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** | **i** |
| **List of Tables** | **ii** |
| **List of Abbreviations** | **iii** |
| **Abstract** | **iv** |
| **1. Introduction** | **1** |
| 1.1. Background?? | 3 |
| 1.2. Contributions?? | 4 |
| **2. System Model** | **50** |
| 2.1. Received hihi | 60 |
| 2.2. bybye | 111 |
| **3. Problem Formulation** | **222** |
| 3.1. hihi | 11 |
| 3.2. efawef | 3 |
| **4. Proposed Solutions** | **24** |
| 4.1. abcd | 33 |
| 4.2. abcd | 2 |
| **5. Numerical Results** | **1** |
| 5.1. dddd | 2 |
| 5.2. eeee | 3 |
| **6. Conclusion** | **123** |
| 6.1. Conclusion | 2 |
| 6.2. Future Work | 1 |
| **Bibliography** | **231** |
| **Abstract** | **3** |

**List of Figures**

|  |  |  |
| --- | --- | --- |
| 1.1 | Schematic diagram | 1 |
| 1.2 | Covert rate versus DEP | 2 |
| 1.3 | DEP versus hihi | 33 |
| 2.1 | DEP versus hihi | 444 |
| 2.2 | DEP versus hihi | 555 |
| 2.3 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**List of Tables**

|  |  |  |
| --- | --- | --- |
| 1.1 | Schematic diagram | 1 |
| 1.2 | Covert rate versus DEP | 2 |
| 1.3 | DEP versus hihi | 33 |
| 2.1 | DEP versus hihi | 444 |
| 2.2 | DEP versus hihi | 555 |
| 2.3 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**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. Many previous studies have presumed that surveillance nodes possess complete knowledge about the hardware specifications of covert nodes. However, covert nodes have the potential to enhance their concealment by masquerading as different functional entities. For example, an initial full-duplex (FD) node transmitting sensitive messages covertly might masquerade as a receiver-only half-duplex (HD) node. To the author's knowledge, there is a scarcity of research on covert communications that incorporates such deceptive strategies.

This study explores a covert communication setup involving a source node and a disguised full-duplex (FD) destination node. Despite appearing as receive-only, this destination node clandestinely transmits vital messages to a concealed receiver using an imperceptible additional antenna, all while minimizing detection by a warden node. We identify the optimal public data rate and the transmit power of the FD destination node that maximizes the worst-DEP at the warden node. We offer analytical solutions and explore how different system parameters affect the minimum DEP using numerical evaluation.

**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**

The primary contributions of our research can be outlined as follows:

1. Unlike previous studies assuming the surveillance party's knowledge of covert node hardware specifications, we advance by exploring a practical scenario where a covert communication node assumes the guise of a different functional entity to enhance its stealth further.

2. The worst-case detection error probability (DEP) is calculated considering the uncertainty of noise at the warden node.

3. Observing that covert communications often experience a limited data rate due to strict requirements on detection error probability.

4. Our focus lies in improving the minimum detection error probability at the warden node by optimizing both the public data rate and transmit power of the FD destination node. Additionally, we prioritize maintaining a minimum covert rate within the system.

5. We explore the impact of diverse system parameters on the worst-case detection error probability (DEP) using numerical analysis.

6. Given that our study offers insights from an information-theoretic standpoint, we propose exploring practical modulation techniques and the implications of imperfect channel state information (CSI) as promising avenues for future research.

**Chapter 2**

**System Model**

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

**Hidden Receiver**, R

A black background with a black square

Description automatically generated with medium confidence

Covert message

A blue lock with a blue keyhole

Description automatically generated with medium confidence

A person and a paper

Description automatically generated

A black and white logo

Description automatically generated A black tower with waves

Description automatically generated

**Self-interference**

Public message

**Source**, S

**Disguised FD destination**, D

A black background with a black square

Description automatically generated with medium confidence

**Warden**, W

**2.1 Received Signals**

Figure 1 depicts the system model we're considering. In this model, there's a source node called S that sends a message to a destination node called D. While this happens, the destination node, which appears to only receive messages, actually secretly sends another message to a hidden receiver node called R using a hidden extra antenna. This covert transmission happens in a full-duplex manner, meaning the destination node can send and receive messages simultaneously. All of this occurs while a warden node, W, is monitoring for any unexpected communications.

First, let's express the received signal at the disguised full-duplex (FD) destination node.

In this system model, the channel coefficient h XY represents communication links between different nodes, such as the source (S), destination(D) , hidden receiver(R), or warden(W). The residual self-interference channel accounts for leftover signals after cancelling self-interference. Public messages and covert messages are transmitted with mean 0 and variance 1. Transmit powers and are set by the source and destination nodes, respectively. Additive noise is present at each node. The destination node can estimate the source channel while the hidden receiver can estimate and if provided with pilot sequences. The warden is assumed to have perfect knowledge of certain channel information for worst-case scenario analysis. The source adopts its data rate based on destination feedback, and the achieved data rate at the destination is denoted according to reference [37].

Next, the hidden receiver receives two types of messages: a public message directly from the source node and a covert message from the destination node.

As a result, the hidden receiver must first decode and remove public messages before accessing covert messages. Consequently, the achievable public data rate, denoted as at the hidden receiver.

The resulting achievable covert rate after removing from can also be calculated as

**2.2 Covert message Detection**

Simultaneously, the warden node intercepts the communications.

It first eliminates public messages from to calculate the effective residual signal , assuming it perfectly knows and [38]. We can consider the following two hypotheses:

In the null hypothesis , we assume that there are no covert messages, while in the alternative hypothesis we presume that the source node did not transmit a covert message.

In this study, a radiometer [39] is utilized as a detection method at the warden. The test statistic T for equation (7), After observing many signals simplifies to the average residual power as [40]

The warden node determines the presence of a covert transmission based on whether the test statistic T surpassed or falls below a predefined threshold .

Specifically, if T is greater than or equal to , the warden node concludes that a covert transmission exists; otherwise, if T is less than , no covert transmission is deemed to be present. This threshold is chosen to balance the trade-off between false positive and false negative in the detection process.

The uncertainty in the noise variance at the warden node is considered, following the approach outlined in the references [39] and [41].

Specifically, we model the noise variance in decibels as where , represents the mean and denotes the bounded range, both of which are non-negative. Subsequently, we derive detection error probability (DEP) , encompassing both false alarm and miss probabilities.

In this scenario, the warden node assumes that the covert transmission occurs randomly, with equal probabilities for both null hypothesis and the alternative hypothesis each set 0.5 [42]. By leveranging the cumulative distribution function (CDF) of (provided in Appendix A). We can further analyz the system performance

,

The false alarm and miss probability are specifically written by.

respectively.

Where and

We encounter two distinct scenarios contingent upon the magnitude of and

If

Where

On the other hand,

With .

The warden node may aim for a specific threshold value that helps minimize the detection error probability (DEP). To achieve this, we observe that equation and decreases monotonically from to as ranges within set , and increases monotonically from to as ranges within set Additionally, the first derivative of the sum is calculated as

The first derivative is consistently positive when belongs to set . Thus, the optimal threshold for the warden node in both equations and is established by the dividing the line between sets and or between and as

It is important to point out that equation presents the wors-case scenario for minimum DEP, assuming that the warden node has precise knowledge of the actual value of

**Chapter 3**

**Problem Formulation**

In this study, we seek to pinpoint the ideal public data rate and transmission power at the full-duplex destination node that will increase the minimum error probability at the warden node as much as possible as

Constraint ensures that the hidden receiver can successfully decode and remove the public message before decoding the covert message. Constraint specifics the maximum achievable public data rate, allowing the destination node to inform the source node for adjustment. In , a minimum quality of services for public transmission is considered. specifies a minimum threshold for the covert data rate, denoted , which represents the lowest acceptable rate for the covert transmission and ensures non-zero DEP. Finally, constraint outlines the power budget, denoted as , for the disguised full-duplex destination node.

**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 solution to fulfill our objective that is to maximize the worst-case detection error probability (DEP) in . This requires careful consideration of the relationship between various parameters.

First, it is important to note that DEP decreases as the transmit power increases. Similarly, the upper limits of the public data rate and also decrease as increases.

However, the covert rate in increases with an increase Therefore, in order to maximize the worst-case DEP, we should aim to minimize which, unfortunately, leads to a decrease in the covert rate.

Given these trade-offs, the goal is to find an optimal value of that both maintains a minimum covert data rate and maximizes the worst-case DEP. This requires a delicate balance between the different parameters to achieve the best possible outcome.

Therefore, the optimal transmit power can be obtained by taking the minimum of lower bound of and minimum of to and we can write optimal

,,

**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**

We assess the proposed methodologies for maximizing the worst-case detection error probability (DEP) with the disguised full-duplex (FD) node through numerical analysis. The forthcoming figures will investigate the impacts of different system parameters, including source transmit power, disguised FD destination transmit power budget, noise uncertainty bound, and minimum quality of service , along with the derived optimal destination transmit power as indicated in equation (20).

We adopt a distance-dependent channel model for ,where Here, represent the path loss between nodes and . In this equation denotes the path loss at a reference distance signifies the path loss exponent, and indicates the distance between nodes and . Additionally, the small-scale channel variable follows a complex normal distribution . The four nodes are positioned at certain distance form the origin in a cartesian coordinate system, with coordinates for and denoted as and respectively (refer to figure 2). The overall system parameters are predefined as follows, unless stated otherwise: BandwidthSource transmit power destination transmit power budget = 23dBm, Public message quality of service mean noise power at the warden node noise uncertainty bound , noise power at the destination node and hidden receiver residual self-interference minimum DEP threshold , and path loss exponent

**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] V. Chamola, V. Hassija, V. Gupta and M. Guizani, "A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact," in IEEE Access, vol. 8, pp. 90225-90265, 2020, doi: 10.1109/ACCESS.2020.2992341. |  |
| [4] S. Revathi, A. Shrivastava, A. Yussupova, A. N. Hidayatulloh, D. Saltanat and A. Mishra, "Role of Wireless Communications in Digital Economy in the Present Context," 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2022, pp. 703-709, doi: 10.1109/ICOEI53556.2022.9777115. |  |
| [5] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, "Artificial-noise-aided secure transmission in wiretap channels with transmitterside correlation," IEEE Trans. Commun., vol. 15, no. 12, pp. 8286--8297, Dec.2016 |  |
| [6] H. Wang, B. Zhao, and T. Zheng, ''Adaptive fullduplex jamming receiver for secure D2D links in random networks;' IEEE Trans. Commun., vol. 67, no. 2, pp. 1254-1267, Feb. 2019 |  |
| [7] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goecke1, "Covert communication in the presence of an uninformed jammer;' IEEE Trans. Wirel. Commun., vol. 16, no. 9, pp. 6193- 6206, Sep. 2017 |  |
| [8] Bash, B.A.; Goeckel, D.; Towsley, D.; Guha, S. Hiding information in noise: Fundamental limits of covert wireless communication.  *IEEE Commun. Mag.* **2015**, *53*, 26–31 |  |
| [9] J. Hu et al., “Covert communication achieved by a greedy relay in wireless networks,” IEEE Trans. Wireless Commun., vol. 17, no. 7, pp. 4766–4779, Jul. 2018 |  |
| [10] Hu, Jinsong & Shahzad, Khurram & Yan, Shihao & Zhou, Xiangyun & Shu, Feng & Li, Jun. (2017). Covert Communications with A Full-Duplex Receiver over Wireless Fading Channels. |  |
| [11] Z. Liu, J. Liu, Y. Zeng, J. Ma and Q. Huang, "On Covert Communication with Interference Uncertainty," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1-6, doi: 10.1109/ICC.2018.8422940.  [12] F. Shu, T. Xu, J. Hu and S. Yan, "Delay-Constrained Covert Communications With a Full-Duplex Receiver," in IEEE Wireless Communications Letters, vol. 8, no. 3, pp. 813-816, June 2019, doi: 10.1109/LWC.2019.2894617  [13] T. Xu, L. Xu, X. Liu and Z. Lu, "Covert Communication with A Full-Duplex Receiver Based on Channel Distribution Information," 2018 12th International Symposium on Antennas, Propagation and EM Theory (ISAPE), Hangzhou, China, 2018, pp. 1-4, doi: 10.1109/ISAPE.2018.8634312.  [14] L. Yang, W. Yang, S. Xu, L. Tang and Z. He, "Achieving Covert Wireless Communications Using a Full-Duplex Multi-Antenna Receiver," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 912-916, doi: 10.1109/ICCC47050.2019.9064154.  [15] J. Wang, Y. Li, W. Tang, X. Li and S. Li, "Channel State Information Based Optimal Strategy for Covert Communication," 2019 11th International Conference on Wireless Communications and Signal Processing (WCSP), Xi'an, China, 2019, pp. 1-6, doi: 10.1109/WCSP.2019.8928142.  [16] N. Garg and T. Ratnarajah, "Power Allocation For Full-duplex Two-way Wiretap Channel," 2022 IEEE 23rd International Workshop on Signal Processing Advances in Wireless Communication (SPAWC), Oulu, Finland, 2022, pp. 1-5, doi: 10.1109/SPAWC51304.2022.9833919  [17] Y. Zhao, Z. Li, N. Cheng, D. Wang, W. Quan and X. Shen, "Joint Power and Position Optimization for the Full-Duplex Receiver in Covert Communication," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148663  [18] Shu, Feng & Xu, Tingzhen & Hu, Jinsong & Yan, Shihao. (2019). Delay-Constrained Covert Communications with A Full-Duplex Receiver. IEEE Wireless Communications Letters. PP. 1-1. 10.1109/LWC.2019.2894617.  [19] Xu, Rui & Guan, Lei & Zhao, Yue & Li, Zan & Wang, Danyang. (2021). Robust Power and Position Optimization for the Full-Duplex Receiver in Covert Communication. 1-6. 10.1109/GLOBECOM46510.2021.9685606.  [20] Y. Zhao, Z. Li, N. Cheng, D. Wang, W. Quan and X. Shen, "Joint Power and Position Optimization for the Full-Duplex Receiver in Covert Communication," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 2020, pp. 1-6, doi: 10.1109/ICC40277.2020.9148663  [21] Chen, X.; Sun, W.; Xing, C.; Zhao, N.; Chen, Y.; Yu, F.R.; Nallanathan, A. Multi-Antenna Covert Communication via Full-Duplex  Jamming Against a Warden With Uncertain Locations. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 5467–5480.  [22] Che, Bohan & Yang, Weiwei & Lu, Xingbo. (2021). Covert Communication for Multi-Channel Transmission with A Full-Duplex Receiver. 1-5. 10.1109/WCSP52459.2021.9613571.  [23] Moon, J. Performance Comparison of Relay-Based Covert Communications: DF, CF and AF. Sensors **2023**, 23, 8747. https://doi.org/10.3390/s23218747  [24] Li, Y.; Zhao, R.; Deng, Y.; Shu, F.; Nie, Z.; Aghvami, A.H. Harvest-and-Opportunistically-Relay: Analyses on Transmission Outage  and Covertness. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 7779–7795. [CrossRef]  [25] Wu, Z.; Guo, K.; Zhu, S. Covert Communication for Integrated Satellite–Terrestrial Relay Networks with Cooperative Jamming. Electronics **2023**, 12,999. <https://doi.org/10.3390/electronics12040999>  [26] E. Bjornson and L. Sanguinetti, “Power scaling laws and near-field behaviors of massive MIMO and intelligent reflecting surfaces,” IEEE Open J. Commun. Soc., vol. 1, pp. 1306–1324, 2020  [27] S. Zhang and R. Zhang, “Capacity characterization for intelligent reflecting surface aided MIMO communication,” IEEE J. Sel. Areas Commun., vol. 38, no. 8, pp. 1823–1838, Aug. 2020.  [28] W. Tang et al., “Wireless communications with reconfigurable intelligent surface: Path loss modeling and experimental measurement,” IEEE Trans. Wireless Commun., vol. 20, no. 1, pp. 421– 439, Jan. 2021.  [29] C. Wu et al., “Intelligent reflecting surface (IRS)- aided covert communication with warden’s statistical CSI,” IEEE Wireless Commun. Lett., vol. 10, no. 7, pp. 1449–1453, Jul. 2021  [30] J. Si, Z. Li, J. Cheng, L. Guan, J. Shi, and N. AlDhahir, “Covert transmission assisted by intelligent reflecting surface,” IEEE Trans. Commun., vol. 69, no. 8, pp. 5394–5408, Aug. 2021.  [31] C. Wang, Z. Li, J. Shi, and D. W. K. Ng, “Intelligent reflecting surface assisted multi-antenna covert communications: Joint active and passive  beamforming optimization,” IEEE Trans. Commun., vol. 69, no. 6, pp. 3984–4000, Jun. 2021  [32] Wang, Chao & Li, Zan & Zheng, Tong-Xing & Ng, Derrick Wing Kwan & Al-Dhahir, N.. (2022). Intelligent Reflecting Surface-Aided Full-Duplex Covert Communications: Information Freshness Optimization. IEEE Transactions on Wireless Communications. PP. 1-1. 10.1109/TWC.2022.3217041.  [33] Wang, C.; Li, Z.; Shi, J.; Ng, D.W.K. Intelligent Reflecting Surface-Assisted Multi-Antenna Covert Communications: Joint Active  and Passive Beamforming Optimization. *IEEE Trans. Commun.* **2021**, *69*, 3984–4000.  [34] Pejoski, S.; Hadzi-Velkov, Z.; Zlatanov, N. FullDuplex Covert Communications Assisted by Intelligent Reflective Surfaces. *IEEE*  *Commun. Lett.* **2022**, *26*, 2846–2850  [35] Wang, M.; Xu, Z.; Xia, B.; Guo, Y. Active Intelligent Reflecting Surface Assisted Covert Communications. *IEEE Trans. Veh. Technol.* **2023**, *72*, 5401–5406.  [36] Wang, C.; Li, Z.; Zheng, T.-X.; Ng, D.W.K.; Al-Dhahir, N. Intelligent Reflecting Surface-Aided Full-Duplex Covert Communications:  Information Freshness Optimization. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 3246–3263.  [37] Z. Guo, S. Zhao, J. Wang, H. Lit and Y. Shen, "Optimal Location Design for UAV Covert Communications with a Full-Duplex Receiver," in 2022 International Conference on Networking and Network Applications (NaNA), Urumqi, China, 2022 pp. 35-40. doi: 10.1109/NaNA56854.2022.00014  [38] Xu, Xiaobei & Hu, Linzi & Wei, Sha & Qian, Yuwen & Yan, Shihao & Shu, Feng & Li, Jun. (2023). On IRS-Assisted Covert Communication with a Friendly UAV. 10.20944/preprints202305.2156.v1.  [39] Zhang, Ran & Chen, Xinying & Liu, Mingqian & Zhao, Nan & Wang, Xianbin & Nallanathan, Arumugam. (2022). UAV Relay Assisted Cooperative Jamming for Covert Communications Over Rician Fading. IEEE Transactions on Vehicular Technology. 71. 10.1109/TVT.2022.3164051.  [40] Zhou, X.; Yan, S.; Shu, F.; Chen, R.; Li, J. UAVEnabled Covert Wireless Data Collection. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 3348–3362.  [41] Li, M.; Tao, X., Wu, H.; Li, N. Joint Trajectory and Resource Optimization for Covert Communication in UAV-Enabled Relaying  Systems. *IEEE Trans. Veh. Technol.* **2023**, *72*, 5518– 5523  [42] R. Chen, J. Shi, L. Yang, C. Wang, Z. Li, P. Xiao, and G. Chen, “Performance analysis for user scheduling in covert cognitive radio networks,” in 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2020, pp. 1–6.  [43] X. Liao, J. Si, J. Shi, Z. Li, and H. Ding, “Generative adversarial network assisted power allocation for cooperative cognitive covert communication system,” IEEE Commun. Lett., vol. 24, no. 7, pp. 1463–1467, 2020.  [44] W. Xiong, Y. Yao, X. Fu, and S. Li, “Covert communication with cognitive jammer,” IEEE Wireless Commun. Lett., vol. 9, no. 10, pp. 1753– 1757, 2020  [45] Wen, Yingkun & Liu, Lei & li, Junhuai & Hou, Xiangwang & Zhang, Ning & Dong, Mianxiong & Atiquzzaman, Mohammed & Wang, Kan & Huo, Yan. (2023). A Covert Jamming Scheme Against an Intelligent Eavesdropper in Cooperative Cognitive Radio Networks. IEEE Transactions on Vehicular Technology. PP. 1-12. 10.1109/TVT.2023.3277457.  [46] Liao, Xiaomin & Si, Jiangbo & Shi, Jia & Li, Zan & Ding, Haiyang. (2020). Generative Adversarial Network Assisted Power Allocation for Cooperative Cognitive Covert Communication System. IEEE Communications Letters. PP. 1-1. 10.1109/LCOMM.2020.2988384.  [47] Sun, Ranran & Yang, Bin & Shen, Yulong & Jiang, Xiaohong & Taleb, Tarik. (2022). Covertness and Secrecy Study in Untrusted Relay-Assisted D2D Networks. IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2022.3201021.  [48] Wang, Y.; Yan, S.; Yang, W.; Zhong, C.; Ng, D.W.K. Probabilistic Accumulate-Then-Transmit in WirelessPowered Covert  Communications. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 10393–10406  [49] Feng, S.; Lu, X.; Sun, S.; Niyato, D. Mean-Field Artificial Noise Assistance and Uplink Power Control in Covert IoT Systems.  *IEEE Trans. Wirel. Commun.* **2022**, *21*, 7358–7373  [50] Liu, J.; Yu, J.; Chen, X.; Zhang, R.; Wang, S.; An, J. Covert Communication in Ambient Backscatter Syst With Uncontrollable  RF Source. *IEEE Trans. Commun.* **2022**, *70*, 1971–1983.  [51]  []52 |  |

**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.