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 Abbreviations** | **iii** |
| **Abstract** | **iv** |
| **1. Introduction** | **1** |
| 1.1. Contributions | 5 |
| **2. System Model** | **7** |
| 2.1. Received Signals | 7 |
| 2.2. Covert Message Detection | 9 |
| **3. Problem Formulation** | **13** |
| **4. Proposed Solutions** | **15** |
| **5. Numerical Results** | **18** |
| **6. Conclusion** | **26** |
| 6.1. Future Work | 27 |
| **Bibliography** | **28** |
| **Abstract** | **36** |

**List of Figures**

|  |  |  |
| --- | --- | --- |
| 1.1 | Schematic Diagram | 7 |
| 5.1 | Node Placement | 19 |
| 5.2 | DEP versus Source Power | 20 |
| 5.3 | DEP versus Covert Rate | 22 |
| 5.4 | DEP versus Minimum Quality of Service for Public Message | 23 |
| 5.5 | DEP versus Destination Transmit Power | 24 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**List of Abbreviations**

|  |  |  |
| --- | --- | --- |
|  | **FD** | **F**ull **D**uplex |
|  | **DEP** | **D**etection **E**rror **P**robability |
|  | **CSI** | **C**hannel **S**tate **I**nformation |
|  | **IRS** | **I**ntelligent **R**eflecting **S**urface |
|  | **AN** | **A**rtificial **N**oise |
|  | **UAV** | **U**nmanned **A**erial **V**ehicle |
|  | **CR** | **C**ognitive **R**adio |
|  | **IoT** | **I**nternet of **T**hings |
|  | **D2D** | **D**evice to **D**evice |
|  | **UE** | **U**ser **E**quipment |
|  | **HD** | **H**alf-**D**uplex |
|  | **MOP** | **M**ulti **O**bjective **O**ptimization **P**roblem |
|  | **ACP** | **A**verage **C**overt **P**robability |
|  | **CF** | **C**ompress-and-**F**orward |
|  | **DF** | **D**ecode-and-**F**orward |
|  | **AF** | **A**mplify-and-**F**orward |
|  | **IoT** | **I**nternet of **T**hings |
|  | **PDD** | **P**enalty **D**ual **D**ecomposition |
|  | **SCA** | **S**uccessive **C**onvex **A**pproximation |
|  | **BS** | **B**ase **S**tation |
|  | **CDF** | **C**umulative **D**istribution **F**unction |

**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. In conclusion, we provide valuable guidance for the design of secure communication systems and suggest for future research direction 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 [1][2]. The widespread adoption of wireless communications, on the other hand, is accompanied by cyberattacks that expose users to the risk of information disclosure [3]. In response to this challenge, cryptography has become extensively utilized, employing secret keys to encode and decode data [4]. Besides, a number of 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]. Nonetheless, even though these technologies keep our messages safe from eavesdroppers, communication links might still be at privacy risk. For instance, the electromagnetic signals from a commander on the battlefield may expose his position to nearby enemies, communicating in the presence of an authoritarian government who may want to curtail any organization by certain entities [7]. A suitable solution for such scenarios involves covert or low-probability-of-detection communications, which conceals the presence of crucial communication links [8].

Extensive research has also been conducted on covert communications within FD systems. The authors in [9] investigated covert communication using an FD receiver under limited channel information and demonstrated that random noise improves performance. By optimizing transmit and AN power to minimize outage probability at Bob, the authors observed a non-linear relationship between AN power and performance. Additionally, the numerical results in [10] presented some performance differences between circumstances with and without CSI. In [11], a constrained MOP was formulated to maximize two conflicting objectives: the transmission rate between legitimate transceivers and the ACP for eavesdroppers. This optimization involves adjusting transmit power and the position of the FD receiver, such as in UAV relay networks. Research on delay-constrained covert communications with fixed AN power was explored in [12], while joint optimization problems for AN power and receiver position were discussed in [13][14]. Consideration of uncertain warden node locations was addressed in [15]. Additionally, [16] studied random covert channel selection by the transmitter to further confuse the warden and identified the DEP under the age of information constraint.

In complex FD systems, the performance of covert communications varies across different relay systems: DF, CF, and AF. The study in [17] compares DF, CF, and AF systems, accounting for system parameters that is processing delay, quality of service, and DEP threshold, revealing performance variations under different conditions. In [18], authors devised a protocol for energy harvesting FD DF relay-based covert communications. Furthermore, [19] investigated FD relay-aided covert communications from a satellite to a ground node in the context of integrated satellite–terrestrial communications. Optimization of both secrecy and covert rates was performed in [20] where an untrusted FD AF relay transmits the covert message to an FD base station. The base station then emits AN to deceive the warden. In the IoT domain, [21] investigated a covert transmitter with optimized transmission probability, powered wirelessly by AN from an FD receiver. Moreover, [22] optimized covert uplink transmissions of devices to FD IoT gateways using a mean-field Stackelberg game approach. Additionally, [23] 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.

Recently, the research community has given significant attention to possibilities of covert communications in IRS [24-27]. The authors of [28] and [29] collectively contribute to advancing the field of covert communication within IRS aided communication systems. They focus on optimizing transmission power, phase shifts, and beamforming vectors to maximize secrecy while leveraging IRS technology. Additionally, they propose novel algorithms to address the optimization challenges posed by imperfect CSI, offering practical solutions to enhance covert communication performance. By exploring the potential of IRS in multi-antenna systems and tackling non-convex optimization problems using PDD and SCA methods, these papers provide valuable insights and techniques for improving covert communication in the presence of surveillance. The authors of [30] examined an IRS communication scenario where a covert user possesses full control over the IRS and remains concealed from the warden. In [31], optimization of a transmit beamforming vector and reflecting coefficients is conducted for IRS-aided covert communications, where an FD receiver emits random AN to confuse the warden. Additionally, [32] explored uplink covert communications assisted by an IRS and [33] discussed the utilization of an active IRS, inherently FD, for covert communications between user pairs.

Moreover, covert communications have been briefly studied in UAV systems. In [34], the authors concentrated on a covert communication setup utilizing UAVs equipped with FD receivers. [35] employed to help the transmission and confuse the warden. The maximum lowest average covert rate was achieved in the case of an FD UAV collecting data from a scheduled user and interfering with unscheduled users using AN [36]. In [37], the authors explored an FD DF UAV relay to facilitate covert communications, where multiple sensors transmit messages to a remote base station in separate time slots.

Some literature investigated covert communications in CR networks. Chen et al. [38] analyzed user scheduling performance in covert CR Networks. In [39], the authors addressed the problem of power allocation with the aid of generative adversarial network in covert CR networks. The authors of [40] considered covert communications by exploiting cognitive jammers to counter an intelligent eavesdropper. Enhancing physical layer security within cooperative cognitive radio networks. In [41] the authors discussed dilemmas, balancing covertness and secrecy. On one hand, the goal is to prevent detection by Willie of the D2D communications, while on the other hand, the untrusted relay poses a threat of eavesdropping on the user equipment (UE) message. Another dilemma arises in determining the optimal power control strategy at the UE, relay, and BS to maximize the average covert rate while ensuring covertness and security requirements are met.

Although numerous communications systems were analyzed from various perspectives of covertness as such, it is worth pointing out that many 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 FD node secretly transmitting sensitive messages might masquerade as a receiver-only HD node. To the author's knowledge, there is has not been sufficient work on covert communications that incorporates such deceptive strategies beside our initial result of [42].

**1.1 Contributions**

In our covert communication system, the setup involves a source node transmitting a public message to a seemingly receive-only destination node. This destination then secretly transmits a covert message to a hidden receiver using an unseen antenna in an FD manner. Our focus is on ensuring secure and undetectable transmission from the destination to the hidden node, all while under the surveillance of the warden node.

The contributions of our research can be outlined as follows:

* Unlike previous studies which assume that the surveillance party is sure of covert node hardware specifications, we consider a practical scenario where a covert communication node disguises as a different functional entity to enhance its stealth further.
* The worst-case DEP is calculated considering the uncertainty of noise at the warden node.
* Our focus lies in improving the minimum DEP 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.
* We explore the impact of diverse system parameters on the worst-case DEP using numerical analysis.
* Given that our study offers insights from an information-theoretic standpoint, we propose exploring practical modulation techniques and the implications of imperfect CSI as promising for future research.

**Chapter 2**

**System Model**

**2.1 Received Signals**

**A diagram of a communication system

Description automatically generated**

**Figure 1.1:** Schematic diagram

Figure 1.1 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. The entire system operates on the same frequency and within the same time slots to avoid detection.

Let us express the received signal at the destination node as

. (1)

In this system model, the channel coefficient represents communication links between different nodes X, Y {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 [43]. The warden is assumed to have perfect knowledge of all 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 [44]

. (2)

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

. (3)

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

. (4)

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

. (5)

**2.2 Covert Message Detection**

The received signal at the warden is expressed by

. (6)

It first eliminates public messages from to calculate the effective residual signal , assuming it perfectly knows and [45]. Then, the warden can consider the following two hypotheses:

(7)

The null hypothesis indicates a case that there are no covert messages, the alternative hypothesis presumes that the destination node transmits a covert message.

In this study, a radiometer [46] 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 [47]

(8)

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 [48,49] and [50].

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

(9)

With equal probabilities for both null hypothesis and the alternative hypothesis [51]. By leveraging the CDF of [42] as

, (10)

the false alarm and miss probability are calculated by

, (11)

, (12)

respectively, where and . We encounter two distinct scenarios upon the magnitude of and

If ,

(13)

where . On the other hand, if ,

(14)

with , , and .

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

(15)

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

, (16)

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)

subject to: , (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 (17f) ensures a non-zero DEP. Finally, constraint (17g) indicates the power budget for the disguised FD destination 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 (i.e., the derivative of DEP equation (15) is negative with respect to .Similarly, the upper limits of the public data rate (17b) and (17c) also decrease as increases ( is denominator at equation (2) and (4)). 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

(18)

However, the covert rate in (17e) 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:

, (19a)

Subject to: , (19b)

, (19c)

, (19d)

, (19e)

, (19f)

Therefore, this leads to the optimal as

. (20)

The analytical solution we derived revealed several key insights as follows.

**Remark 1**: In certain scenarios, the upper bound may be lower than the lower bound. In such infeasible cases, the transmit power can be simply set to 0 in an effort to evade from detection.

**Remark 2:** 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. In such a case, the hidden receiver may consider directly decoding the covert message instead of first decoding and subtracting the public message.

**Remark 3:** 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.

**Remark 4:** 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.

**Chapter 5**

**Numerical Results**

We assess the maximum achievable worst-case DEP with the disguised FD node through numerical analysis. We 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 from (20).

We adopt the distance-dependent channel model from [52] where represents the path loss between nodes and , denotes the path loss at a reference distance m, signifies the path loss exponent, and indicates the distance between nodes and . Additionally, the small-scale channel variable follows the complex normal distribution . The four nodes are positioned at certain distance from the origin in the cartesian coordinate system, with coordinates for and denoted by and respectively (Figure 5.1). The overall system parameters are predefined as follows, unless otherwise stated: bandwidth MHz, m, source transmit power dBm, destination transmit power budget = 23dBm, public message quality of service bps/Hz, mean noise power at the warden node dBm/Hz, noise uncertainty bound dB, noise power at the destination node and hidden receiver dBm/Hz, residual self-interference dB, minimum DEP threshold , and path loss exponent

A grid with different colored dots and numbers

Description automatically generated with medium confidence

Figure 5.1: Node placement

A graph of a number of data

Description automatically generated with medium confidence

Figure 5.2: Worst-case DEP versus source power

Figure 5.2 illustrates how the worst-case DEP changes with the source transmit power Since it is necessary for the destination transmit power to be significantly lower than to ensure covertness, we compare the optimal solution with fixed power schemes "" in which is set to min ( ). We observe that applying more to a covert transmission induces a higher worst-case DEP rate when is low, while less is preferred when is high. First, when is low, the public data rate constraints in (17b) and (17c) dominate the determining form (20). If then any schemes with are likely to be infeasible on average. It can be inferred form Figure 5.2 that for our system setup since performs the best among the other fixed schemes. On the other hand, when is high, the power budget dominate deciding . Hence, only the schemes with sufficiently low can meet these requirements and be feasible on average. This explains the reason why outperforms those with higher in Figure in the high region. The figure also indicates that the proposed strategy, incorporating the public data rate optimization from equation (18) and the destination transmit power optimization from equation (20), consistently yields the highest worst-case DEP rate across various values. This underscores the critical importance of optimizing both and .

A graph of different numbers

Description automatically generated with medium confidence

Figure 5.3: DEP versus covert rate

Figure 5.3 presents the average worst-case DEP with changes in the covert rate threshold . It is evident that the worst-case DEP exhibits a monotonically decreasing trend as the guaranteed covet rate increases. This observation stems from the fact that higher requires higher transmit power which, in turn, decreases the DEP since DEP is decreasing function of . It can be seen that and random schemes perform comparatively better than the other fixed power schemes in terms of average worst-case DEP. To maintain the covert rate, a certain minimum power must be provided. As the covert rate increases, higher is required, and this explains why scheme exhibits higher DEP than the other fixed power strategies.

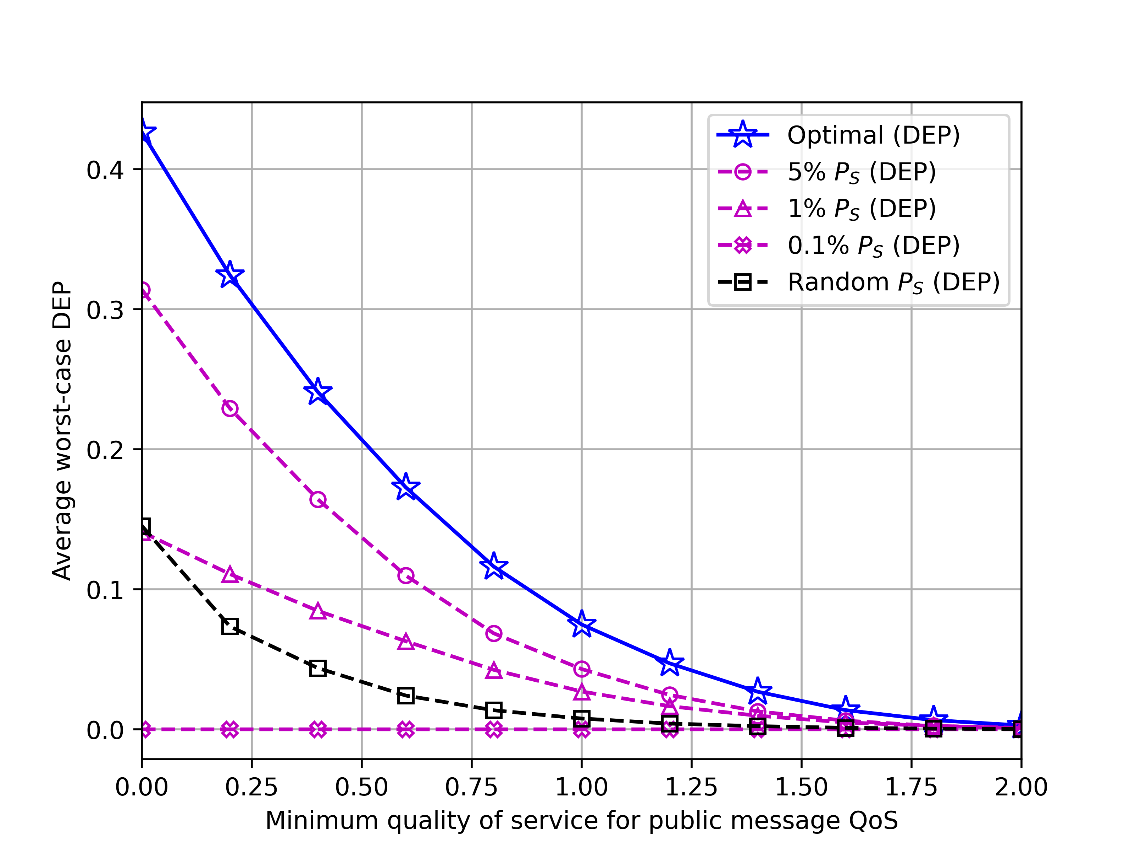


Figure 5.4: DEP versus minimum quality of service for public message QoS

Figure 5.4 illustrates the average worst-case DEP for different minimum quality of services for public message . The average worst-case DEP decline in monotonic manner as increases as expected.

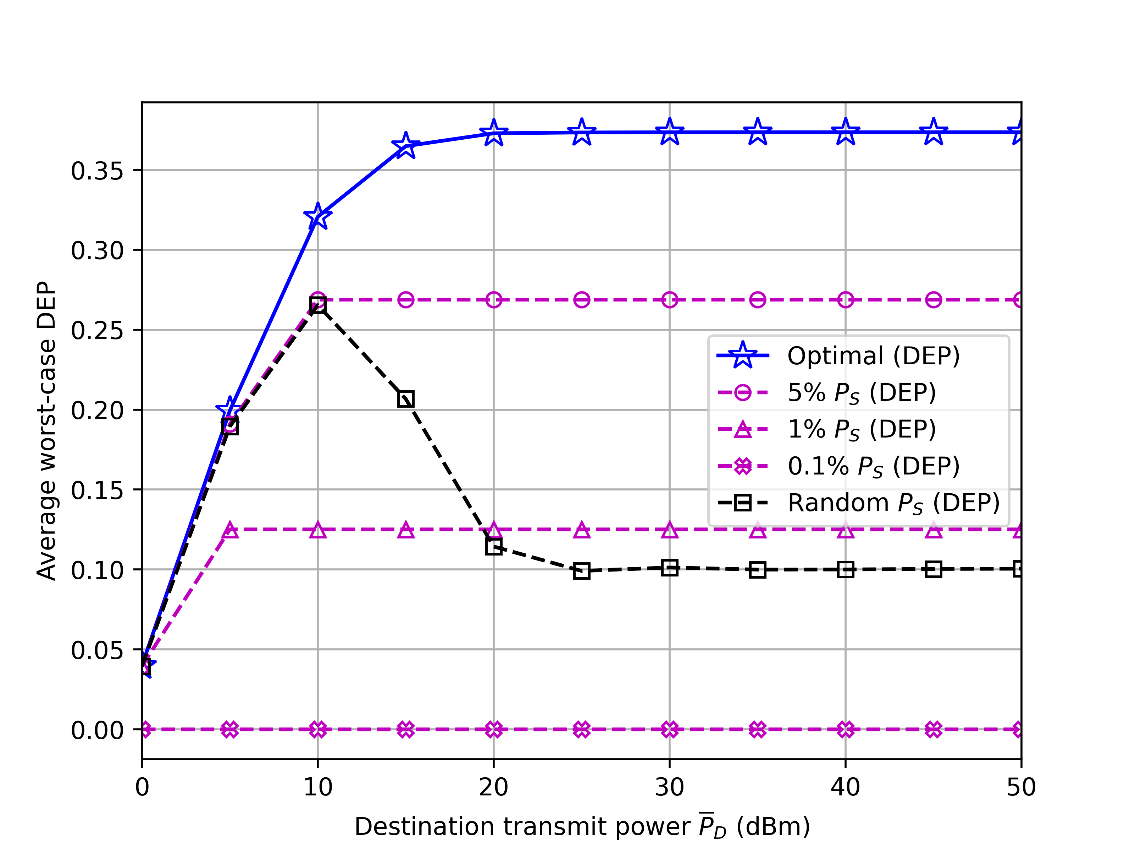


Figure 5.5: DEP versus destination transmit power budget.

Figure 5.5 shows the average worst-case DEP​ for different destination transmits power budget ​. Notably, when ​ is low, both the "" and random ​ schemes demonstrate performance close to the optimal scheme. This closeness in performance arises because ​ is dominantly determined by from (20), and the of the compared schemes with fixed or randomly chosen converges to ​​. This figure also clarifies that increasing cannot further improve DEP because it does not affect in (20). As a result, the DEP saturates beyond a certain in the figure. We would also like to highlight that our proposed solution consistently achieves the highest worst-case DEP, which once again underscores the importance of optimizing both and .

**Chapter 6**

**Conclusion**

In this study, we explored a covert communication setup where a source node communicates with a 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 wors-case DEP at the warden node.

The analytical solution we derived revealed several key insights as follows.

In certain scenarios, the upper bound may be lower than the lower bound. In such infeasible cases, the transmit power can be simply set to 0 in an effort to evade from detection.

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. In such a case, the hidden receiver may consider directly decoding the covert message instead of first decoding and subtracting the public message.

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.

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.

**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, could also be explored to enhance the system's capabilities and adaptability to evolving communication landscape.

**Bibliography**

|  |  |
| --- | --- |
| [1] | 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. |
| [2] | 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. |
| [3] | J. Zhang, Z. Yan, S. Fei, M. Wang, T. Li and H. Wang, "Is Today's End-to-End Communication Security Enough for 5G and Its Beyond?" in IEEE Network, vol. 36, no. 1, pp. 105-112, January/February 2022, doi: 10.1109/MNET.101.2100189. |
| [4] | Forouzan, B.A Cryptography and Network security; McGraw-Hill: New York, NY, USA |
| [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," in IEEE Transactions on Wireless Communications, vol. 15, no. 12, pp. 8286-8297, Dec. 2016, doi: 10.1109/TWC.2016.2613860. |
| [6] | H. -M. Wang, B. -Q. Zhao and T. -X. Zheng, "Adaptive Full-Duplex Jamming Receiver for Secure D2D Links in Random Networks," in IEEE Transactions on Communications, vol. 67, no. 2, pp. 1254-1267, Feb. 2019, doi: 10.1109/TCOMM.2018.2880216. |
| [7] | 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. |
| [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. 26-31, Dec. 2015, doi: 10.1109/MCOM.2015.7355562. |
| [9] | 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. |
| [10] | 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. |
| [11] | 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. |
| [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] | 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. 1-6, doi: 10.1109/GLOBECOM46510.2021.9685606. |
| [14] | 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. |
| [15] | 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. |
| [16] | 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. |
| [17] | Moon, Jihwan. (2023). Covert communications in a compress-and-forward relay system. ICT Express. 10.1016/j.icte.2023.08.005. |
| [18] | 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. |
| [19] | 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. |
| [20] | K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian and K. K. Leung, "Secrecy Rate Optimizations for a MIMO Secrecy Channel with a Multiple-Antenna Eavesdropper," in IEEE Transactions on Vehicular Technology, vol. 63, no. 4, pp. 1678-1690, May 2014, doi: 10.1109/TVT.2013.2285244. |
| [21] | 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. |
| [22] | 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. |
| [23] | 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. |
| [24] | Wu, Zeke & Guo, Kefeng & Zhu, Shibing. (2023). Covert Communication for Integrated Satellite–Terrestrial Relay Networks with Cooperative Jamming. Electronics. 12. 999. 10.3390/electronics12040999. |
| [25] | S. Zhang and R. Zhang, "Capacity Characterization for Intelligent Reflecting Surface Aided MIMO Communication," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 8, pp. 1823-1838, Aug. 2020, doi: 10.1109/JSAC.2020.3000814. |
| [26] | 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. |
| [27] | 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. |
| [28] | J. Si et al., "Covert Transmission Assisted by Intelligent Reflecting Surface," in IEEE Transactions on Communications, vol. 69, no. 8, pp. 5394-5408, Aug. 2021, doi: 10.1109/TCOMM.2021.3082779. |
| [29] | 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. |
| [30] | 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. |
| [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] | 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. |
| [33] | 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. |
| [34] | 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. |
| [35] | X. Jiang et al., "Covert Communication in UAV-Assisted Air-Ground Networks," in IEEE Wireless Communications, vol. 28, no. 4, pp. 190-197, August 2021, doi: 10.1109/MWC.001.2000454. |
| [36] | X. Zhou, S. Yan, F. Shu, R. Chen and J. Li, "UAV-Enabled Covert Wireless Data Collection," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 11, pp. 3348-3362, Nov. 2021, doi: 10.1109/JSAC.2021.3088688. |
| [37] | 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. |
| [38] | 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. |
| [39] | 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. |
| [40] | 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. |
| [41] | 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 |
| [42] | Moon, Jihwan. (2023). Disguised Full-Duplex Covert Communications. Sensors. 23. 6515. 10.3390/s23146515. |
| [43] | S. W. Kim and H. Q. Ta, "Covert Communications Over Multiple Overt Channels," in IEEE Transactions on Communications, vol. 70, no. 2, pp. 1112-1124, Feb. 2022, doi: 10.1109/TCOMM.2021.3127532 |
| [44] | Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; John Wiley & Sons, Inc.: New Jersey, NJ, USA, 2005 |
| [45] | S. W. Kim and H. Q. Ta, "Covert Communications Over Multiple Overt Channels," in IEEE Transactions on Communications, vol. 70, no. 2, pp. 1112-1124, Feb. 2022, doi: 10.1109/TCOMM.2021.3127532. |
| [46] | 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. |
| [47] | 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. |
| [48] | 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. |
| [49] | 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. |
| [50] | J. Si et al., "Covert Transmission Assisted by Intelligent Reflecting Surface," in IEEE Transactions on Communications, vol. 69, no. 8, pp. 5394-5408, Aug. 2021, doi: 10.1109/TCOMM.2021.3082779. |
| [51] | 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. |
| [52] | J. Moon, S. H. Lee, H. Lee and I. Lee, "Proactive Eavesdropping With Jamming and Eavesdropping Mode Selection," in IEEE Transactions on Wireless Communications, vol. 18, no. 7, pp. 3726-3738, July 2019, doi: 10.1109/TWC.2019.2918452. |

**ABSTRACT**

Detection Error Probability Maximization for Disguised Full-Duplex Covert Communications

Refat Khan

Dept. of Mobile Convergence Engineering

Graduate School of Software Convergence

Hanbat National University

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. In conclusion, we provide valuable guidance for the design of secure communication systems and suggest for future research direction in this critical domain.