e1}=\tilde{\boldsymbol{H}}_e\mathbf{f}_1\mathbf{f}_1^H\tilde{\boldsymbol{H}}_e^H$ and $\tilde{\boldsymbol{H}}_{e2}=\tilde{\boldsymbol{H}}_e\mathbf{f}_2\mathbf{f}_2^H\tilde{\boldsymbol{H}}_e^H$. Thus, R_e in (9) can be changed into

$$R_e=\log_2\left(1+\frac{\frac{1}{\sigma^2}\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_{e1}\tilde{\boldsymbol{\theta}}^H}{\frac{1}{\sigma^2}\tilde{\boldsymbol{\theta}}\tilde{\boldsymbol{H}}_{e2}\tilde{\boldsymbol{\theta}}^H+1}\right), \tag{40}$$

However, the optimization problem is still non-convex. By applying the semidefinite relaxation (SDR), P1 can be turned into

$$\textbf{P3:} \max_{\mathbf{\Theta},L_r} \left\{\ln\left[\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathrm{H}}_{\mathrm{b1}}+\tilde{\mathrm{H}}_{\mathrm{b2}}\right)\tilde{\Theta}+1\right]+\ln S_b^*+1\right.$$
$$-S_b^*\left[\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathrm{H}}_{\mathrm{b2}}\tilde{\Theta}\right)+1\right]+\ln\left[\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathrm{H}}_{\mathrm{e2}}\tilde{\Theta}\right)+1\right]$$
$$\left.S_e^*\left[\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathrm{H}}_{\mathrm{e1}}+\tilde{\mathrm{H}}_{\mathrm{e2}}\right)\tilde{\Theta}+1\right]+\ln S_e^*+1\right\}\frac{1}{\ln 2} \tag{41a}$$
$$s.t. \quad \tilde{\mathbf{\Theta}}\succeq 0, \tag{41b}$$
$$\tilde{\mathbf{\Theta}}_{nn}=1, \tag{41c}$$

where $\tilde{\mathbf{\Theta}}=\tilde{\boldsymbol{\theta}}^H\tilde{\boldsymbol{\theta}}\in\mathbb{C}^{N+1\times N+1}$ and $\mathrm{Tr}(*)$ is the trace of $*$. S_b^* and S_e^* can be derived according to [11] as

$$S_b^*=\left[\frac{1}{\sigma^2}\mathrm{Tr}\left(\tilde{\mathrm{H}}_{\mathrm{b2}}\tilde{\mathbf{\Theta}}^{(\mathrm{r})}\right)+1\right]^{-1}, \tag{42}$$

and

$$S_e^* = \left[\frac{1}{\sigma^2}\mathrm{Tr}\left(\left(\tilde{\mathrm{H}}_{\mathrm{e1}}+\tilde{\mathrm{H}}_{\mathrm{e2}}\right)\tilde{\boldsymbol{\Theta}}^{(\mathrm{r})}\right)+1\right]^{-1}, \qquad (43)$$

where $\tilde{\boldsymbol{\Theta}}^{(r)}$ is the optimal value derived from the r-th derivation. Till now, P3 is convex and mathematically solvable through alternative optimization.

To obtain $\boldsymbol{\Theta}$ from $\tilde{\boldsymbol{\Theta}}$, we can apply eigenvalue decomposition via Gaussian randomizing. The overall algorithm summarisation can be found in Algorithm 1.

Algorithm 1 Secure data transmission

```
**Initialization** Initialize $\tilde{\boldsymbol{\theta}}^{(0)}, L_r^{(0)}$.
Set iteration index $i = 0$.
**repeat**
    Set iteration index $i = 0$. $\tilde{\boldsymbol{\Theta}}^{(0)} = \tilde{\boldsymbol{\theta}}^H\tilde{\boldsymbol{\theta}}$.
    **repeat**
        With given $\tilde{\boldsymbol{\Theta}}^{(0)}$, find the optimal $L_r^{(k)}$ by solving P2.1.
        Update $k = k + 1$.
    **until** The objective value of P2.1 reaches convergence.
    Update $L_r^{(0)} = L_r^{(k)}$.
    Set interaction index $j = 0$.
    **repeat**
        With given $L_r^{(0)}$, find the optimal $\tilde{\boldsymbol{\Theta}}^{(j)}$ by solving P3.
        Update $j = j + 1$.
    **until** The objective value of P3 reaches convergence.
    Update $\tilde{\boldsymbol{\Theta}}^{(0)} = \tilde{\boldsymbol{\Theta}}^{(j)}$.
**until** The objective value of P1 reaches convergence
Recover $\boldsymbol{\Theta}$ from $\tilde{\boldsymbol{\Theta}}^{(0)}$
```

IV. Simulation

Simulation results are presented and discussed in this section to evaluate the effectiveness of the proposed scheme. The location coordinates of BS, Bob, and Eav are assumed to be $L_a = (0, 0, 20)$, $L_b = (200, 0, 0)$, and $L_e = (200, 100, 0)$ in meter, respectively. The path loss reference at 1 m is set to $\rho_0 = -30$ dB and the large-scale path loss exponent is set to $\alpha = 3$. The Rician factor K is set to 5. Then, the antennas on BS and the reflection elements of IRS are set to $M = 8$ and $N = 25$, respectively. $P_{amax} = 1$ W and $\sigma^2 = -110$ dBm.

In Fig. 2, the effectiveness of the proposed scheme is investigated. The achievable secrecy rate is compared over the proposed scheme, when there is no IRS optimization, and when there is no location optimization. The location of IRS is set to $L_r = (0, 100, 50)$ when there is no location optimization. We only consider the direct link when there is no $\boldsymbol{\Theta}$ optimization. From the results, we can see that the proposed scheme can achieve a higher R_s compared with when there is no $\boldsymbol{\Theta}$ optimization or no L_r optimization. In addition, we can see that the secrecy rate increases with the maximum allowed transmit power. The achievable secrecy rate is higher in the No IRS optimization scheme compared with the No location optimization scheme. This is because there are two path losses considered in the No location optimization scheme, which are BS-IRS and IRS-Bob, which will introduce a higher loss in the transmitted signals.

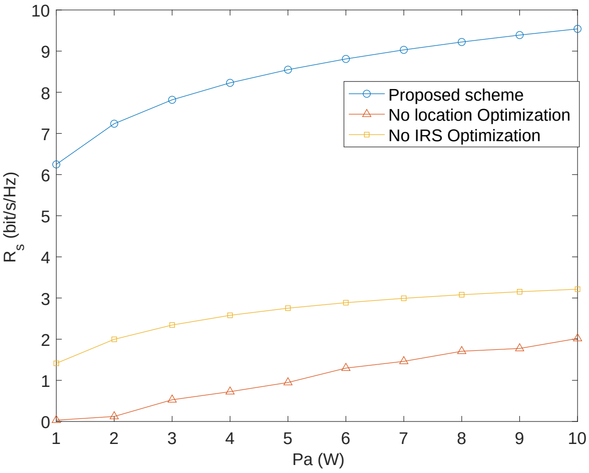


Fig. 2. Comparision of the achievable secrecy rate among the proposed scheme, without IRS optimization, and without location optimization.

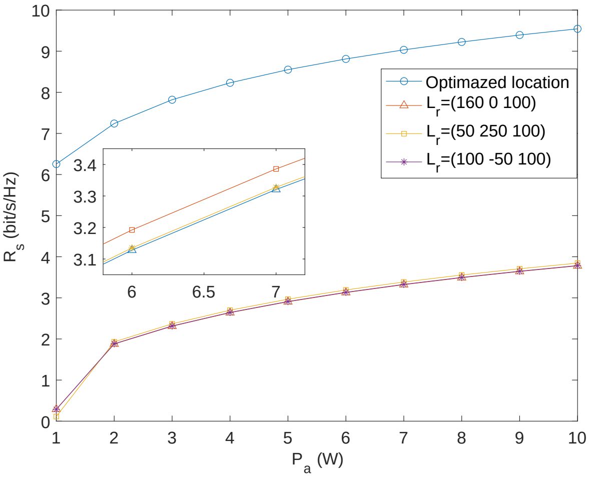


Fig. 3. Comparision of the achievable secrecy rate with different transmit power when the IRS is at different locations.

The impact of different IRS locations L_r and transmit power P_{amax} on the secrecy rate R_s are investigated in Fig. 3. We have the IRS locates at the optimized location, $L_r = (160, 0, 100)$, $L_r = (50, 250, 100)$, and $L_r = (150, -50, 100)$. The optimized IRS location is derived from Algorithm 1 listed in Table 1. From the results, we can see that the secrecy rate with L_r derived by the proposed scheme is higher than the other locations. In addition, the secrecy rate R_s also increases with the rising of the maximum allowed transmit power P_{amax}.

V. Conclusion

A secure IRS-on-UAV assisted wireless communication network is proposed and optimized in this paper. We proposed a secure transmission scheme to leverage both IRS and

$$
\begin{aligned}
R_e^{x'}(x_k, y_k) = & \frac{\alpha \mathrm{e}^{-\frac{\alpha}{2}\mathrm{x_k}}}{\ln 2\Gamma_e^k} \left\{ \frac{\left[\left(R_1^{x\,2} + I_1^{x\,2}\right)\left(R_3^x R_4^e + I_3^x I_4^e\right) - \left(R_3^{x\,2} + I_3^{x\,2}\right)\left(R_1^x R_2^e + I_1^x I_2^e\right)\right] {Y_k}^2}{\left(R_3^{x\,2} + I_3^{x\,2}\right){Y_k}^2 + \left(R_3^x R_4^e + I_3^x I_4^e\right) Y_k + R_4^{e\,2} + I_4^{e\,2} + \sigma^2} \right. \\
& + \frac{\left[\left(R_1^{x\,2} + I_1^{x\,2}\right)\left(R_4^{e\,2} + I_4^{e\,2} + \sigma^2\right) - \left(R_3^{x\,2} + I_3^{x\,2}\right)\left(R_2^{e\,2} + I_2^{e\,2}\right)\right] Y_k}{\left(R_3^{x\,2} + I_3^{x\,2}\right){Y_k}^2 + \left(R_3^x R_4^e + I_3^x I_4^e\right) Y_k + R_4^{e\,2} + I_4^{e\,2} + \sigma^2} \\
& \left. + \frac{\left(R_1^{x\,2} + I_1^{x\,2}\right)\left(R_4^{e\,2} + I_4^{e\,2} + \sigma^2\right) - \left(R_3^x R_4^e + I_3^x I_4^e\right)\left(R_2^{e\,2} + I_2^{e\,2}\right)}{\left(R_3^{x\,2} + I_3^{x\,2}\right){Y_k}^2 + \left(R_3^x R_4^e + I_3^x I_4^e\right) Y_k + R_4^{e\,2} + I_4^{e\,2} + \sigma^2} \right\},
\end{aligned}
\tag{44}
$$

$$
\begin{aligned}
R_e^{y'}(x_k, y_k) = & \frac{\alpha \mathrm{e}^{-\frac{\alpha}{2}\mathrm{y_k}}}{\ln 2\Gamma_e^k} \left\{ \frac{\left[\left(R_1^{y\,2} + I_1^{y\,2}\right)\left(R_3^y R_4^e + I_3^y I_4^e\right) - \left(R_3^{y\,2} + I_3^{y\,2}\right)\left(R_1^y R_2^e + I_1^y I_2^e\right)\right] {X_k}^2}{\left(R_3^{y\,2} + I_3^{y\,2}\right){X_k}^2 + \left(R_3^y R_4^e + I_3^y I_4^e\right) X_k + R_4^{e\,2} + I_4^{e\,2} + \sigma^2} \right. \\
& + \frac{\left[\left(R_1^{y\,2} + I_1^{y\,2}\right)\left(R_4^{e\,2} + I_4^{e\,2} + \sigma^2\right) - \left(R_3^{y\,2} + I_3^{y\,2}\right)\left(R_2^{e\,2} + I_2^{e\,2}\right)\right] X_k}{\left(R_3^{y\,2} + I_3^{y\,2}\right){X_k}^2 + \left(R_3^y R_4^e + I_3^x I_4^e\right) X_k + R_4^{e\,2} + I_4^{e\,2} + \sigma^2} \\
& \left. + \frac{\left(R_1^{y\,2} + I_1^{y\,2}\right)\left(R_4^{e\,2} + I_4^{e\,2} + \sigma^2\right) - \left(R_3^y R_4^e + I_3^y I_4^e\right)\left(R_2^{e\,2} + I_2^{e\,2}\right)}{\left(R_3^{y\,2} + I_3^{y\,2}\right){X_k}^2 + \left(R_3^y R_4^e + I_3^y I_4^e\right) X_k + R_4^{e\,2} + I_4^{e\,2} + \sigma^2} \right\},
\end{aligned}
\tag{50}
$$

precoding to maximize the secrecy rate while preventing eavesdropping. In the proposed scheme, we optimize the location and phase-shifting matrix to maximize the secrecy rate, where the optimization problem is non-convex and cannot be solved via a mathematical method. The location and phase-shifting vector are alternatively optimized to solve the problem. The SCA and first-order Taylor expansion are leveraged to optimize the hovering location of the UAV. Then, SDR is applied to derive the optimized phase-shifting matrix. With alternative optimization, both the phase shifting matrix and location are optimized to achieve a maximum achievable secrecy rate. Finally, simulation results are demonstrated and discussed to evaluate the effectiveness of our proposed scheme. In future work, multi-antenna will be designed and utilized to further improve the performance of this algorithm.

Appendix A
Details of $\tilde{R}_e(x, y)$

Based on (32), the first-order derivative of R_e with respect to x can be illustrated as

where $Y_k = \mathrm{e}^{\frac{\alpha}{2}\mathrm{y_k}}$ and $X_k = \mathrm{e}^{\frac{\alpha}{2}\mathrm{x_k}}$. Γ_e^k is defined as

$$
\Gamma_e^k = \frac{\left| X_k Y_k \tilde{\mathbf{h}}_{ae}^r \mathbf{f}_1 + \mathbf{h}_{ae}\mathbf{f}_1 \right|^2}{\left| X_k Y_k \tilde{\mathbf{h}}_{ae}^r \mathbf{f}_2 + \mathbf{h}_{ae}\mathbf{f}_2 \right|^2 + \sigma^2} + 1, \tag{45}
$$

In addition, we define R_1^x, I_1^x, R_2^e, I_2^e, R_3^x, I_3^x, R_4^e, and I_4^e in (44) as

$$
Y_k \tilde{\mathbf{h}}_{ae}^r \mathbf{f}_1 = R_1^x + iI_1^x, \tag{46}
$$

$$
\mathbf{h}_{ae}\mathbf{f}_1 = R_2^e + iI_2^e, \tag{47}
$$

$$
Y_k \tilde{\mathbf{h}}_{ae}^r \mathbf{f}_2 = R_3^x + iI_3^x, \tag{48}
$$

$$
\mathbf{h}_{ae}\mathbf{f}_2 = R_4^e + iI_4^e, \tag{49}
$$

On the other hand, $R_e^{y'}(x_k, y_k)$ can be expressed as (50). We further define R_1^y, I_1^y, R_3^y, and I_3^y in (50) as

$$
X_k \tilde{\mathbf{h}}_{ae}^r \mathbf{f}_1 = R_1^y + iI_1^y, \tag{51}
$$

$$
X_k \tilde{\mathbf{h}}_{ae}^r \mathbf{f}_2 = R_3^y + iI_3^y. \tag{52}
$$

Till now, the details of $\tilde{R}_e(x, y)$ are demonstrated.

References

[1] B. Zheng, C. You, W. Mei, and R. Zhang, "A survey on channel estimation and practical passive beamforming design for intelligent reflecting surface aided wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1035–1071, 2nd Quart. 2022.

[2] C. You and R. Zhang, "Wireless communication aided by intelligent reflecting surface: Active or passive?," *IEEE Wireless Commun. Lett.*, vol. 10, no. 12, pp. 2659–2663, Dec. 2021.

[3] W. Wang, X. Liu, J. Tang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Beamforming and jamming optimization for IRS-aided secure NOMA networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 3, pp. 1557–1569, Mar. 2022.

[4] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2283–2314, 4th Quart. 2020.

[5] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, 2nd Quart. 2016.

[6] X. Chen, M. Sheng, N. Zhao, W. Xu, and D. Niyato, "UAV-relayed covert communication towards a flying warden," *IEEE Trans. Commun.*, vol. 69, no. 11, pp. 7659–7672, Nov. 2021.

[7] B. Zhu, E. Bedeer, H. H. Nguyen, R. Barton, and J. Henry, "UAV trajectory planning in wireless sensor networks for energy consumption minimization by deep reinforcement learning," *IEEE Trans. Vehi. Tech.*, vol. 70, no. 9, pp. 9540–9554, Sept. 2021.

[8] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K.-K. Wong, "IRS-assisted secure UAV transmission via joint trajectory and beamforming design," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1140–1152, Feb. 2022.

[9] S. Jiao, F. Fang, X. Zhou, and H. Zhang, "Joint beamforming and phase shift design in downlink UAV networks with IRS-assisted noma," *J. Commun. Inf. Networks*, vol. 5, no. 2, pp. 138–149, Jun. 2020.

[10] Z. Mohamed and S. Aissa, "Leveraging UAVs with intelligent reflecting surfaces for energy-efficient communications with cell-edge users," in *Proc. IEEE ICC Workshops*, pp. 1–6, Dublin, Ireland, 2020.

[11] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sept. 2013.

IV

ENHANCING COVERT SECRECY RATE IN A ZERO-FORCING UAV JAMMER-ASSISTED COVERT COMMUNICATION

by

Xinying Chen, Zheng Chang, and Timo Hämäläinen 2024

IEEE Wireless Communications Letters, accepted for publication

Enhancing Covert Secrecy Rate in A Zero-Forcing UAV Jammer-Assisted Covert Communication

Xinying Chen, Zheng Chang, *Senior Member, IEEE,* and Timo Hämäläinen, *Senior Member, IEEE*

***Abstract*—Covert communications can hide confidential signals in environmental noise to avoid being detected and provide comprehensive security for wireless transmissions. However, there still exist significant risks in wireless transmission once being detected. In this paper, we propose a more secure covert scheme, where a multiple antennas transmitter, assisted by a multi-antenna UAV jammer, maximizes the covert secrecy rate under the scenarios of both correct and incorrect detection by a warden with both error detection probability and eavesdropping rate limitations satisfied. The transmitter and jammer adopt maximum ratio transmission (MRT) and zero-forcing, respectively, to maximize the transmission rate and minimize the interference at the legitimate receiver. First, we analyze the monotonicity of error detection probability to determine the optimal power detection threshold and the corresponding smallest error detection probability. Then, under this worst case, we jointly optimize the transmit and jamming power to maximize the covert secrecy rate while guaranteeing the covert and eavesdropping limits meet their requirements, respectively. Finally, simulation results are presented to prove the correctness of the theoretical conclusion and evaluate the effectiveness of our proposed scheme.**

***Index Terms*—Covert communication, Gaussian signaling, secure transmission, UAV, zero-forcing.**

I. Introduction

Wireless communication has brought tremendous convenience and enabled fast connections to everyone. However, the characteristic of broadcasting in wireless networks also posts confidential messages under the risk of leakage. Therefore, transmission security becomes more and more important, especially when the messages contain personal data or sensitive information [1]. There are two typical methods to achieve secure wireless communications, i.e., physical layer security (PLS) and covert communications [2]. PLS attains secure transmission by utilizing the randomness of wireless channels combined with precoding and signal processing, which aims to reduce the eavesdropping rate [3]. However, PLS can still be exposed to a higher risk of being eavesdropped as the wireless techniques develop. Different from PLS, covert communications provide concealment via hiding confidential signals in environmental noise, where the warden does not decode the signals without detection, and thus provide transmission security [4]. Nevertheless, the covert communication cannot provide secure transmission once the transmission behavior is correctly detected.

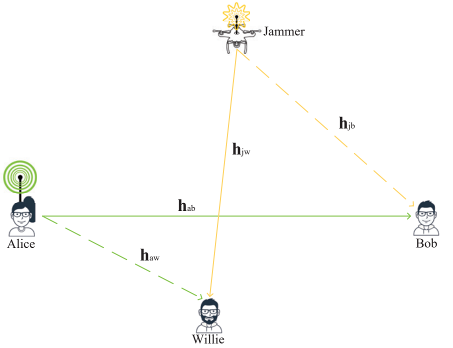


Fig. 1. System model of a zero-forcing UAV jammer-assisted covert communication network.

The unmanned aerial vehicle (UAV), widely exploited in wireless communications, has plenty of advantages, e.g., fast deployment, light volume, and high mobility, among which it can also leverage the air-to-ground line-of-sight (LoS) channels [5]. Channel randomness has been exploited to offer secure transmission in PLS and covert networks, which also brings the difficulties of obtaining channel state information (CSI). In one respect, the difficulty of acquiring CSI makes it hard for malicious users to eavesdrop; in another respect, it is also difficult to obtain CSI for legitimate users while utilizing channel uncertainty [6]. The introduction of UAVs changes this predicament. Although the characteristic of the LoS channel increases the risk of information leakage, on the other hand, benefiting from the UAV employment, it also enables legitimate users to obtain CSI easily within the network [7]. The easy obtainment of CSI in LoS channels proliferates the study and application of the multi-antenna technique. The multi-antenna technique, which leverages channel multiplexing, has been broadly exploited in PLS and covert communications to achieve better transmission performance [8]. The multiple antennas can be used to realize maximum ratio transmission (MRT), where the precoding vector is designed according to the CSI to achieve a maximum signal-to-interference ratio (SINR) [9]. It can also be employed in jamming-assisted networks to realize zero-forcing, which can minimize the undesired interference at specific users [10].

Unlike most of the existing research works on covert communications, which primarily focuses on improving the performance during miss detection phase, i.e., maximizing the transmission rate, this paper investigates a covert network that aims to provide comprehensive security protection for both correct and incorrect detection cases [4], [7], [9]. We jointly optimize the transmit and jamming power to maximize the covert secrecy rate while avoiding being detected and eavesdropped, thereby ensuring secure transmission even when the transmission behavior of the transmitter is correctly detected. First, the optimal power detection threshold and the corresponding minimized error detection probability at the warden are derived. Then, the transmit and jamming power are optimized to achieve a higher covert secrecy rate while

This work is partly supported by the National Natural Science Foundation of China (NSFC) under Grant 62071105 and supported in part by Horizon EU Grant No. 101086159.

X. Chen and Timo Hämäläinen are with the Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, FIN-40014 Jyväskylä, Finland (email: xinying.x.chen@jyu.fi; timo.t.hamalainen@jyu.fi).

Z. Chang is with School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, China, and also with Faculty of Information Technology, University of Jyväskylä, P.O. Box 35, FIN-40014 Jyväskylä, Finland. (email: zheng.chang@jyu.fi).

This article has been accepted for publication in IEEE Wireless Communications Letters. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/LWC.2024.3465871

guaranteeing both the optimal error detection probability and the eavesdropping rate are within the limits.

II. System Model

Consider a covert communication system where Alice transmits confidentially to Bob while avoiding detection by Willie, aided by a UAV jammer emitting jamming signals constantly, as shown in Fig.1. The locations of Alice, the jammer, Bob, and Willie are $L_a(x_a, y_a, 0)$, $L_j(x_j, y_j, H)$[1], $L_b(x_b, y_b, 0)$, $L_w(x_w, y_w, 0)$, respectively, where H is the fixed hovering altitude of the drone jammer. Assume that Alice is equipped with M antennas, the jammer is equipped with N antennas, while both Bob and Willie are equipped with single receiving antennas. The channel coefficients for ground users from Alice to Bob $\mathbf{h}_{ab} \in \mathbb{C}^{1\times M}$ and to Willie $\mathbf{h}_{aw} \in \mathbb{C}^{1\times M}$ are assumed to follow a large-scale path loss and a small-scale Rayleigh fading, which can be described as

$$\mathbf{h}_{ab} = \sqrt{\rho_0/d_{ab}^{-\alpha}}\mathbf{g}_{ab}, \tag{1}$$

$$\mathbf{h}_{aw} = \sqrt{\rho_0/d_{aw}^{-\alpha}}\mathbf{g}_{aw}, \tag{2}$$

where $d_{ab} = ||L_a - L_b||$ and $d_{aw} = ||L_a - L_w||$ are the distances from Alice to Bob and to Willie, respectively. ρ_0 is the reference power gain at 1 m and α denotes the large-scale path loss exponent. In addition, each Rayleigh fading component $g_{a_i b}$ and $g_{a_i w}$, $\forall i \in \{1, \cdots, M\}$, in both $\mathbf{g}_{ab}$ and $\mathbf{g}_{aw}$ is independent and identically distributed (i.i.d), which follows complex Gaussian distribution with zero mean and unit variance, i.e., $g_{a_i b} \sim \mathcal{CN}(0, 1)$ and $g_{a_i w} \sim \mathcal{CN}(0, 1)$.

The air-to-ground channels from the jammer to Bob $\mathbf{h}_{jb} \in \mathbb{C}^{1\times N}$ and to Willie $\mathbf{h}_{jw} \in \mathbb{C}^{1\times N}$ are assumed to be LoS channels. They can be denoted as

$$\mathbf{h}_{jb} = \sqrt{\rho_0/d_{jb}^{-\alpha}}\mathbf{g}_{jb}, \tag{3}$$

$$\mathbf{h}_{jw} = \sqrt{\rho_0/d_{jw}^{-\alpha}}\mathbf{g}_{jw}, \tag{4}$$

where $d_{jb} = ||L_j - L_b||$ and $d_{jw} = ||L_j - L_w||$ are the distances from the jammer to Bob and to Willie, respectively. $\forall i \in \{1, \cdots, N\}$, we have $|g_{j_i b}| = |g_{j_i w}| = 1$, where $g_{j_i b} \in \mathbf{g}_{jb}$ and $g_{j_i w} \in \mathbf{g}_{jw}$.

In order to achieve higher uncertainty and avoid being detected by Willie, Alice selects time slots with a probability of $\pi = 0.5$ to transmit baseband signal $x[k]$ with transmit power P_a to Bob. Suppose the CSI among legitimate users is known to each other, which can be obtained through channel sounding, CSI feedback, and fast CSI reporting techniques. Alice adopts MRT towards Bob to achieve better performance, where her precoding vector $\mathbf{u} \in \mathbb{C}^{M\times 1}$ can be defined as

$$\mathbf{u} = \mathbf{g}_{ab}^H/||\mathbf{g}_{ab}||. \tag{5}$$

Additionally, the jammer constantly emits jamming signals to assist Alice in avoiding being detected by Willie. In order to introduce uncertainty at Willie, the jammer applies Gaussian signaling $\mathbb{J}x_j[k] \sim \mathcal{CN}(0, P_j)$. With CSI $\mathbf{g}_{jb}$ obtainable at the jammer, it can employ zero-forcing precoding towards Bob, where the precoding vector $\mathbf{v} \in \mathbb{C}^{N\times 1}$can be described as

$$\begin{cases} \mathbf{g}_{jb}\mathbf{v} = 0, \\ ||\mathbf{v}||^2 = 1. \end{cases} \tag{6}$$

Therefore, the received signals at Bob in each time slot can be denoted as

$$y_b[k] = \sqrt{P_a}\mathbf{h}_{ab}\mathbf{u}x[k] + n_b[k], \tag{7}$$

where $n_b[k]$ is the additive white Gaussian noise (AWGN) received at Bob, and it follows complex Gaussian distribution, i.e., $n_b[k] \sim \mathcal{CN}(0, \sigma_b^2)$. Correspondingly, the transmission rate R_b at Bob can be expressed as

$$R_b = \log_2\left(1 + P_a\rho_0|\mathbf{g}_{ab}\mathbf{u}|^2/(d_{ab}^{\alpha}\sigma_b^2)\right). \tag{8}$$

Since the zero-forcing is designed towards only Bob, Willie receives signals from both Alice and the jammer, which can be denoted as

$$y_w[k] = \sqrt{P_a}\mathbf{h}_{aw}\mathbf{u}x[k] + \mathbb{J}\mathbf{h}_{jw}\mathbf{v}x_j[k] + n_w[k], \tag{9}$$

where $n_w[k]$ is the i.i.d AWGN received at Willie in each time slot and follows $n_w[k] \sim \mathcal{CN}(0, \sigma_w^2)$. The corresponding eavesdropping rate R_e at Willie can be calculated as

$$R_e = \log_2\left(1 + \frac{P_a\rho_0|\mathbf{g}_{aw}\mathbf{u}|^2/d_{aw}^{\alpha}}{\rho_0|\mathbf{g}_{jw}\mathbf{v}|^2P_j/d_{jw}^{\alpha} + \sigma_w^2}\right). \tag{10}$$

III. The Optimal Detection of Willie

Willie needs to decide whether Alice is transmitting $\mathcal{H}_1$ or silent $\mathcal{H}_0$ according to his received signal power, and then decide whether to decode the received signals or not. The received signals of the two above-mentioned cases can be denoted as

$$y_w[k]=\begin{cases} \mathbb{J}\mathbf{h}_{jw}\mathbf{v}x_j[k] + n_w[k], & \mathcal{H}_0, \\ \sqrt{P_a}\mathbf{h}_{aw}\mathbf{u}x[k] + \mathbb{J}\mathbf{h}_{jw}\mathbf{v}x_j[k] + n_w[k], & \mathcal{H}_1. \end{cases} \tag{11}$$

Willie measures his received samples N times and derives the averaged received signal power P_w to compare with his preset power detection threshold ξ, and then makes his decision. The decision rule can be described as

$$P_w = \frac{1}{N}\sum_{k=1}^{N}|y_w[k]|^2 \overset{\mathcal{D}_1}{\underset{\mathcal{D}_0}{\gtrless}} \xi, \tag{12}$$

where N is the number of samples. Willie decides that Alice is transmitting $\mathcal{D}_1$ when P_w is larger than ξ, and Alice keeps silent $\mathcal{D}_0$ when P_w is smaller than ξ.

We consider the interference limit network, i.e., σ_b^2 and σ_w^2 can be ignored in Willie's detection. As the signal samples get larger, i.e., $N \to \infty$, the averaged received power P_w can be rewritten as

$$P_w = \begin{cases} J, & \mathcal{H}_0, \\ S + J, & \mathcal{H}_1, \end{cases} \tag{13}$$

where J and S represent the jamming and signal power, respectively. They can be summarized as

$$J = |\mathbb{J}x_j[k]|^2|\mathbf{h}_{jw}\mathbf{v}|^2, \tag{14}$$

$$S = P_a|\mathbf{h}_{aw}\mathbf{u}|^2. \tag{15}$$

According to the decision rule in (12), there are two types of mistakes that Willie may make, which are the false alarm (FA) and the miss detection (MD). The FA mistake indicates that Willie believes that Alice is transmitting while she is silent. MD indicates that Willie believes that Alice is silent while she is transmitting. The error detection probability p_e is defined as the probability that Willie makes FA and MD mistakes, which can be described as

$$p_e=\mathbb{P}_{FA}+\mathbb{P}_{MD}=\mathbb{P}(\mathcal{D}_1|\mathcal{H}_0)+\mathbb{P}(\mathcal{D}_0|\mathcal{H}_1)=\mathbb{P}(J\geq\xi)+\mathbb{P}(J+S\leq\xi). \tag{16}$$

On the other hand, the correct detection probability of Willie can be expressed as

[1] The jammer can adjust its location and track Willie for optimal jamming once Willie's location is obtainable.

$$\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1) = \mathbb{P}(J + S \geq \xi). \tag{17}$$

Owing to $\mathbb{J}x_j[k] \sim \mathcal{CN}(0, P_j)$, $|\mathbb{J}x_j[k]|^2$ follows a chi-square distribution with 2 degrees of freedom, which equivalents to exponential distribution. Thus, we can conclude $J \sim \exp(\lambda_j)$, $\lambda_j = \frac{d_{jw}^{\alpha}}{P_j \rho_0 |\mathbf{g}_{jw}\mathbf{v}|^2}$.

As for $\mathbf{g}_{aw} \sim \mathcal{CN}(0, \mathbf{I})$ and $\mathbf{g}_{ab} \sim \mathcal{CN}(0, \mathbf{I})$ are i.i.d and follow the same distribution, we can conclude that $|\mathbf{h}_{aw}\mathbf{u}|^2 \sim \exp(1)$. This further leads to $S \sim \exp(\lambda_s)$, where denote $\lambda_s = \frac{d_{aw}^{\alpha}}{P_a \rho_0}$.

Correspondingly, p_e in (16) can be changed into

$$\begin{aligned} p_e &= 1 - \mathbb{F}_J(\xi) + \mathbb{F}_{J+S}(\xi) = e^{-\lambda_j \xi} + \int_0^{\xi} \mathbb{F}_J(\xi - x) f_S(x) dx \\ &= \begin{cases} 1 - \lambda_j \left(e^{-\lambda_j \xi} - e^{-\lambda_s \xi}\right) / (\lambda_s - \lambda_j), & \lambda_s \neq \lambda_j, \\ 1 - \lambda_s \xi e^{-\lambda_s \xi}, & \lambda_s = \lambda_j. \end{cases} \end{aligned} \tag{18}$$

Similarly, the correct detection probability $\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1)$ in (17) can be altered to

$$\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1) = \begin{cases} \left(\lambda_s e^{-\lambda_j \xi} - \lambda_j e^{-\lambda_s \xi}\right) / (\lambda_s - \lambda_j), & \lambda_s \neq \lambda_j, \\ (1 + \lambda_s \xi) e^{-\lambda_s \xi}, & \lambda_s = \lambda_j. \end{cases} \tag{19}$$

From the definition of λ_j, λ_s, and the expression of p_e in (18), we can see that p_e is related to ξ. Willie can achieve a smaller p_e by properly choosing his power detection threshold. The optimal ξ to minimize Willie's error detection probability p_e is derived in Proposition 1.

Proposition 1: The optimal power detection threshold at Willie can be expressed as

$$\xi^* = \begin{cases} (\ln \lambda_s - \ln \lambda_j) / (\lambda_s - \lambda_j), & \lambda_s \neq \lambda_j, \\ 1/\lambda_s, & \lambda_s = \lambda_j. \end{cases} \tag{20}$$

and the corresponding minimized error detection probability p_e^* can be derived as

$$p_e^* = \begin{cases} 1 - (\lambda_s/\lambda_j)^{-\frac{\lambda_s}{\lambda_s - \lambda_j}}, & \lambda_s \neq \lambda_j, \\ 1 - 1/e, & \lambda_s = \lambda_j. \end{cases} \tag{21}$$

Proof. We first analyze the general case when $\lambda_s \neq \lambda_j$. The impact of ξ on p_e can be obtained by analyzing the monotonicity of p_e. The first-order derivative of p_e with respect to ξ can be derived as

$$p_e'(\xi) = -\lambda_j \left(-\lambda_j e^{-\lambda_j \xi} + \lambda_s e^{-\lambda_s \xi}\right) / (\lambda_s - \lambda_j). \tag{22}$$

The zeros of $p_e'(\xi)$ in (22) can be derived as $\xi_0 = \frac{\ln \lambda_s - \ln \lambda_j}{\lambda_s - \lambda_j}$.

Based on the definition of λ_s and λ_j, we can have $\lambda_s > 0$ and $\lambda_j > 0$. We discuss the monotonicity of p_e with respect to ξ under two cases, i.e., $\lambda_s > \lambda_j$ and $\lambda_s < \lambda_j$, to derive the optimal ξ.

- $\lambda_s > \lambda_j$: In this case, we can conclude that $p_e'(\xi) > 0$, when $\xi > \xi_0$; and $p_e'(\xi) < 0$, when $\xi < \xi_0$. This indicates that p_e monotonically decreases with ξ, when $\xi < \xi_0$; and monotonically increases, when $\xi > \xi_0$. p_e obtains its minimum at ξ_0.
- $\lambda_s < \lambda_j$: We can also have $p_e'(\xi) > 0$, when $\xi > \xi_0$; and $p_e'(\xi) < 0$, when $\xi < \xi_0$. This also indicates that p_e monotonically decreases when $\xi < \xi_0$, and increases when $\xi > \xi_0$. p_e reaches its minimum at ξ_0 as well.

Both cases lead to the same optimal detection threshold ξ^* as shown in (20). Based on (18), the corresponding p_e^* is presented in (21). The conclusion for case $\lambda_s = \lambda_j$ can be derived similarly. □

With the optimal power detection threshold ξ^* in (20), the correct detection probability in (19) becomes

$$\mathbb{P}^*(\mathcal{D}_1|\mathcal{H}_1) = \begin{cases} (\lambda_s/\lambda_j)^{-\frac{\lambda_s}{\lambda_s - \lambda_j}} + (\lambda_s/\lambda_j)^{-\frac{\lambda_j}{\lambda_s - \lambda_j}}, & \lambda_s \neq \lambda_j, \\ 2/e, & \lambda_s = \lambda_j. \end{cases} \tag{23}$$

IV. Transmit and Jamming Power Optimization for a More Secure Covert Communication

A. Problem Formulation

We aim to provide a more secure transmission for covert communication between Alice and Bob against Willie. In this section, we jointly optimize transmit and jamming power to maximize the covert secrecy rate while guaranteeing Willie's optimal error detection probability is larger than the limit and the eavesdropping rate is lower than the limit. The optimization problem can be summarized as

$$\begin{aligned} \textbf{P1:} \quad & \max_{P_a, P_j} \; R_{cs} && \text{(24a)} \\ & s.t. \quad p_e^* \geq \epsilon, && \text{(24b)} \\ & \qquad R_e \leq r_e, && \text{(24c)} \\ & \qquad R_b \geq r, && \text{(24d)} \\ & \qquad P_a \leq P_{amax}, && \text{(24e)} \\ & \qquad P_j \leq P_{jmax}, && \text{(24f)} \end{aligned}$$

where ϵ is the lower limit of Willie's error detection probability, r_e represents the upper limit of Willie's eavesdropping rate, r is the lower threshold of transmission rate, P_{amax} and P_{jmax} are the maximum allowed transmit and jamming power, respectively. In addition, the covert secrecy rate R_{cs} is defined as the secrecy rate in covert communication when Alice is transmitting. It includes two cases: 1) Willie decides $\mathcal{D}_0$ when $\mathcal{H}_1$. Willie does not attempt to decode Alice's signals when he believes she is silent. 2) Willie decides $\mathcal{D}_1$ when $\mathcal{H}_1$. Alice is still possible to transmit securely without the risk of being eavesdropped on. Therefore, R_{cs} can be denoted as

$$R_{cs} = R_b \mathbb{P}(\mathcal{D}_0|\mathcal{H}_1) + (R_b - R_e) \mathbb{P}(\mathcal{D}_1|\mathcal{H}_1) = R_b - \mathbb{P}(\mathcal{D}_1|\mathcal{H}_1) R_e. \tag{25}$$

B. Impact of Constraint ϵ on P_a and P_j

According to Proposition 1, Willie can obtain his minimum error detection probability p_e^* by setting the power detection threshold as (20). To guarantee that p_e^* satisfies the constraint, the requirement of P_a and P_j is shown in Proposition 2.

Proposition 2: To guarantee (24b), the transmit and jamming power should satisfy

$$\frac{P_a}{P_j} \leq \frac{d_{aw}^{\alpha} |\mathbf{g}_{jw}\mathbf{v}|^2}{d_{jw}^{\alpha}} \frac{\mathscr{W}_0\left((1 - \epsilon) \ln(1 - \epsilon)\right)}{\ln(1 - \epsilon)}. \tag{26}$$

Proof. With the expression of p_e^* in (21) and in order to satisfy the constraint in (24b), we have

$$\left(\frac{\lambda_s}{\lambda_j}\right)^{-\frac{\frac{\lambda_s}{\lambda_j}}{\frac{\lambda_s}{\lambda_j} - 1}} \leq 1 - \epsilon. \tag{27}$$

Let $t = \frac{\lambda_s}{\lambda_j}$, and we have $t > 0$. Then, (27) can be altered to

$$\frac{t}{t - 1} \ln \frac{1}{t} \leq \ln(1 - \epsilon). \tag{28}$$

To further obtain the limitation of P_a and P_j, we need to discuss t by classifying $t > 1$ and $0 < t < 1$.

- Case $t > 1$:
  With $t \in (1, \infty)$, (28) can be changed into
  $$\begin{aligned} \ln \frac{1}{t} &\leq \frac{t-1}{t} \ln(1-\epsilon) \\ \frac{1}{t} &\leq e^{-\frac{\ln(1-\epsilon)}{t}} e^{\ln(1-\epsilon)}. \end{aligned} \tag{29}$$
  Owing to $\ln(1-\epsilon) < 0$, (29) can be altered to
  $$\ln(1-\epsilon)e^{\ln(1-\epsilon)} \leq \frac{\ln(1-\epsilon)}{t} e^{\frac{\ln(1-\epsilon)}{t}} < 0, \tag{30}$$
  which satisfies the form of the Lambert W function. Therefore, we can have
  $$\frac{\ln(1-\epsilon)}{t} \leq \mathscr{W}_{-1}(\ln(1-\epsilon)e^{\ln(1-\epsilon)}), \tag{31}$$
  or
  $$\mathscr{W}_0(\ln(1-\epsilon)e^{\ln(1-\epsilon)}) \leq \frac{\ln(1-\epsilon)}{t} < 0, \tag{32}$$
  where $\mathscr{W}_0(*)$ is the principle branch of Lambert W function, and $\mathscr{W}_{-1}(*)$ represents the negative branch.
  Practically, the error detection probability limit ϵ is close to 1. Therefore, from (31) we can have
  $$0 < \frac{\lambda_s}{\lambda_j} \leq \frac{\ln(1-\epsilon)}{\mathscr{W}_{-1}\left((1-\epsilon)\ln(1-\epsilon)\right)} = 1, \tag{33}$$
  which is against the initial assumption of $t > 1$.
  From (32), we can have
  $$\frac{\lambda_s}{\lambda_j} \geq \frac{\ln(1-\epsilon)}{\mathscr{W}_0\left((1-\epsilon)\ln(1-\epsilon)\right)}. \tag{34}$$
  Then, we can further derive the upper limit of P_a/P_j as shown in (26).
- Case $0 < t < 1$:
  Similarly, when $t \in (0, 1)$, (28) can be changed into
  $$\begin{aligned} \ln \frac{1}{t} &\geq \left(1 - \frac{1}{t}\right) \ln(1-\epsilon) \\ \frac{1}{t} &\geq e^{-\frac{\ln(1-\epsilon)}{t}} e^{\ln(1-\epsilon)} \\ \frac{\ln(1-\epsilon)}{t} e^{\frac{\ln(1-\epsilon)}{t}} &\leq \ln(1-\epsilon)e^{\ln(1-\epsilon)}. \end{aligned} \tag{35}$$
  According to Lambert W function, the solution to (35) can be derived as
  $$\frac{\ln(1-\epsilon)}{\mathscr{W}_{-1}((1-\epsilon)\ln(1-\epsilon))} \leq \frac{\lambda_s}{\lambda_j} \leq \frac{\ln(1-\epsilon)}{\mathscr{W}_0((1-\epsilon)\ln(1-\epsilon))}. \tag{36}$$
  Owing to $\frac{\ln(1-\epsilon)}{\mathscr{W}_{-1}((1-\epsilon)\ln(1-\epsilon))} = 1$, (36) is against the assumption of $t \in (0, 1)$.

The overall constraint of P_a/P_j is demonstrated in (26). □

C. Optimize P_a and P_j to Maximize R_{cs}

To maximize the covert secrecy rate R_{cs}, the transmit power P_a and jamming power P_j need to be adjusted properly while satisfying constraints in (24). The objective function (24a) is non-convex and mathematically difficult to solve. Based on the expression of $\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1)^*$ in (23) and R_{cs} in (25), we can further conclude
$$R_{cs} \geq R_b - R_e = \tilde{R}_{cs}, \tag{37}$$
where $\tilde{R}_{cs}$ can be defined as
$$\tilde{R}_{cs} = \log_2\left(1 + \frac{P_a \rho_0 |\mathbf{g}_{ab}\mathbf{u}|^2}{d_{ab}^{\alpha}\sigma_b^2}\right) - \log_2\left(1 + \frac{P_a \rho_0 |\mathbf{g}_{aw}\mathbf{u}|^2 / d_{aw}^{\alpha}}{\rho_0 |\mathbf{g}_{jw}\mathbf{v}|^2 P_j / d_{aw}^{\alpha} + \sigma_w^2}\right). \tag{38}$$
Thus, maximize R_{cs} is equivalent to maximize $\tilde{R}_{cs}$. Then, We analyze the monotonicity of $\tilde{R}_{cs}$ with respect to P_a and P_j to derive the optimal transmit and jamming power.

The first-order derivative of $\tilde{R}_{cs}$ with respect to P_a and P_j can be demonstrated respectively as
$$\tilde{R}'_{cs}(P_a) = \frac{||\mathbf{h}_{ab}||^2(|\mathbf{h}_{jw}\mathbf{v}|^2 P_j + \sigma_w^2) - |\mathbf{h}_{aw}\mathbf{u}|^2 \sigma_b^2}{\ln 2\,(P_a||\mathbf{h}_{ab}||^2 + \sigma_b^2)(|\mathbf{h}_{aw}\mathbf{u}|^2 P_a + |\mathbf{h}_{jw}\mathbf{v}|^2 P_j + \sigma_w^2)}, \tag{39}$$
$$\tilde{R}'_{cs}(P_j) = \frac{\left(|\mathbf{h}_{jw}\mathbf{v}|^2 P_j + \sigma_w^2\right) |\mathbf{h}_{aw}\mathbf{u}|^2 |\mathbf{h}_{jw}\mathbf{v}|^2 P_a}{\ln 2 (P_a||\mathbf{h}_{ab}||^2 + \sigma_b^2)(|\mathbf{h}_{aw}\mathbf{u}|^2 P_a + |\mathbf{h}_{jw}\mathbf{v}|^2 P_j + \sigma_w^2)^2}. \tag{40}$$
From (39), we can see that $\tilde{R}_{cs}$ monotonically increases with P_a. To achieve larger $\tilde{R}_{cs}$, P_a needs to be set to its maximum. However, P_a is still constrained by (24b), (24c), (24d), and (24e). From (40), we can see that $\tilde{R}_{cs}$ monotonically increases with P_j. A larger $\tilde{R}_{cs}$ can be achieved by setting P_j to its maximum, where P_j is constrained by (24b), (24c), and (24f).

To meet the constraints (24d) and (24e), the transmit power P_a needs to satisfy
$$\frac{(2^r - 1)\sigma_b^2}{||\mathbf{h}_{ab}||^2} \leq P_a \leq P_{amax}. \tag{41}$$

To comply the constraints (24c) and (24f), the jamming power P_j needs to satisfy
$$\frac{|\mathbf{h}_{aw}\mathbf{u}|^2 P_a - (2^{r_e} - 1)\sigma_w^2}{(2^{r_e} - 1)|\mathbf{h}_{jw}\mathbf{v}|^2} \leq P_j \leq P_{jmax}. \tag{42}$$
From (42), we can further conclude the constraints for P_a as
$$P_a \leq \frac{P_j(2^{r_e} - 1)|\mathbf{h}_{jw}\mathbf{v}|^2 + (2^{r_e} - 1)\sigma_w^2}{|\mathbf{h}_{aw}\mathbf{u}|^2} = P_a^{URe}. \tag{43}$$

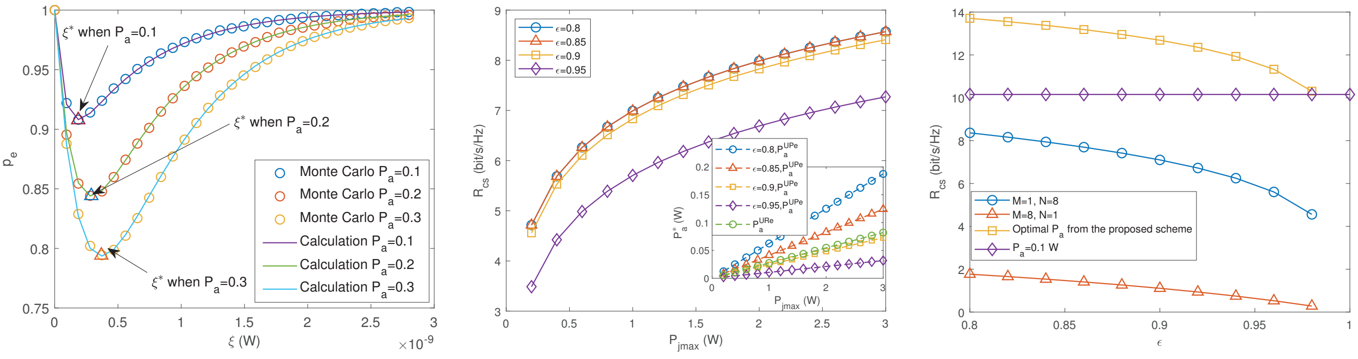
In addition, according to the constraint (24b) and the corresponding conclusion in Proposition 1, we can further conclude
$$P_a \leq \frac{d_{aw}^{\alpha}|\mathbf{g}_{jw}\mathbf{v}|^2}{d_{jw}^{\alpha}} \frac{\mathscr{W}_0\left((1-\epsilon)\ln(1-\epsilon)\right)}{\ln(1-\epsilon)} P_j = P_a^{Upe}. \tag{44}$$

Overall, we can set P_j as its maximum and P_a satisfy constraints of (43) and (44) to obtain the optimal transmit power P_a^* and jamming power P_j^* as
$$\begin{cases} P_j^* = P_{jmax}, \\ P_a^* = \min\{P_a^{URe}, P_a^{Upe}\}. \end{cases} \tag{45}$$

Therefore, the maximum R_{cs} can be achieved by setting P_a and P_j according to (45).

V. Simulation

In this section, simulation results are presented and discussed to evaluate the effectiveness of our proposed covert communication scheme. We assume that Alice, Bob, Willie, and the jammer are located at $L_a = (0, 0, 0)$, $L_b = (200, 0, 0)$, $L_w = (200, 100, 0)$, and $L_j = (200, 100, 130)$ in meters, respectively. The large-scale path loss exponent is set to $\alpha = 2.6$, and the reference power gain at the distance of 1 m is set to $\rho_0 = -30$ dB [1], [11]. Without loss of generality, we set the AWGN variance received at Bob and Willie as $\sigma_b^2 = \sigma_w^2 = -120$ dBm, since both Bob and Willie are on the ground.



(a)

(b)

(c)

Fig. 2. (a) Error detection probability versus power detection threshold at Willie; (b) Achievable covert secrecy rate versus maximum allowed jamming power; (c) Achievable covert secrecy rate versus error detection probability limit in different schemes.

In Fig. 2(a), the impact of power detection threshold ξ on the error detection probability p_e is investigated under different transmit power P_a. The transmit and jamming antennas are set to $M = 8$ and $N = 8$, respectively. $P_{jmax} = 1$ W. From the results, we can see that the Monte Carlo simulation results match our theoretical calculation results as shown in (18). In addition, we can also see that p_e first decreases then increases with ξ, which indicates there exists the optimal power detection threshold to minimize p_e. The results also show that the ξ^* derived from (20) corresponds to the simulation results and leads to the minimum p_e, which agrees with Proposition 1. We can further see from the results that the error detection probability p_e decreases as P_a increases. This is because larger transmit power leads to a higher risk of being detected. Therefore, Alice can reduce her transmit power for better covertness.

Fig. 2(b) demonstrate the influence of the maximum allowed jamming power P_{jmax} on the achievable secrecy rate R_{cs} under different error detection probability limits ϵ. The transmit power at Alice and jamming power are set according to (45). The transmit and jamming antennas are set to $M = 8$ and $N = 8$, respectively. From the results, we can see that R_{cs} increases as P_{jmax} gets larger. This is because the transmit power P_a^* increases as P_{jmax} rises, and thus results in a larger R_{cs}. Additionally, it also indicates that R_{cs} decreases with ϵ, however, $\epsilon = 0.8$ and $\epsilon = 0.85$ result to the same R_{cs}. This is because when $\epsilon = 0.8$ and $\epsilon = 0.85$ we have $P_a^{URe} < P_a^{Upe}$, therefore, P_a^* in both cases are set to P_a^{URe}.

The effectiveness of our proposed covert scheme is compared in Fig. 2(c) with No MRT, no zero-forcing, and fixed transmit power of $P_a = 0.1$ W scheme. In our proposed scheme, the transmit and jamming antennas are set to $M = 8$ and $N = 8$, respectively. $P_{jmax} = 1$ W. From the results, we can see that the covert secrecy rate R_{cs} decreases with the error detection probability limit ϵ. This is because a larger ϵ requirement leads to stricter covert constraint, and thus the allowed transmit power P_a gets smaller. We can further observe from the results that our proposed scheme is much more effective in covertness compared with other schemes, which is more obvious when there is no zero-forcing applied. This is because the jamming signal inevitably reduces the transmission rate when there is no zero-forcing adopted.

VI. Conclusion

In this paper, we proposed a more secure UAV-assisted covert communication scheme, where a multi-antenna MRT transmitter transmits covertly against a warden assisted by a multi-antenna zero-forcing UAV jammer, to achieve a higher covert secrecy rate while guaranteeing the covertness. The security and performance can be improved with more antennas applied. In addition, this scheme also guarantees the security when the transmission is correctly detected by the warden. Under the worst case of the warden's optimal detection, we jointly optimized the transmit and jamming power to maximize the covert secrecy rate in both detected and undetected situations while guaranteeing the error detection probability and eavesdropping rate both under their limits. Simulation results prove the correctness and effectiveness of our proposed covert scheme. In our future work, we will focus on adapting our scheme to a more complex multi-receiver scenario with the location uncertainty of the warden considered.

References

[1] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K.-K. Wong, "IRS-assisted secure UAV transmission via joint trajectory and beamforming design," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1140–1152, Feb. 2022.

[2] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert communications: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173–1198, 2nd Quart. 2023.

[3] X. Chen, N. Zhao, Z. Chang, T. Hämäläinen, and X. Wang, "UAV-aided secure short-packet data collection and transmission," *IEEE Trans. Commun.*, vol. 71, no. 4, pp. 2475–2486, Apr. 2023.

[4] X. Chen, F. Gao, M. Qiu, J. Zhang, F. Shu, and S. Yan, "Achieving covert communication with a probabilistic jamming strategy," *IEEE Trans. Info. Forensics. Security*, vol. 19, pp. 5561–5574, May 2024.

[5] Y. Bai, H. Zhao, X. Zhang, Z. Chang, R. Jäntti, and K. Yang, "Toward autonomous multi-UAV wireless network: A survey of reinforcement learning-based approaches," *IEEE Commun Surveys Tuts.*, vol. 25, no. 4, pp. 3038–3067, 4th quart. 2023.

[6] X. Yu, D. Li, Z. Wang, and S. Sun, "An integrated new deep learning framework for reliable CSI acquisition in connected and autonomous vehicles," *IEEE Network*, vol. 37, no. 4, pp. 216–222, Jul./Aug. 2023.

[7] Z. Chen, S. Yan, X. Zhou, F. Shu, and D. W. K. Ng, "Intelligent reflecting surface-assisted passive covert wireless detection," *IEEE Trans. Vehi. Tech.*, vol. 73, no. 2, pp. 2954–2959, Feb. 2024.

[8] X. Chen, Z. Chang, N. Zhao, and T. Hämäläinen, "IRS-based secure UAV-assisted transmission with location and phase shifting optimization," in *Proc. IEEE ICC Workshops'23*, pp. 1672–1677, Rome, Italy, 2023.

[9] L. Lv, Z. Li, H. Ding, N. Al-Dhahir, and J. Chen, "Achieving covert wireless communication with a multi-antenna relay," *IEEE Trans. Info. Forensics Security*, vol. 17, pp. 760–773, Feb. 2022.

[10] Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, and M.-S. Alouini, "Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5574–5587, Aug. 2019.

[11] Y. Zeng, X. Xu, and R. Zhang, "Trajectory design for completion time minimization in UAV-enabled multicasting," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2233–2246, Apr. 2018.

V

ACHIEVING IMPROVED SECURITY IN UAV-ASSISTED COVERT COMMUNICATION NETWORKS

by

Xinying Chen, Zheng Chang, and Timo Hämäläinen 2024

2024 IEEE/CIC International Conference on Communications in China
(ICCC Workshops), pp. 323–328,
https://doi.org/10.1109/ICCCWorkshops62562.2024.10693776

Achieving Improved Security in UAV-Assisted Covert Communication Networks

Xinying Chen[II], Zheng Chang[II,†], and Timo Hämäläinen[II]
[II]Faculty of Information Technology, University of Jyväskylä, P. O. Box 35, FIN-40014 Jyväskylä, Finland.
[†]School of Computer Science and Engineering, University of Electronic Science
and Technology of China, 611731, Chengdu, China.

***Abstract*—Covert communication can hide confidential signals in environmental noise to avoid being detected and provide comprehensive security for wireless transmission. However, there still exists significant risks in the wireless transmission once being detected. In this paper, we propose a more secure covert scheme, where a multiple antennas transmitter assisted by a multi-antenna UAV jammer maximizes the covert secrecy rate under the scenarios of both correct and incorrect detection by a warden with both error detection probability and eavesdropping rate limitations satisfied. The transmitter and jammer adopt maximum ratio transmission (MRT) and zero-forcing to maximize the transmission rate and minimize the interference at the receiver, respectively. First, we analyze the monotonicity of error detection probability to determine the optimal power detection threshold and the corresponding largest error detection probability. Then, under this worst case, we jointly optimize the transmit and jamming power to maximize the covert secrecy rate while guaranteeing the covert and eavesdropping limits meet their respective requirements. Finally, simulation results are presented to prove the correctness of the theoretical conclusion and evaluate the effectiveness of our proposed scheme.**

***Index Terms*—Covert communication, Gaussian signaling, secure transmission, UAV, zero-forcing.**

I. Introduction

Wireless communication has brought tremendous convenience and enabled fast connections to everyone [1]. However, the characteristic of broadcasting in wireless networks also posts confidential messages under the risk of leakage [2]. Therefore, secure transmission becomes more and more important, especially when the messages contain personal data or sensitive information [3]. There are two methods of achieving security in wireless communications, i.e., physical layer security (PLS) and covert communications [4]. PLS attains secure transmission by utilizing the randomness of wireless channels combined with precoding and signal processing, which aims to reduce the eavesdropping rate. In [5], Chen *et al.* investigated the secure transmission of an UAV data collection network, where the trajectory, the user slot schedule, and the flight duration are jointly optimized to achieve a higher energy efficiency. Then, the authors adjust the transmit power and the blocklength to maximize the secrecy rate after the data collection phase. However, PLS can be exposed to higher risk of being eavesdropped as the wireless techniques develop. Different from PLS, covert communications provide concealment via hiding confidential signals in environmental noise, where the warden will not decode the signals without detection, and thus lead to transmission security. Chen *et al.* designed the strategies of covert communication under three perspectives in [6], i.e., the standpoint of Alice, the jammer, and the global system, where they derived the minimum jamming power to maintain the covertness and proved the effectiveness of the proposed probabilistic jamming strategy. Nevertheless, the covert communication cannot provide secure transmission once the transmission behavior is correctly detected .

The unmanned aerial vehicle (UAV), widely exploited in wireless communications, has plenty of advantages, e.g., fast deployment, light volume, and high mobility, among which it can also leverage the air-to-ground line-of-sight (LoS) channels [7]. Channel randomness has been exploited to offer secure transmission in PLS and covert networks, which also brings the difficulties of obtaining channel state information (CSI). In one respect, the difficulty of acquiring CSI makes it hard for malicious users to eavesdrop; in another respect, it is also difficult to obtain CSI for legitimate users while utilizing channel uncertainty. In [8], Yu *et al.* proposed a new framework where two deep learning models are adopted to obtain the performance degradation resulting from CSI acquisition. They also trained the proposed deep learning model by continual learning to improve the adaptability. The LoS channels benefited from employing the UAV, enable legitimate users to obtain CSI within the networks. Chen *et al.* optimized the transmit power and the IRS phase shifting matrix to maximize the covert transmission performance in [9] while guaranteeing the error detection probability no less than its constraint, where the LoS channels are considered and thus simplify the CSI acquisition for IRS. However, the LoS channels, on the contrary, increase the risk of information leakage.

In addition, benefiting from the utilization of channel multiplexing, multi-antenna technique has been broadly exploited in PLS and covert communications to achieve better transmission performance [10]. The multiple antennas can be used to realize maximum ratio transmission (MRT), where the precoding vector is designed according to the CSI to achieve a maximum signal-to-interference ratio (SINR). In [11], Lv *et al.* studied covert communication under random and MRT beamforming schemes, where the transmit power allocation is optimized to achieve the maximum covert rate in a multi-antenna relay network. Multiple antennas can also be employed to realize zero-forcing, which can minimize the undesired interference at specific users. Cao *et al.* analyzed the secrecy performance of a cooperative non-orthogonal multiple access network aided by a multi-antenna full-duplex

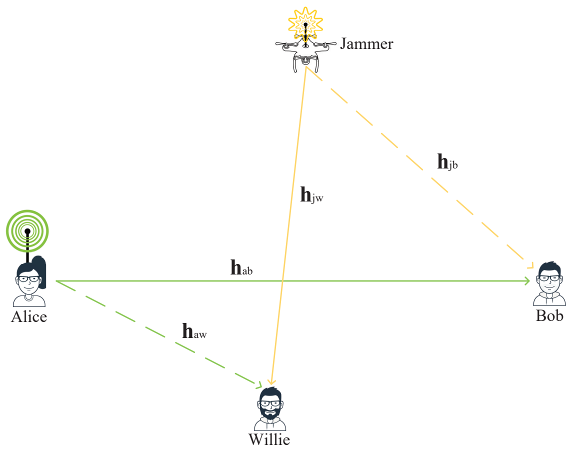


Fig. 1. System model of a zero-forcing UAV jammer-assisted covert communication network.

relay in [12], where the jamming signal is zero-forced at the legitimate user via relay beamforming to eliminate the undesired interference.

Different from most of the existing research work on covert communications, which only focuses on improve the performance during miss detection phase, this paper inspects covert networks aiming to provide comprehensive, secure protection for both correct and incorrect detection phases. We jointly optimize the transmit and jamming power to maximize the covert secrecy rate while avoiding being detected and eavesdropped. First, the optimal power detection threshold and the corresponding minimized error detection probability at the warden are derived. Then, the transmit and jamming power are optimized to guarantee that both the optimal error detection probability and the eavesdropping rate are within the limits.

II. System Model

We consider a covert communication system where Alice transmits to Bob confidentially with the assistance of a UAV jammer to avoid being detected by Willie, as shown in Fig. 1. The locations of Alice, the jammer, Bob, and Willie are $L_a(x_a, y_a, 0)$, $L_j(x_j, y_j, H)$, $L_b(x_b, y_b, 0)$, $L_w(x_w, y_w, 0)$, respectively, where H is the fixed hovering altitude of drone jammer. Assume that Alice is equipped with M antennas, the jammer is equipped with N antennas, while both Bob and Willie are equipped with single receiving antennas. The channel coefficients from Alice to Bob $\mathbf{h}_{ab} \in \mathbb{C}^{1\times M}$ and Willie $\mathbf{h}_{aw} \in \mathbb{C}^{1\times M}$ are assumed to follow a large scale path-loss and a small scale Rayleigh fading, which can be described as

$$\mathbf{h}_{ab} = \sqrt{\frac{\rho_0}{d_{ab}^{-\alpha}}}\mathbf{g}_{ab}, \tag{1}$$

and

$$\mathbf{h}_{aw} = \sqrt{\frac{\rho_0}{d_{aw}^{-\alpha}}}\mathbf{g}_{aw}, \tag{2}$$

where $d_{ab} = ||L_a - L_b||$ and $d_{aw} = ||L_a - L_w||$ are the distances from Alice to Bob and Willie, respectively. ρ_0 is the reference power gain at 1 m and α denotes the large-scale path-loss exponent. In addition, each Rayleigh fading component $g_{a_i b}$ or $g_{a_i w}$, $\forall i \in \{1, \cdots, M\}$, in both $\mathbf{g}_{ab}$ and $\mathbf{g}_{aw}$ is independent and identically distributed (i.i.d), which follows complex Gaussian distribution with zero mean and unit variance, i.e., $g_{a_i b} \sim \mathcal{CN}(0,1)$ and $g_{a_i w} \sim \mathcal{CN}(0,1)$.

The air-to-ground channels from the jammer to Bob $\mathbf{h}_{jb} \in \mathbb{C}^{1\times N}$ and to Willie $\mathbf{h}_{jw} \in \mathbb{C}^{1\times N}$ are assumed to be LoS channels. They can be denoted as

$$\mathbf{h}_{jb} = \sqrt{\frac{\rho_0}{d_{jb}^{-\alpha}}}\mathbf{g}_{jb}, \tag{3}$$

and

$$\mathbf{h}_{jw} = \sqrt{\frac{\rho_0}{d_{jw}^{-\alpha}}}\mathbf{g}_{jw}, \tag{4}$$

where $d_{jb} = ||L_j - L_b||$ and $d_{jw} = ||L_j - L_w||$ are the distances from the jammer to Bob and to Willie, respectively. $\forall i \in \{1, \cdots, N\}$, $g_{j_i b} \in \mathbf{g}_{jb}$ and $g_{j_i w} \in \mathbf{g}_{jw}$, and we have $|g_{j_i b}| = |g_{j_i w}| = 1$.

In order to achieve higher uncertainty and avoid being detected by Willie, Alice selects a time slot with a probability of $\pi = 0.5$ to transmit baseband signal $x[k]$ to Bob, where the transmit power is P_a. Suppose the CSI among legitimate users is known to each other. Alice adopts MRT towards Bob to achieve better performance, where the precoding vector $\mathbf{u} \in \mathbb{C}^{M\times 1}$ at Alice can be defined as

$$\mathbf{u} = \frac{\mathbf{g}_{ab}^H}{||\mathbf{g}_{ab}||}. \tag{5}$$

On the other hand, the jammer constantly emits jamming signals to assist Alice in avoiding being detected by Willie. In order to introduce uncertainty at Willie, the jammer applies Gaussian signaling $\mathbb{J}x_j[k] \sim \mathcal{CN}(0, P_j)$. With the CSI $\mathbf{g}_{jb}$ obtainable at the jammer, it can employ zero-forcing precoding towards Bob, where the precoding vector $\mathbf{v} \in \mathbb{C}^{N\times 1}$can be defined as

$$\begin{cases} \mathbf{g}_{jb}\mathbf{v} = 0, \\ ||\mathbf{v}||^2 = 1. \end{cases} \tag{6}$$

Therefore, the received signals at Bob in each time slot can be denoted as

$$y_b[k] = \sqrt{P_a}\mathbf{h}_{ab}\mathbf{u}x[k] + n_b[k], \tag{7}$$

where $n_b[k]$ is the additive white Gaussian noise (AWGN) received at Bob, and it follows complex Gaussian distribution, i.e., $n_b[k] \sim \mathcal{CN}(0, \sigma_b^2)$. Correspondingly, the transmission rate R_b at Bob can be expressed as

$$R_b = \log_2\left(1 + \frac{P_a\rho_0|\mathbf{g}_{ab}\mathbf{u}|^2}{d_{ab}^{\alpha}\sigma_b^2}\right). \tag{8}$$

Since the zero-forcing is designed towards only Bob, Willie receives signals from both Alice and the jammer, which can be denoted as

$$y_w[k] = \sqrt{P_a}\mathbf{h}_{aw}\mathbf{u}x[k] + \mathbb{J}\mathbf{h}_{jw}\mathbf{v}x_j[k] + n_w[k], \tag{9}$$

where $n_w[k]$ is the i.i.d AGWN received at Willie in each time slot and follows $n_w[k] \sim \mathcal{CN}(0,\sigma_w^2)$. The corresponding eavesdropping rate R_e at Willie can be calculated as

$$R_e = \log_2\left(1+\frac{P_a\rho_0|\mathbf{g}_{aw}\mathbf{u}|^2/d_{aw}^{\alpha}}{\rho_0|\mathbf{g}_{jw}\mathbf{v}|^2 P_j/d_{aw}^{\alpha}+\sigma_b^2}\right). \tag{10}$$

III. The Optimal Detection of Willie

Willie needs to decide whether Alice is transmitting $\mathcal{H}_1$ or silent $\mathcal{H}_0$ according to his received signal power, and then decide whether to decode the received signals. The received signals of the two cases mentioned above can be denoted as

$$y_w[k]=\begin{cases}\mathbb{J}\mathbf{h}_{jw}\mathbf{v}x_j[k]+n_w[k], & \mathcal{H}_0,\\ \sqrt{P_a}\mathbf{h}_{aw}\mathbf{u}x[k]+\mathbb{J}\mathbf{h}_{jw}\mathbf{v}x_j[k]+n_w[k], & \mathcal{H}_1.\end{cases} \tag{11}$$

Willie measures his received samples N times and derives the averaged received signal power P_w to compare with his preset power detection threshold ξ, and then makes his decision. The decision rule can be described as

$$P_w = \frac{1}{N}\sum_{k=1}^{N}|y_w[k]|^2 \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \xi, \tag{12}$$

where N is the sample numbers. Willie decides that Alice is transmitting $\mathcal{D}_1$ when P_w is larger than ξ, and Alice keeps silent $\mathcal{D}_0$ when P_w is smaller than ξ.

We consider the interference limit network, i.e., σ_b^2 and σ_w^2 can be ignored in Willie's detection. As the signal samples get larger, i.e.$N \to \infty$, the averaged received power P_w can be rewritten as

$$P_w = \begin{cases} J, & \mathcal{H}_0,\\ S+J, & \mathcal{H}_1,\end{cases} \tag{13}$$

where J and S represent the jamming and signal power, respectively. They can be summarized as

$$J = |\mathbb{J}x_j[k]|^2|\mathbf{h}_{jw}\mathbf{v}|^2, \tag{14}$$

and

$$S = P_a|\mathbf{h}_{aw}\mathbf{u}|^2. \tag{15}$$

According to the decision rule in (12), there are two types of mistakes that Willie may make, which are the false alarm (FA) and the miss detection (MD). The FA mistake indicates that Willie believes that Alice is transmitting while she is silent. MD indicates that Willie believes that Alice is silent while she is transmitting. The error detection probability p_e is defined as the probability that Willie makes FA and MD mistakes, which can be described as

$$\begin{aligned} p_e &= \mathbb{P}_{FA}+\mathbb{P}_{MD} = \mathbb{P}(\mathcal{D}_1|\mathcal{H}_0)+\mathbb{P}(\mathcal{D}_0|\mathcal{H}_1)\\ &= \mathbb{P}(J \geq \xi)+\mathbb{P}(J+S \leq \xi).\end{aligned} \tag{16}$$

On the other hand, the correct detection probability of Willie can be expressed as

$$\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1) = \mathbb{P}(J+S \geq \xi). \tag{17}$$

Based on the distribution of jamming signals $\mathbb{J}x_j[k] \sim \mathcal{CN}(0,P_j)$, we can conclude

$$J \sim \exp(\frac{d_{jw}^{\alpha}}{P_j\rho_0|\mathbf{g}_{jw}\mathbf{v}|^2}). \tag{18}$$

Denote $\lambda_j = \frac{d_{jw}^{\alpha}}{P_j\rho_0|\mathbf{g}_{jw}\mathbf{v}|^2}$.

As for $\mathbf{g}_{aw} \sim \mathcal{CN}(0,\mathbf{I})$ and $\mathbf{g}_{ab} \sim \mathcal{CN}(0,\mathbf{I})$ are i.i.d and follow the same distribution, we can conclude that $|\mathbf{h}_{aw}\mathbf{u}|^2 \sim \exp(1)$. This further leads to

$$S \sim \exp(\frac{d_{aw}^{\alpha}}{P_a\rho_0}). \tag{19}$$

Denote $\lambda_s = \frac{d_{aw}^{\alpha}}{P_a\rho_0}$.

Correspondingly, p_e in (16) can be changed into

$$\begin{aligned} p_e &= 1-\mathbb{F}_J(\xi)+\mathbb{F}_{J+S}(\xi)\\ &= e^{-\lambda_j\xi}+\int_0^{\xi}\mathbb{F}_J\left(\xi-x\right)f_S\left(x\right)dx\\ &= 1-\frac{\lambda_j}{\lambda_s-\lambda_j}\left(e^{-\lambda_j\xi}-e^{-\lambda_s\xi}\right).\end{aligned} \tag{20}$$

Similarly, the correct detection probability $\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1)$ in (17) can be altered to

$$\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1) = \frac{1}{\lambda_s-\lambda_j}\left(\lambda_s e^{-\lambda_j\xi}-\lambda_j e^{-\lambda_s\xi}\right). \tag{21}$$

From the definition of λ_j, λ_s, and the expression of p_e in (20), we can see that p_e is related to ξ. Willie can achieve a lower p_e by properly choosing his power detection threshold. The optimal ξ to minimize Willie's error detection probability p_e is derived in Proposition 1.

Proposition 1: The optimal power detection threshold at Willie can be expressed as

$$\xi^* = \frac{\ln\lambda_s-\ln\lambda_j}{\lambda_s-\lambda_j}, \tag{22}$$

and the corresponding minimized error detection probability p_e^* can be derived as

$$p_e^* = 1-\left(\frac{\lambda_s}{\lambda_j}\right)^{-\frac{\lambda_s}{\lambda_s-\lambda_j}}. \tag{23}$$

Proof. The impact of ξ on p_e can be obtained by analyzing the monotonicity of p_e. The first-order derivative of p_e with respect to ξ can be derived as

$$p_e'(\xi) = -\frac{\lambda_j}{\lambda_s-\lambda_j}\left(-\lambda_j e^{-\lambda_j\xi}+\lambda_s e^{-\lambda_s\xi}\right). \tag{24}$$

The zeros of $p_e'(\xi)$ in (24) can be derived as

$$\xi_0 = \frac{\ln\lambda_s-\ln\lambda_j}{\lambda_s-\lambda_j}. \tag{25}$$

Based on the definition of λ_s and λ_j, we can have $\lambda_s > 0$ and $\lambda_j > 0$. We discuss the monotonicity of p_e with respect to ξ under two cases, i.e., $\lambda_s > \lambda_j$ and $\lambda_s < \lambda_j$ to derive the optimal ξ.

- $\lambda_s > \lambda_j$: In this case, we can conclude that $p_e'(\xi) > 0$ when $\xi > \frac{\ln\lambda_s-\ln\lambda_j}{\lambda_s-\lambda_j}$, and $p_e'(\xi) < 0$ when $\xi < \frac{\ln\lambda_s-\ln\lambda_j}{\lambda_s-\lambda_j}$. This indicates that p_e monotonically decreases with ξ when $\xi < \frac{\ln\lambda_s-\ln\lambda_j}{\lambda_s-\lambda_j}$, and monotonically increases when $\xi > \frac{\ln\lambda_s-\ln\lambda_j}{\lambda_s-\lambda_j}$. p_e obtains the minimum at ξ_0.

- $\lambda_s < \lambda_j$: We can also have $p_e'(\xi) > 0$ when $\xi > \frac{\ln\lambda_s - \ln\lambda_j}{\lambda_s - \lambda_j}$, and $p_e'(\xi) < 0$ when $\xi < \frac{\ln\lambda_s - \ln\lambda_j}{\lambda_s - \lambda_j}$. This also indicates that p_e monotonically decreases when $\xi < \frac{\ln\lambda_s - \ln\lambda_j}{\lambda_s - \lambda_j}$, and increases when $\xi > \frac{\ln\lambda_s - \ln\lambda_j}{\lambda_s - \lambda_j}$. p_e reaches its minimum at ξ_0 as well.

Both cases lead to the same optimal detection threshold ξ^* as shown in (22). Based on (20), the corresponding p_e^* is presented in (23). □

With the optimal power detection threshold ξ^* in (22), the correct detection probability in (21) can be expressed as

$$\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1)^* = \left(\frac{\lambda_s}{\lambda_j}\right)^{-\frac{\lambda_s}{\lambda_s - \lambda_j}} + \left(\frac{\lambda_s}{\lambda_j}\right)^{-\frac{\lambda_j}{\lambda_s - \lambda_j}}. \tag{26}$$

IV. Transmit and Jamming Power Optimization for a More Secure Covert Communication

A. Problem Formulation

We aim to provide a more secure transmission for covert communication between Alice and Bob against Willie. In this section, we jointly optimize transmit and jamming power to maximize the covert secrecy rate while guaranteeing Willie's optimal error detection probability larger than the threshold and the eavesdropping rate lower than the limit. The optimization problem can be summarized as

$$\begin{aligned}
\textbf{P1:}\ \max_{P_a, P_j}\ & R_{cs} && \text{(27a)}\\
s.t.\ \ & p_e^* \geq \epsilon, && \text{(27b)}\\
& R_e \leq r_e, && \text{(27c)}\\
& R_b \geq r, && \text{(27d)}\\
& P_a \leq P_{amax}, && \text{(27e)}\\
& P_j \leq P_{jmax}, && \text{(27f)}
\end{aligned}$$

where ϵ is the lower limit of Willie's error detection probability, r_e represents the upper limit of Willie's eavesdropping rate, r is the lower threshold of transmission rate, P_{amax} and P_{jmax} are the maximum allowed transmit and jamming power, respectively. In addition, the covert secrecy rate R_{cs} is defined as the secrecy rate in covert communication when Alice is transmitting. It includes two cases of Willie deciding that Alice is silent $\mathcal{D}_0$ and Alice is transmitting $\mathcal{D}_1$, when Alice is transmitting $\mathcal{H}_1$. Willie does not decode Alice's signals when he believes Alice is silent. R_{cs} can be denoted as

$$\begin{aligned}
R_{cs} &= R_b\mathbb{P}(\mathcal{D}_0|\mathcal{H}_1) + (R_b - R_e)\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1)\\
&= R_b - \mathbb{P}(\mathcal{D}_1|\mathcal{H}_1)R_e.
\end{aligned} \tag{28}$$

B. Impact of Constraint ϵ on P_a and P_j

According to Proposition 1, Willie can obtain his minimum error detection probability p_e^* by setting the power detection threshold as (22). To guarantee that p_e^* satisfies the constraint, the requirement of P_a and P_j is shown in Proposition 2.

Proposition 2: To guarantee (27b), the transmit and jamming power should satisfy

$$\frac{P_a}{P_j} \leq \frac{d_{aw}^{\alpha}|\mathbf{g}_{jw}\mathbf{v}|^2}{d_{jw}^{\alpha}} \frac{\mathscr{W}_0\left((1-\epsilon)\ln(1-\epsilon)\right)}{\ln(1-\epsilon)}. \tag{29}$$

Proof. With the expression of p_e^* in (23) and in order to satisfy the constraint in (27b), we can have

$$\left(\frac{\lambda_s}{\lambda_j}\right)^{-\frac{\frac{\lambda_s}{\lambda_j}}{\frac{\lambda_s}{\lambda_j}-1}} \leq 1 - \epsilon. \tag{30}$$

Let $t = \frac{\lambda_s}{\lambda_j}$, and we have $t > 0$. Then, (30) can be altered to

$$\frac{t}{t-1}\ln\frac{1}{t} \leq \ln(1-\epsilon). \tag{31}$$

To further obtain the limitation of P_a and P_j, we need to discuss t by classifying $t > 1$ and $0 < t < 1$.

- Case $t > 1$:
  With $t \in (1, \infty)$, (31) can be changed into

$$\begin{aligned}
\ln\frac{1}{t} &\leq \frac{t-1}{t}\ln(1-\epsilon)\\
\frac{1}{t} &\leq e^{-\frac{\ln(1-\epsilon)}{t}} e^{\ln(1-\epsilon)}.
\end{aligned} \tag{32}$$

  Owing to $\ln(1-\epsilon) < 0$, (32) can be changed into

$$\ln(1-\epsilon)e^{\ln(1-\epsilon)} \leq \frac{\ln(1-\epsilon)}{t} e^{\frac{\ln(1-\epsilon)}{t}} < 0, \tag{33}$$

  which satisfies the form of the Lambert W function. Therefore, we can have

$$\frac{\ln(1-\epsilon)}{t} \leq \mathscr{W}_{-1}(\ln(1-\epsilon)e^{\ln(1-\epsilon)}), \tag{34}$$

  or

$$\mathscr{W}_0(\ln(1-\epsilon)e^{\ln(1-\epsilon)}) \leq \frac{\ln(1-\epsilon)}{t} < 0, \tag{35}$$

  where $\mathscr{W}_0(*)$ is the principle branch of Lambert W function, and $\mathscr{W}_{-1}(*)$ represents the negative branch. Practically, the error detection threshold ϵ is close to 1. Therefore, from (34) we can have

$$0 < \frac{\lambda_s}{\lambda_j} \leq \frac{\ln(1-\epsilon)}{\mathscr{W}_{-1}\left((1-\epsilon)\ln(1-\epsilon)\right)} = 1, \tag{36}$$

  which is against the initial assumption of $t > 1$.
  From (35), we can have

$$\frac{\lambda_s}{\lambda_j} \geq \frac{\ln(1-\epsilon)}{\mathscr{W}_0\left((1-\epsilon)\ln(1-\epsilon)\right)}. \tag{37}$$

  Then, we can further derive the upper limit of P_a/P_j as shown in (29).
- Case $0 < t < 1$:
  Similarly, when $t \in (0, 1)$, (31) can be changed into

$$\begin{aligned}
\ln\frac{1}{t} &\geq \left(1 - \frac{1}{t}\right)\ln(1-\epsilon)\\
\frac{1}{t} &\geq e^{-\frac{\ln(1-\epsilon)}{t}} e^{\ln(1-\epsilon)}\\
\frac{\ln(1-\epsilon)}{t} e^{\frac{\ln(1-\epsilon)}{t}} &\leq \ln(1-\epsilon)e^{\ln(1-\epsilon)}.
\end{aligned} \tag{38}$$

  According to Lambert W function, the solution to (38)

$$\tilde{R}_{cs} = \log_2\left(1+\frac{P_a\rho_0|\mathbf{g}_{ab}\mathbf{u}|^2}{d_{ab}^{\alpha}\sigma_b^2}\right) - \log_2\left(1+\frac{P_a\rho_0|\mathbf{g}_{aw}\mathbf{u}|^2/d_{aw}^{\alpha}}{\rho_0|\mathbf{g}_{jw}\mathbf{v}|^2P_j/d_{aw}^{\alpha}+\sigma_b^2}\right). \tag{41}$$

$$\tilde{R}'_{cs}(P_a) = \frac{1}{\ln 2}\left(\frac{||\mathbf{h}_{ab}||^2\left(|\mathbf{h}_{aw}\mathbf{u}|^2P_a+|\mathbf{h}_{jw}\mathbf{v}|^2P_j+\sigma_w^2\right)-|\mathbf{h}_{aw}\mathbf{u}|^2\left(P_a||\mathbf{h}_{ab}||^2+\sigma_b^2\right)}{\left(P_a||\mathbf{h}_{ab}||^2+\sigma_b^2\right)\left(|\mathbf{h}_{aw}\mathbf{u}|^2P_a+|\mathbf{h}_{jw}\mathbf{v}|^2P_j+\sigma_w^2\right)}\right) > 0. \tag{42}$$

$$\tilde{R}'_{cs}(P_j) = \frac{1}{\ln 2}\left(\frac{\left(|\mathbf{h}_{jw}\mathbf{v}|^2P_j+\sigma_w^2\right)|\mathbf{h}_{aw}\mathbf{u}|^2|\mathbf{h}_{jw}\mathbf{v}|^2P_a}{\left(P_a||\mathbf{h}_{ab}||^2+\sigma_b^2\right)\left(|\mathbf{h}_{aw}\mathbf{u}|^2P_a+|\mathbf{h}_{jw}\mathbf{v}|^2P_j+\sigma_w^2\right)^2}\right) > 0. \tag{43}$$

can be derived as

$$\frac{\ln(1-\epsilon)}{\mathscr{W}_{-1}((1-\epsilon)\ln(1-\epsilon))} \leq \frac{\lambda_s}{\lambda_j} \leq \frac{\ln(1-\epsilon)}{\mathscr{W}_0((1-\epsilon)\ln(1-\epsilon))}. \tag{39}$$

Owing to $\frac{\ln(1-\epsilon)}{\mathscr{W}_{-1}((1-\epsilon)\ln(1-\epsilon))} = 1$, (39) is against the assumption of $t \in (0,1)$.

Thus, the overall constraint of P_a/P_j is demonstrated in (29). □

C. Optimize P_a and P_j to Maximize R_{cs}

To maximize the covert secrecy rate R_{cs}, the transmit power P_a and jamming power P_j need to be adjusted properly while satisfying constraints in (27). The objective function (27a) is non-convex and mathematically difficult to solve. Based on the expression of $\mathbb{P}(\mathcal{D}_1|\mathcal{H}_1)^*$ in (26) and R_{cs} in (28), we can further conclude

$$R_{cs} \geq R_b - R_e = \tilde{R}_{cs}, \tag{40}$$

where $\tilde{R}_{cs}$ can be defined as (41) on the top of this page.

Thus, maximize R_{cs} is equivalent to maximize $\tilde{R}_{cs}$. Then, We analyze the monotonicity of $\tilde{R}_{cs}$ with respect to P_a and P_j to derive the optimal transmit and jamming power.

The first-order derivative of $\tilde{R}_{cs}$ with respect to P_a and P_j can be demonstrated as (42) and (43) on the top of this page, respectively.

From (42), we can see that $\tilde{R}_{cs}$ monotonically increases with P_a. To achieve higher $\tilde{R}_{cs}$, P_a needs to be set to its maximum. However, P_a is still constrained by (27b), (27c), (27d), and (27e). From (43), we can see that $\tilde{R}_{cs}$ monotonically increases with P_j. A larger $\tilde{R}_{cs}$ can be achieved by setting P_j to its maximum, where P_j is constrained by (27b), (27c), and (27f).

To meet the constraints (27d) and (27e), the transmit power P_a needs to satisfy

$$\frac{(2^r-1)\sigma_b^2}{||\mathbf{h}_{ab}||^2} \leq P_a \leq P_{amax}. \tag{44}$$

To comply the constraints (27c) and (27f), the jamming power P_j needs to satisfy

$$\frac{|\mathbf{h}_{aw}\mathbf{u}|^2P_a-(2^{r_e}-1)\sigma_w^2}{(2^{r_e}-1)|\mathbf{h}_{jw}\mathbf{v}|^2} \leq P_j \leq P_{jmax}. \tag{45}$$

From (45), we can further conclude the constraints for P_a as

$$P_a \leq \frac{P_j(2^{r_e}-1)|\mathbf{h}_{jw}\mathbf{v}|^2+(2^{r_e}-1)\sigma_w^2}{|\mathbf{h}_{aw}\mathbf{u}|^2} = P_a^{URe}. \tag{46}$$

In addition, according to the constraint (27b) and the corresponding conclusion in Proposition 1, we can further conclude

$$P_a \leq \frac{d_{aw}^{\alpha}|\mathbf{g}_{jw}\mathbf{v}|^2}{d_{jw}^{\alpha}}\frac{\mathscr{W}_0\left((1-\epsilon)\ln(1-\epsilon)\right)}{\ln(1-\epsilon)}P_j = P_a^{Upe}. \tag{47}$$

Overall, we can set P_j as its maximum and P_a satisfy constraints in (46) and (47) to obtain the optimal transmit power P_a^* and jamming power P_j^* as

$$\begin{cases} P_j^* = P_{jmax}, \\ P_a^* = \min\{P_a^{URe}, P_a^{Upe}\}. \end{cases} \tag{48}$$

Therefore, the maximum R_{cs} can be achieved by setting P_a and P_j according to (48).

V. Simulation

In this section, simulation results are presented and discussed to evaluated the effectiveness of our proposed covert communication scheme. We assume that Alice, Bob, Willie, and the jammer are located at $L_a = (0,0,0)$, $L_b = (200,0,0)$, $L_w = (200,100,0)$, and $L_j = (200,100,130)$ in meters, respectively. The large-scale path-loss exponent is set to $\alpha = 2.6$, and the reference power gain at the distance of 1 m is set to $\rho_0 = -30$ dB. Without loss of generality, we set the AWGN variance received at Bob and Willie as $\sigma_b^2 = \sigma_w^2 = -120$ dBm, since both Bob and Willie are on the ground. In addition, the jamming signal variance is set to $P_j = 1$ W.

In Fig. 2, the impact of power detection threshold ξ on the error detection probability p_e is investigated under different transmit power P_a. The transmit and jamming antennas are set to $M = 8$ and $N = 8$, respectively. From the results, we can see that the Monte Carlo simulation results match our theoretical calculation results as shown in (20). In addition, we can also see that p_e first decreases then increases with ξ, which indicates there exists the optimal power detection threshold to minimize p_e. The results also show that the ξ^* derived from (22) corresponds to the simulation results and leads to the minimum p_e, which agrees Proposition 1. We can

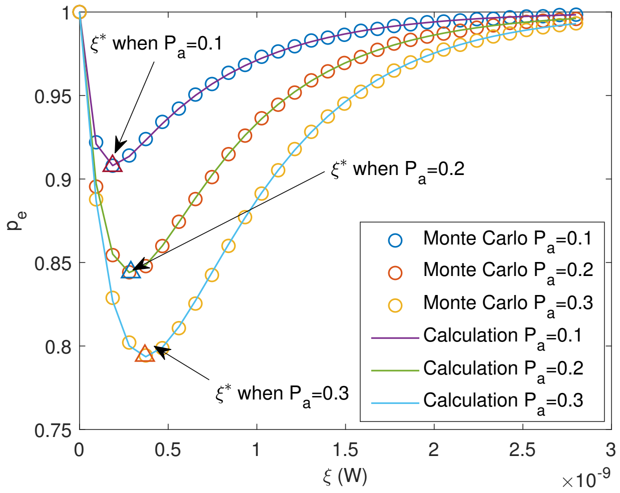


Fig. 2. Comparison of the error detection probability p_e under different power detection threshold ξ for the simulation and the calculation results. Three cases of transmit power $P_a = 0.1$ W, $P_a = 0.2$ W, $P_a = 0.3$ W are considered.

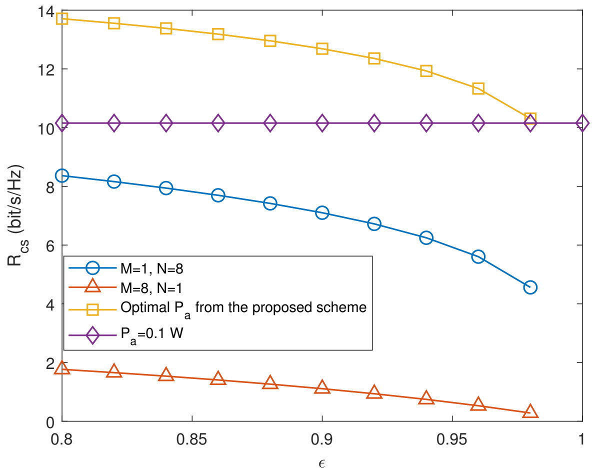


Fig. 3. Comparision of the achievable covert secrecy rate R_{cs} under different error detection probability limit among our proposed scheme, no MRT scheme , no zero-forcing scheme, and fixed transmit power scheme.

also see from the result that the error detection probability p_e decreases as P_a increases. This is because higher transmit power leads to higher risk of being detected. Therefore, Alice can reduce her transmit power for better stealthy.

The effectiveness of our proposed covert scheme is compared with other schemes in Fig. 3. The impact of error detection probability lower limit ϵ on the covert secrecy rate R_{cs} is examined over our proposed scheme, without MRT, without zero-forcing, and fixed transmit power of $P_a = 0.1$ W. In our propose scheme, the transmit and jamming antennas are set to $M = 8$ and $N = 8$, respectively. From the results, we can see that the covert secrecy rate R_{cs} decreases with the lower error detection probability limit ϵ. This is because higher ϵ requirement leads to stricter covert constraint, and thus the allowed transmit power P_a gets smaller. We can further observe from the results that our proposed scheme is much more effective in covertness compared with other schemes, which is more obvious when there is no zero-forcing applied. This is because the jamming signal inevitably reduces the transmission rate when there is no zero-forcing adopted.

VI. Conclusion

In this paper, we proposed a more secure UAV-assisted covert communication scheme. The covert communication, where a multi-antenna MRT transmitter transmits covertly against a warden assisted by a multi-antenna zero-forcing UAV jammer, is assured to achieve a higher covert secrecy rate while guaranteeing the error detection probability is larger than the limit. In addition, this scheme also guarantees the security when the transmission is correctly detected by the warden. The optimal power detection threshold and the corresponding minimum error detection probability are discussed and demonstrated. Under the worst case of the warden's optimal detection, we jointly optimized the transmit and jamming power to maximize the covert secrecy rate in both detected and undetected situations while guaranteeing the error detection probability and eavesdropping rate both under their limits. Simulation results are presented to evaluate the correctness and effectiveness of our proposed covert scheme.

References

[1] J. Zhao, F. Huang, L. Liao, and Q. Zhang, "Blockchain-based trust management model for vehicular Ad Hoc networks," *IEEE Internet Things J.*, vol. 11, no. 5, pp. 8118–8132, Sept. 2024.

[2] J. Zhao, H. Hu, F. Huang, Y. Guo, and L. Liao, "Authentication technology in internet of things and privacy security issues in typical application scenarios," *Electronics*, vol. 12, no. 8, p. 1812, 2023.

[3] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K.-K. Wong, "IRS-assisted secure UAV transmission via joint trajectory and beamforming design," *IEEE Trans. Commun.*, vol. 70, no. 2, pp. 1140–1152, Feb. 2022.

[4] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert communications: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173–1198, 2nd Quart. 2023.

[5] X. Chen, N. Zhao, Z. Chang, T. Hämäläinen, and X. Wang, "UAV-aided secure short-packet data collection and transmission," *IEEE Trans. Commun.*, vol. 71, no. 4, pp. 2475–2486, Apr. 2023.

[6] X. Chen, F. Gao, M. Qiu, J. Zhang, F. Shu, and S. Yan, "Achieving covert communication with a probabilistic jamming strategy," *IEEE Trans. Info. Forensics. Security*, vol. 19, pp. 5561–5574, May 2024.

[7] Y. Bai, H. Zhao, X. Zhang, Z. Chang, R. Jäntti, and K. Yang, "Toward autonomous multi-UAV wireless network: A survey of reinforcement learning-based approaches," *IEEE Commun Surveys Tuts.*, vol. 25, no. 4, pp. 3038–3067, 4th quart. 2023.

[8] X. Yu, D. Li, Z. Wang, and S. Sun, "An integrated new deep learning framework for reliable CSI acquisition in connected and autonomous vehicles," *IEEE Network*, vol. 37, no. 4, pp. 216–222, Jul./Aug. 2023.

[9] Z. Chen, S. Yan, X. Zhou, F. Shu, and D. W. K. Ng, "Intelligent reflecting surface-assisted passive covert wireless detection," *IEEE Trans. Vehi. Tech.*, vol. 73, no. 2, pp. 2954–2959, Feb. 2024.

[10] X. Chen, Z. Chang, N. Zhao, and T. Hämäläinen, "IRS-based secure UAV-assisted transmission with location and phase shifting optimization," in *Proc. IEEE ICC Workshops'23*, pp. 1672–1677, Rome, Italy, 2023.

[11] L. Lv, Z. Li, H. Ding, N. Al-Dhahir, and J. Chen, "Achieving covert wireless communication with a multi-antenna relay," *IEEE Trans. Info. Forensics Security*, vol. 17, pp. 760–773, Feb. 2022.

[12] Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, and M.-S. Alouini, "Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5574–5587, Aug. 2019.