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** | **6** |
| 1.1. Background | 12 |
| 1.2. Contributions | 12 |
| **2. System Model** | **14** |
| 2.1. Received Signals | 15 |
| 2.2. Covert Message Detection | 17 |
| **3. Problem Formulation** | **21** |
| **4. Proposed Solutions** | **23** |
| **5. Numerical Results** | **25** |
| **6. Conclusion** | **32** |
| 6.1. Future Work | 34 |
| **Bibliography** | **35** |
| **Abstract** | **44** |

**List of Figures**

|  |  |  |
| --- | --- | --- |
| 1.1 | Schematic diagram | 14 |
| 1.2 | Node Placement | 27 |
| 1.3 | DEP versus Source Power | 28 |
| 2.1 | DEP versus Covert rate | 29 |
| 2.2 | DEP versus Minimum Quality of Service for Public Message | 30 |
| 2.3 | DEP versus Destination Transmit Power | 31 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**List of Tables**

|  |  |  |
| --- | --- | --- |
| 1.1 | Schematic diagram | 14 |
| 1.2 | Node Placement | 27 |
| 1.3 | DEP versus Source Power | 28 |
| 2.1 | DEP versus Covert rate | 29 |
| 2.2 | DEP versus Minimum Quality of Service for Public Message | 30 |
| 2.3 | DEP versus Destination Transmit Power | 31 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**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** | **M**ultiple **I**nput **M**ultiple **O**utput |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Abstract**

Detection Error Probability Maximization for Disguised Full-Duplex Covert Communications

Refat Khan

Advisor: Jihwan Moon

This thesis delves into reliable covert communications with a disguised full-duplex (FD) node. Seemingly half-duplex receive-only, this node in our considered system simultaneously listens to a transmitter and secretly transmits covert messages to another hidden receiver. In the meantime, a warden attempts to detect this covert link. We first study the detection error probability (DEP) and identify the minimum DEP from the perspective of the warden. After that, we derive an optimal transmit power of the disguised FD node that concurrently maximizes the minimum DEP and guarantees a given reliability of covert rate. Numerical results validate the effectiveness of our proposed solution, and present how different system parameters affect the DEP performance. Numerical results validate the effectiveness of our proposed solution, and present how different system parameters affect the DEP performance. In conclusion, we provide valuable guidance for the design of secure communication systems and suggest avenues for future research in this critical domain.

**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 [3][4]. 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 [5][6]. 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 [7]. A suitable solution for such scenarios involves covert or low-probability-of-detection communications, which

conceal the presence of crucial communication links [8]. 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 [9][10][11]. 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 [12]. 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 [13]. In previous research, [14] explored receiver antenna selection, while [15] 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 [16]. 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 non-deployed zones (NDZ) [17]. Research on delay-constrained covert communications with fixed artificial noise (AN) power was explored in [18], while joint optimization problems for AN power and receiver position were discussed in [19,20]. Consideration of uncertain warden node locations was addressed in [21]. Additionally, [22] studied random covert channel selection by the transmitter to further confuse the warden, and [23] 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 [24]. In [25], 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, [26] 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 [27][28][29]. References [30] and [31] presuppose that the presence of the covert device is acknowledged by the warden. Reference [32] examines an IRS communication scenario where a covert user possesses full control over the IRS and remains concealed from the warden. In [33] the authors Analyz that covert user is unknown to the warden and the covert user does not have control over the IRS. In [34], 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, [35] explores uplink covert communications assisted by an IRS. [36] discusses the utilization of an active IRS, inherently full duplex, for covert communications between user pairs. Finally, [37] 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 [38]. 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 [39].[40] 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) [41]. In [42], 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 [43]. At present, some literature investigates covert communication in CR networks. Chen et al. [44] have analyzed user scheduling performance in covert CR Networks. In [45], the authors have addressed the problem of power allocation with the aid of generative adversarial network in covert CR networks. The authors of [46] 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 [47] 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, [48] investigated a covert transmitter with optimized transmission probability, powered wirelessly by artificial noise (AN) from an FD receiver. Moreover, [49] optimized covert uplink transmissions of devices to FD IoT gateways using a mean-field Stackelberg game approach. Additionally, [50] 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**

In our covert communication system, the setup involves a source node transmitting a public message to a destination node. What makes our system unique is that the transmission from the seemingly receive-only destination node is conducted covertly. This covert signal is then transmitted to a hidden receiver using an unseen antenna setup. Our transmission environment utilizes full-duplex (FD) communication, allowing for simultaneous transmission and reception. However, we operate under the watchful eye of a warden node, which monitors for any suspicious communications. Our primary focus is on ensuring secure and undetectable transmission from the destination to the hidden node, all while under the surveillance of the warden node.

**1.2 Contributions**

While [1] delves into enhancing cloud radio access networks by optimizing data transfer and adapting to changing connection quality, and [2] explores securing wireless communication against eavesdropping using energy harvesting jamming, my work extends these concepts by focusing on the optimization of covert communication systems in practical scenarios. 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**

**2.1 Received Signals**

A diagram of a communication system

Description automatically generated

**Figure 1.** System Model

Figure 1 depicts the system model we are considering. There is a source node that sends a public message to a destination node which appears to be half-duplex receive-only, but in fact, secretly sends a covert message to a hidden receiver node using a concealed extra antenna. Meanwhile, a warden node monitors for any unexpected communications i.e., covert messages.

Let us express the received signal at the destination node as

In this system model, the channel coefficient represents communication links between different nodes X, Y \in {S, D, R, W}. The residual self-interference channel accounts for leftover signals after cancelling self-interference. Public messages and covert messages are transmitted. Transmit power and by the source and destination nodes, respectively. Additive noise is present at each node, and we assume that the destination node can estimate the while the hidden receiver can estimate and if provided with pilot sequences [37]. The warden is assumed to have perfect knowledge of all channel state information (CSI) for the worst-case scenario analysis. We also consider that the source adopts its data rate based on destination feedback, and the achievable data rate at the destination is denoted by as [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. Accordingly, the received signal of the hidden receiver can be written by

the hidden receiver first decodes and removes the public message before accessing the covert message. Consequently, the achievable public data rate, denoted by , at the hidden receiver is given as

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

**2.2 Covert message Detection**

The received signal at the warden is expressed by

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

The null hypothesis indicates a case that there are no covert messages, the alternative hypothesis presumes that the destination node did not transmit a covert message.

In this study, a radiometer [51] is utilized as a detection method at the warden. The test statistic for equation (7), after observing number of symbols leads to the average residual power as [52]

The warden node determines the presence of a covert transmission if surpasses a predefined threshold .

In this thesis, we consider uncertainty on the noise variance at the warden, similar to [51] and [53].

Specifically, we model the noise variance in decibels as where represents the mean and denotes the bounded range. The resulting detection error probability (DEP) , that encompasses both false alarm and miss detection probabilities is then expressed by

with equal probabilities for both null hypothesis and the alternative hypothesis [54]. By leveranging the cumulative distribution function (CDF) of as

,

the false alarm and miss probability are calculated by

respectively.

Where and

We encounter two distinct scenarios upon the magnitude of and

If ,

Where

On the other hand, if ,

With .

It is apparent that the warden prefers to set the threshold that helps minimize the (DEP). To achieve this, we observe that equation and decreases monotonically from to for , and increases monotonically from to as . Additionally, the first derivative of the sum is calculated as

which is consistently positive . Thus, the optimal threshold for the warden node in both equations and is obtained by

It is worth pointing out that we take a conservative assumption that the warden has perfect knowledge of the actual value of , which corresponds to the worst-case scenario from the perspective of covert communications.

**Chapter 3**

**Problem Formulation**

In this study, we aim to optimize the public data rate and transmission power at the disguised FD destination node that maximizes the minimum error probability at the warden node as

(17a)

(17b)

(17c)

(17d)

(17e)

(17f)

(17g)

Constraint (17b) ensures that the hidden receiver can successfully decode and remove the public message before decoding the covert message. Constraint (17c) specifies the maximum achievable public data rate, allowing the destination node to inform the source node for adjustment. In (17d), a minimum quality of services for public transmission is considered. (17e) specifies a minimum threshold for the covert data rate for reliable covert transmission and ensures a non-zero DEP. Finally, constraint indicates the power budget for the disguised FD node.

**Chapter 4**

**Proposed Solutions**

This chapter discusses the solution for (P1) that maximizes the worst-case DEP in (17a).

First, it is important to note that DEP is a decreasing function of . Similarly, the upper limits of the public data rate and also decrease as increases. This implies that the public rate cannot surpass a certain threshold, which is defined by the minimum of two upper limits, namely , i.e. Consequently, it's advantageous for to remain at its lowest feasible level to consistently uphold a minimum public rate, given by

However, the covert rate in increases with an increase Therefore, in order to maximize the worst-case DEP, we can easily see that the covert rate should be set to the minimum possible value, which is the required threshold .

Given these trade-offs, (P1) reduces to the following:

Therefore, this leads to the optimal as

(19a)

(19b)

(19c)

(19d)

(19e)

(19f)

,,

**Remark 1**: In certain scenarios, it is plausible for the upper bound to be lower than the lower bound. In such cases, the optimal transmit power is determined to be zero.

**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 from 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

A grid with different colored dots and numbers

Description automatically generated with medium confidence

**Figure 2.** Node Placement

Figure illustrates how the minimum detection error probability (DEP) changes with variations in the source transmit power Recognizing the necessity for the destination transmit power to be significantly lower than to ensure successful covert transmission. We evaluate the performance of the optimal scheme against an alternative approach denoted as “”. In this alternative scheme, is fixed as the minimum value between a certain percentage of and the average destination transmit power. Our observation indicates that the proposed strategy, incorporating the public data rate optimization from equation and the destination transmit power optimization from equation , Consistently yields the highest worst-DEP rate across various values. This underscores the critical importance of optimization both and .

A graph of a number of data

Description automatically generated with medium confidence

**Figure 3**. The average minimum DEP versus the source node power

Figure 4 presents a comparison of the average worst-case Detection Error Probability (DEP) with changes in the covert rate . It's evident that the worst-case DEP exhibits a monotonically decreasing trend as the covert rate increases. This observation stems from the fact that while the destination transmit power increases, the covert rate consistently increases, resulting in a decrease in DEP.

​

A graph of different colored lines

Description automatically generated

**Figure 4.** Covert rate versus the average worst-DEP: optimal shows the highest decreasing rate of DEP compared to the other schemes.

Figure illustrate the average worst-DEP and minimum quality of services for public message respectively, when the changes. The average worst-DEP rates decline in monotonic manner as increases.

Figure 6 illustrates a comparison of the average worst-DEP​ with variations in the destination transmit power budget ​. Notably, when ​ is low, both the "" and random ​ schemes demonstrate performance close to the optimal scheme . This closeness in performance arises because the influence of ​ is dominant in this range, and the fixed or randomly chosen ​ in the compared schemes converges to ​ if ​. However, for other regions of , our proposed solutions consistently achieve the highest Worst-DEP rate. This once again underscores the importance of optimizing both and .

A graph of the average amount of service for public messages

Description automatically generated

**Figure 5.** The average worst-DEP versus the minimum quality of service for public message.

A graph of a number of points

Description automatically generated

**Figure 6.** The average worst-DEP versus the destination node power budget : Close performance among the presented schemes for low since the optimal is dominantly limited by

**Chapter 6**

**Conclusion**

In this study, we explored a covert communication setup where a source node communicates with a disguised full-duplex (FD) destination node. Despite appearing as a receiver-only node, the destination secretly transmits crucial messages to a hidden receiver while evading detection by a monitoring warden node. Our focus was on determining the optimal public data rate and transmit power for the FD destination node, aiming to maximize the minimum detection error probability (DEP) at the warden node.

The analytical solution we derived revealed several key insights: When the link between the destination and receiver is exceptionally strong, the optimal transmit power for the destination node tends towards zero. This occurs because the hidden receiver cannot effectively filter out source messages before receiving covert messages. Similarly, insufficient suppression of self-interference also leads to an optimal transmit power close to zero, as the public data rate cannot maintain the required quality of service. Additionally, in scenarios where the channel gain between the destination and warden node is significantly high, the optimal transmit power for the destination node approaches zero, as the warden node can more easily detect the covert link due to the large power difference.

Given that our work offers valuable insights from an information-theoretic perspective, we recommend further exploration of practical modulation techniques and the impact of imperfect channel state information (CSI) as promising avenues for future research.

**6.1 Future Work**

Future work for this research paper could encompass several avenues of exploration. First and foremost, practical implementation of the proposed covert communication system in real-world scenarios would be essential to validate its efficacy and assess its performance under realistic conditions. This could involve field tests or simulations to evaluate its robustness and reliability. Additionally, further analysis could delve into the security aspects of the system, investigating its resilience against potential attacks or vulnerabilities. Integration with emerging technologies, such as artificial intelligence or blockchain, could also be explored to enhance the system's capabilities and adaptability to evolving communication landscapes. Moreover, considerations regarding legal and ethical frameworks surrounding covert communication systems would be pertinent, ensuring compliance with regulations and ethical standards. Incorporating user feedback and iterative improvements based on user experiences could further refine the system's design and usability, ensuring it meets the needs and expectations of its intended users.

**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 transmitter side correlation," IEEE Trans. Commun., IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 15, NO. 12, DECEMBER 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] | B. A. Bash, D. Goeckel, D. Towsley and S. Guha, "Hiding information in noise: fundamental limits of covert wireless communication," in IEEE Communications Magazine, vol. 53,no.12,pp.2631,Dec.2015,doi:10.1109/MCOM.2015.7355562 |
| [9] | J. Hu, S. Yan, X. Zhou, F. Shu, J. Li and J. Wang, "Covert Communication Achieved by a Greedy Relay in Wireless Networks," in IEEE Transactions on Wireless Communications, vol. 17, no. 7, pp. 4766-4779, July 2018, doi: 10.1109/TWC.2018.2831217. |
| [10] | J. Hu, K. Shahzad, S. Yan, X. Zhou, F. Shu and J. Li, "Covert Communications with a Full-Duplex Receiver over Wireless Fading Channels," 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1-6, doi: 10.1109/ICC.2018. 8422941. |
| [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.16,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, VOL. 8, NO. 3, JUNE 2019 |
| [19] | R. Xu, L. Guan, Y. Zhao, Z. Li and D. Wang, "Robust Power and Position Optimization for the Full-Duplex Receiver in Covert Communication," 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain,2021,pp.16,doi: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.16,doi:10.1109/ICC40277.2020.9148663 |
| [21] | X.Chen etal.,"MultiAntenna Covert Communication via Full Duplex Jamming Against a Warden With Uncertain Locations," in IEEE Transactions on Wireless Communications,vol.20,no.8,pp.54675480, Aug. 2021, doi: 10.1109/TWC.2021.3068096. |
| [22] | B. Che, W. Yang and X. Lu, "Covert Communication for Multi-Channel Transmission with A Full-Duplex Receiver," 2021 13th International Conference on Wireless Communications and Signal Processing (WCSP), Changsha, China,2021,pp.15, doi: 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] | Y. Li, R. Zhao, Y. Deng, F. Shu, Z. Nie and A. H. Aghvami, "Harvest-and-Opportunistically-Relay: Analyses on Transmission Outage and Covertness," in IEEE Transactions on Wireless Communications, vol. 19, no. 12, pp. 7779-7795, Dec. 2020, doi: 10.1109/TWC.2020.3015816 |
| [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. Björnson and L. Sanguinetti, "Power Scaling Laws and Near-Field Behaviors of Massive MIMO and Intelligent Reflecting Surfaces," in IEEE Open Journal of the Communications Society, vol. 1, pp. 1306-1324, 2020, doi: 10.1109/OJCOMS.2020.3020925 |
| [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," in IEEE Transactions on Wireless Communications, vol. 20, no. 1, pp. 421-439, Jan. 2021, doi: 10.1109/TWC.2020.3024887. |
| [29] | C. Wu, S. Yan, X. Zhou, R. Chen and J. Sun, "Intelligent Reflecting Surface (IRS)-Aided Covert Communication with Warden’s Statistical CSI," in IEEE Wireless Communications Letters, vol. 10, no. 7, pp. 1449-1453, July 2021, doi: 10.1109/LWC.2021.3069778 |
| [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," in IEEE Transactions on Communications, vol. 69, no. 6, pp. 3984-4000, June 2021, doi: 10.1109/TCOMM.2021.3062376. |
| [32] | C. Wang, Z. Li, T. -X. Zheng, D. W. K. Ng and N. Al-Dhahir, "Intelligent Reflecting Surface-Aided Full-Duplex Covert Communications: Information Freshness Optimization," in IEEE Transactions on Wireless Communications, vol. 22, no. 5, pp. 3246-3263, May 2023, doi: 10.1109/TWC.2022.3217041. |
| [33] | 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," in IEEE Transactions on Communications, vol. 69, no. 6, pp. 3984-4000, June 2021, doi: 10.1109/TCOMM.2021.3062376 |
| [34] | S. Pejoski, Z. Hadzi-Velkov and N. Zlatanov, "Full-Duplex Covert Communications Assisted by Intelligent Reflective Surfaces," in IEEE Communications Letters, vol. 26, no. 12, pp. 2846-2850, Dec. 2022, doi: 10.1109/LCOMM.2022.3206962. |
| [35] | M. Wang, Z. Xu, B. Xia and Y. Guo, "Active Intelligent Reflecting Surface Assisted Covert Communications," in IEEE Transactions on Vehicular Technology, vol. 72, no. 4,pp.5401-5406,April2023,doi:10.1109/TVT.2022.3224024. |
| [36] | C. Wang, Z. Li, T. -X. Zheng, D. W. K. Ng and N. Al-Dhahir, "Intelligent Reflecting Surface-Aided Full-Duplex Covert Communications: Information Freshness Optimization," in IEEE Transactions on Wireless Communications, vol. 22, no. 5, pp. 3246-3263, May 2023, doi: 10.1109/TWC.2022.3217041. |
| [37] | Z. Guo, S. Zhao, J. Wang, H. Lit and Y. Shen, "Optimal Location Design for UAV Covert Communications with a Full-Duplex Receiver," 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. Drones. 7. 453. 10.3390/drones7070453. |
| [39] | R. Zhang, X. Chen, M. Liu, N. Zhao, X. Wang and A. Nallanathan, "UAV Relay Assisted Cooperative Jamming for Covert Communications Over Rician Fading," in IEEE Transactions on Vehicular Technology, vol. 71, no. 7, pp. 7936-7941, July 2022, doi: 10.1109/TVT.2022.3164051. |
| [40] | Zhou, X.; Yan, S.; Shu, F.; Chen, R.; Li, J. UAV Enabled Covert Wireless Data Collection. IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 39, NO. 11, NOVEMBER 2021 |
| [41] | M. Li, X. Tao, H. Wu and N. Li, "Joint Trajectory and Resource Optimization for Covert Communication in UAV-Enabled Relaying Systems," in IEEE Transactions on Vehicular Technology, vol. 72, no. 4, pp. 5518-5523, April 2023, doi: 10.1109/TVT.2022.3225508. |
| [42] | R. Chen et al., "Performance Analysis for User Scheduling in Covert Cognitive Radio Networks," 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications, London, UK, 2020, pp. 1-6, doi: 10.1109/PIMRC48278.2020.9217377. |
| [43] | X. Liao, J. Si, J. Shi, Z. Li and H. Ding, "Generative Adversarial Network Assisted Power Allocation for Cooperative Cognitive Covert Communication System," in IEEE Communications Letters, vol. 24, no. 7, pp. 1463-1467, July 2020, doi: 10.1109/LCOMM.2020.2988384. |
| [44] | W. Xiong, Y. Yao, X. Fu, and S. Li, “Covert communication with cognitive jammer,” IEEE WIRELESS COMMUNICATIONS LETTERS, VOL. 9, NO. 10, OCTOBER 2020  . |
| [45] | Y. Wen et al., "A Covert Jamming Scheme Against an Intelligent Eavesdropper in Cooperative Cognitive Radio Networks," in IEEE Transactions on Vehicular Technology, vol. 72, no. 10, pp. 13243-13254, Oct. 2023, doi: 10.1109/TVT.2023.3277457. |
| [46] | X. Liao, J. Si, J. Shi, Z. Li and H. Ding, "Generative Adversarial Network Assisted Power Allocation for Cooperative Cognitive Covert Communication System," in IEEE Communications Letters, vol. 24, no. 7, pp. 1463-1467, July 2020, doi: 10.1109/LCOMM.2020.2988384. |
| [47] | R. Sun, B. Yang, Y. Shen, X. Jiang and T. Taleb, "Covertness and Secrecy Study in Untrusted Relay-Assisted D2D Networks," in IEEE Internet of Things Journal, vol. 10, no. 1, pp. 17-30, 1 Jan.1, 2023, doi: 10.1109/JIOT.2022.3201021 |
| [48] | Y. Wang, S. Yan, W. Yang, C. Zhong and D. W. K. Ng, "Probabilistic Accumulate-Then-Transmit in Wireless-Powered Covert Communications," in IEEE Transactions on Wireless Communications, vol. 21, no. 12, pp. 10393-10406, Dec. 2022, doi: 10.1109/TWC.2022.3183892 |
| [49] | S. Feng, X. Lu, S. Sun and D. Niyato, "Mean-Field Artificial Noise Assistance and Uplink Power Control in Covert IoT Systems," in IEEE Transactions on Wireless Communications, vol. 21, no. 9, pp. 7358-7373, Sept. 2022, doi: 10.1109/TWC.2022.3157885 |
| [50] | J. Liu, J. Yu, X. Chen, R. Zhang, S. Wang and J. An, "Covert Communication in Ambient Backscatter Systems With Uncontrollable RF Source," in IEEE Transactions on Communications, vol. 70, no. 3, pp. 1971-1983, March 2022, doi: 10.1109/TCOMM.2022.3144447. |
| [51] | B. He, S. Yan, X. Zhou and V. K. N. Lau, "On Covert Communication With Noise Uncertainty," in IEEE Communications Letters, vol. 21, no. 4, pp. 941-944, April 2017, doi: 10.1109/LCOMM.2016.2647716. [CrossRef]. |
| [52] | T. V. Sobers, B. A. Bash, S. Guha, D. Towsley and D. Goeckel, "Covert Communication in the Presence of an Uninformed Jammer," in IEEE Transactions on Wireless Communications, vol. 16, no. 9, pp. 6193-6206, Sept. 2017, doi: 10.1109/TWC.2017.2720736. |
| [53] | Si, J.; Li, Z.; Zhao, Y.; Cheng, J.; Guan, L.; Shi, J.; Al-Dhahir, N. Covert Transmission Assisted by Intelligent Reflecting Surface.  *IEEE Trans. Commun.* **2021**, *69*, 5394–5408. [CrossRef] |
| [54] | Z. Liu, J. Liu, Y. Zeng and J. Ma, "Covert Wireless Communications in IoT Systems: Hiding Information in Interference," in IEEE Wireless Communications, vol. 25, no. 6, pp. 46-52, December 2018, doi: 10.1109/MWC.2017.1800070 [CrossRef] |

|  |  |
| --- | --- |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  |  |

**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 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 performance guidelines 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.