碩士學位論文

위장 전이중 은닉 통신에서의 탐지 오류 확률 최대화

Detection Error Probability Maximization for Disguised Full-Duplex Covert Communications

國立한밭大學校 소프트웨어융합大學院

모바일융합工學科

Refat Khan

2024년 08월

위장 전이중 은닉 통신에서의 탐지 오류 확률 최대화

Detection Error Probability Maximization for Disguised Full-Duplex Covert Communications

指導敎授 문 지 환

이 論文을 工學碩士學位
請求論文으로 제출함

2024년 05월

國立한밭大學校 소프트웨어융합大學院

모바일융합工學科

Refat Khan

Refat Khan의 碩士學位 論文을 認准함

審査委員長 ________________________(인)

審 査 委 員 ________________________(인)

審 査 委 員 ________________________(인)

2024년 06월

國立한밭大學校 소프트웨어융합大學院

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ADC	**A**nalog-to-**D**igital **C**onverter
AQNM	**A**dditive **Q**uantization **N**oise **M**odel
AP	**A**ccess **P**oint
BUG	**B**eamforming **U**ncertainty **U**nit
MIMO	

Abstract

Detection Error Probability Maximization for Disguised Full-Duplex Covert Communications

Refat Khan

Advisor: Jihwan Moon

Covert communications have arisen as an effective communications security measure that overcomes some of the limitations of cryptography and physical layer security. The main objective is to completely conceal from external devices the very existence of the link

for exchanging confidential messages. In this paper, we take a step further and consider a scenario in which a covert communications node disguises itself as another functional entity for even more covertness. To be specific, we study a system where a source node communicates with a seemingly receive-only destination node which, in fact, is full-duplex (FD) and covertly delivers critical messages to another hidden receiver while evading the surveillance. Our aim is to identify the achievable covert rate at the hidden receiver by optimizing the public data rate and the transmit power of the FD destination node subject to the worst-case detection error probability (DEP) of the warden. Closed-form solutions are provided, and we investigate the effects of various system parameters on the covert rate through numerical results, one of which reveals that applying more (less) destination transmit power achieves a higher covert rate when the source transmit power is low (high). Since our work provides a performance guideline from the information-theoretic point of view, we conclude this paper with a discussion on possible future research such as analyses with practical modulations and imperfect channel state information.

Chapter 1

Introduction

Wireless technology has transformed numerous facets of human existence, including connectivity, healthcare, education, and economic systems, reshaping the very fabric of daily life [1][2]. The foundational studies in traditional cryptography and physical layer security hold profound importance in fortifying information security against unauthorized interception, paving the way for advancements in safeguarding sensitive data [3][4]. Even though cryptography and physical layer security can keep your messages safe from eavesdroppers, your communication habits might still pose privacy risks. The way we communicate can sometimes lead to privacy worries. For instance, if a commander's position is exposed because of electromagnetic signals on the battlefield, it could have serious consequences [5]. A suitable solution for such scenarios involves covert or low-probability-of-detection communications, which conceal the presence of crucial communication links [6]. Covert communication is designed to allow two users to communicate while ensuring there's very little chance that a warden will detect this communication. It works by hiding the fact that any transmission is happening, which helps reduce the risk of the transmitter or the communication itself being discovered in wireless networks [7][8][9]. Extensive research has also been conducted on covert communications within full duplex systems. Let's imagine a situation where there's someone sending secret messages (Alice) to another person who can both send and receive messages at the same time (Bob). But there's a third person (Willie) keeping an eye on them, trying to figure out if Alice and Bob are talking to each other or not. In this setup, Alice, and Willie each have one antenna. On the other hand, Bob has a receiver antenna and an extra antenna for transmitting a signal, which we'll call AN. This additional signal aims to confuse Willie and create uncertainty for him [10]. The paper investigates covert communication using a full-duplex receiver under limited channel information and demonstrates that random noise improves performance. By optimizing transmit and AN power to minimize outage probability at Bob, Authors observe a non-linear relationship between AN power and performance. Additionally, simulations reveal differences in performance behavior between channel distribution information (CDI) and channel state information (CSI) scenarios [11]. In previous research, [12] explored receiver antenna selection, while [13] proposed a strategy for transmission time selection and power control, utilizing channel state information (CSI). This paper examines a two-way wiretap channel with a multi-antenna Eve, employing artificial noise (AN) and deriving a secrecy rate approximation. Simulations indicate that optimized power allocation minimizes Eve's rates while maximizing the sum rates [14]. In the studied paper, a constrained multi objective optimization problem (MOP) is formulated to maximize two conflicting objectives: the transmission rate between legitimate transceivers and the average covert probability (ACP) for eavesdroppers. This optimization involves adjusting transmit power and the position of the full-duplex (FD) receiver, such as in UAV relay networks. Constraints encompass conditions necessary for achieving covert communication and establishing no-deployed-zones (NDZ) [15]. Research on delay-constrained covert communications with fixed artificial noise (AN) power was explored in [16], while joint optimization problems for AN power and receiver position were discussed in [17,18]. Consideration of uncertain warden node locations was addressed in [19]. Additionally, [18] studied random covert channel selection by the transmitter to further confuse the warden, and [20] identified the maximum detection error probability (DEP) under the age of information constraint. As for more complex FD systems, covert communications performance in different relay systems: decode-and-forward (DF), compress-and-forward (CF), and amplify-and-forward (AF). By optimizing power distribution between public and covert messages, considering minimum detection error probability (DEP) at the relay, it achieves maximum covert rate. The study compares DF, CF, and AF systems, accounting for system parameters like processing delay, quality of service, and DEP threshold, revealing performance variations under different conditions [21]. In [22], authors devised a protocol for energy harvesting full-duplex decode-and-forward (DF) relay-based covert communications. This protocol allows the relay to both forward and harvest energy simultaneously. Furthermore, [23] investigated full-duplex relay-aided covert communications from a satellite to a ground node in the context of integrated satellite–terrestrial communications. Recently, the research community has given significant attention to the IRS communication paradigm [24][25][26]. References [27] and [28] presuppose that the presence of the covert device is acknowledged by the warden. Reference [29] examines an IRS communication scenario where a covert user possesses full control over the IRS and remains concealed from the warden. In [30] the authors Analyz that covert user is unknown to the warden and the covert user does not have control over the IRS. In [31], optimization of a transmit beamforming vector and reflecting coefficients is conducted for intelligent reflecting surface (IRS)-aided covert communications, where an FD receiver emits random artificial noise (AN) to confuse the warden. Additionally, [32] explores uplink covert communications assisted by an IRS. [33] discusses the utilization of an active IRS, inherently full duplex, for covert communications between user pairs. Finally, [34] focuses on minimizing the age of information in a scenario where a receiver covertly transmits confidential messages to the transmitter, protected under public transmissions from the transmitter to the receiver facilitated. The paper centers on a covert communication setup utilizing UAVs equipped with full-duplex receivers. It delves into optimizing the system's location design leveraging physical layer security technology [34]. A novel scheme is proposed via a UAV carrying an IRS to establish air-ground links to assist covert transmission, where the phase shifts of IRS are randomized to preserve the covertness. Additionally, the legitimate receiver can act as a jammer in the full-duplex mode to defuse the detection of a warden [35].[36] employed to help the transmission and confuse the warden. The maximum lowest average covert rate was achieved in the case of an FD unmanned aerial vehicle (UAV) collecting data from a scheduled user and interfering with unscheduled users using artificial noise (AN) [37]. In [30], the authors explored an FD decode-and-forward (DF) UAV relay to facilitate covert communications, where multiple sensors transmit messages to a remote base station in separate time slots [38]. At present, some literature investigates covert communication in CR networks. Chen et al. [39] have analyzed user scheduling performance in covert CR Networks. In [40], the authors have addressed the problem of power allocation with the aid of generative adversarial network in covert CR networks. The authors of [41] have considered covert communication by exploiting cognitive jammers. In this work, a covert jamming scheme is designed to counter an intelligent eavesdropper, enhancing physical layer security within cooperative cognitive radio networks. Investigated [43] in this letter is a power allocation dilemma within a cooperative cognitive covert communication system. Here, the relay secondary transmitter (ST) discretely transmits confidential data under the guidance of the primary transmitter (PT). Optimization of both secrecy and covert rates was performed in [44] where an untrusted full-duplex (FD) amplify-and-forward (AF) relay transmits the covert message to an FD base station. The base station then emits artificial noise (AN) to deceive the warden. In the IoT domain, [45] investigated a covert transmitter with optimized transmission probability, powered wirelessly by artificial noise (AN) from an FD receiver. Moreover, [46] optimized covert uplink transmissions of devices to FD IoT gateways using a mean-field Stackelberg game approach. Additionally, [47] utilized an ambient backscatter system, where a radio frequency tag modulates an ambient signal into a covert signal for an FD receiver concurrently broadcasting AN.

1.1 Background

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

1.2 Contributions

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

Chapter 2

System Model

This chapter gives the…. Fig. 2.1 shows that….

2.1 Received Signals

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

2.2 Hihihihi

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

Chapter 3

Problem Formulation

This chapter gives the….

3.1 Problem?

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

3.2 Hihihihi

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

Chapter 4

Proposed Solutions

This chapter gives the….

4.1 Received Signals

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

4.2 Hihihihi

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

Chapter 5

Numerical Results

This chapter gives the….

5.1 System Setups

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

5.2 DEP versus blahblah

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

Chapter 6

Conclusion

This chapter gives the….

6.1 Conclusion

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

6.2 Future Work

Wireless technology has revolutionized the way people live in various ways. However, behind the proliferation of wireless communications are cyberattacks that leave users open to information leakage \cite{JZhang:22}. To cope with this, cryptography has widely been adopted, which encrypts and decrypts data using secret keys \cite{BAForouzan:07}. Nevertheless, this approach has certain limitations, e.g., high complexity for generating secret keys and vulnerability to eavesdroppers with stronger computational power, which are particularly unfavorable for the Internet of Things (IoT) devices. These downsides have led researchers to examine the possibility of utilizing physical layer security \cite{ADWyner:75}. Its main characteristic is that a wireless link from legitimate entities to eavesdroppers can be effectively obstructed, either by nullifying beamforming with multiple antennas, or by disruption with artificial noise (AN) \cite{PAngueira:22}. Hence, the dependency on secret key agreements and the need of avoiding high-powered adversaries can be greatly alleviated.

Bibliography

[1] Y. Jeon, S.-H. Park, C. Song, J. Moon, S. Maeng, and I. Lee, "Joint Designs of Fronthaul Compression and Precoding for Full-duplex Cloud Radio Access Networks," IEEE Wireless Communications Letters, Vol. 5, No. 6, pp. 632 - 635, Dec. 2016.

[2] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy Performance Optimization for Wireless Powered Communication Networks With an Energy Harvesting Jammer," IEEE Transactions on Communications, Vol. 65, No. 2, pp. 764 - 774, Feb. 2017.

[3]

[4]

[5]

[6]

[7]

[8]

[9]

[10]

[11]

Abstract

Detection Error Probability Maximization for Disguised Full-Duplex Covert Communications

Refat Khan

Advisor: Jihwan Moon

Covert communications have arisen as an effective communications security measure that overcomes some of the limitations of cryptography and physical layer security. The main objective is to completely conceal from external devices the very existence of the link for exchanging confidential messages. In this paper, we take a step further and consider a scenario in which a covert communications node disguises itself as another functional entity for even more covertness. To be specific, we study a system where a source node communicates with a seemingly receive-only destination node which, in fact, is full-duplex (FD) and covertly delivers critical messages to another hidden receiver while evading the surveillance. Our aim is to identify the achievable covert rate at the hidden receiver by optimizing the public data rate and the transmit power of the FD destination node subject to the worst-case detection error probability (DEP) of the warden. Closed-form solutions are provided, and we investigate the

effects of various system parameters on the covert rate through numerical results, one of which reveals that applying more (less) destination transmit power achieves a higher covert rate when the source transmit power is low (high). Since our work provides a performance guideline from the information-theoretic point of view, we conclude this paper with a discussion on possible future research such as analyses with practical modulations and imperfect channel state information.