Covert communications with channel inversion power control in uplink NOMA systems

Maochun Wang,1, 2 Jia Tu,3, † Meng Wang,1 Yida Wang,1 Hui Shi,1 and Weivei Yang†
1 College of Communication Engineering, Army Engineering University of PLA, Nanjing, China
2 Beijing Satellite Navigation Center, Beijing, China
3 College of International Studies, National University of Defense Technology, Nanjing, China
† Email: tujia_666@163.com

Covert communications hide the very existence of wireless transmissions and thus can address privacy and security issues in non-orthogonal multiple access (NOMA) systems. In this paper, we investigate covert communications in uplink NOMA systems with channel inversion power control (CIPC), where a public user’s transmission is exploited to confuse a warden’s detection on a covert user’s communication behaviour. More precisely, the public link with CIPC causes the channel uncertainty of received signals at the warden. Specifically, the warden’s detection error probability is derived and a guideline to make the optimal choice of CIPC parameters to obtain the maximum covert rate is proposed. The analysis and simulation results show that the covert rate is restricted by the interference between two users when the public user’s CIPC parameter is relatively large.

Introduction: Non-orthogonal multiple access (NOMA) has been proposed as one of the key technologies in next-generation communications for its higher spectrum efficiency, user fairness and massive connection support [1]. However, the broadcast nature of wireless transmission makes security become one of the most severe issues in wireless communications [2]. Some researchers studied secure transmission in NOMA networks based on physical layer security (PLS) [3, 4], which focused on the protection of communication content. Nevertheless, sensitive information (e.g., military intelligence or private medical information) transmission requires stronger security, which needs to hide the communication behaviour and the location of transmitter [5]. Covert communications aim to enable a communication between two nodes while guaranteeing a negligible detection probability of that communication at a watchful adversary [6, 7]. The information-theoretic fundamental limit on covert communications was disclosed in [6]. Following the pioneering researches, [7] studied covert communications in additive white Gaussian noise (AWGN) channels with the help of a jammer. The authors in [8, 9] investigated covert communications in downlink NOMA systems and device-to-device systems with uplink NOMA, respectively. Unfortunately, the aforementioned works overlooked the protection of covert information source’s location. As a feasible solution, the channel inversion power control (CIPC) technology avoids the source broadcasting pilot signals for channel estimation or feeding back the estimated channel to the receiver, which aids hiding the source’s location [10].

In this paper, we investigate covert communications in uplink NOMA systems with CIPC, where a covert user attempts to transmit sensitive information to a receiver under the shield of a transmission from a public user to the same receiver. It is noted that a warden is present to detect the covert user’s communication behaviour. We derive the closed-form expression of the warden’s detection error probability, and we further optimize the CIPC parameters to maximize the covert rate. Our analysis reveals that the maximum covert rate is a continuously increasing function of the public user’s CIPC parameter and restricted by the covertness and reliability requirements.

System model: We investigate an uplink NOMA system with a covert user (U1), a public user (U2), a receiver (Bob), and a warden (Willie). With the help of the public link from U2 to Bob, U1 intends to transmit private signals to Bob under the supervision of Willie. It is assumed that the wireless channels experience the block-static Rayleigh fading, which means that all the channel coefficients are independent and remain constant within one time slot but varying from one time slot to another. The channel from i (i.e., U1 and U2) to j (i.e., Bob and Willie) is denoted by $h_{ij}$, with $E(|h_{ij}|^2) = \lambda_{ij}$, where $i \in \{u_1, u_2, w_1, w_2\}$.

U1 and U2 estimate $h_{u_i}$ and $h_{w_i}$ by the pilots which are periodically broadcasted by Bob. Based on channel reciprocity, we have $h_{w_i} = h_{u_i}^*$ and $h_{u_i}^* = h_{w_i}$. Since U1 and U2 do not send pilots, U1 can possibly hide its location from Willie. Also, Willie is hard to acquire the CSI of $h_{w_i}$ and $h_{u_i}$, while Willie still can acquire the statistics information of $h_{w_i}$ and $h_{u_i}$, i.e., $\lambda_{w_i}$ and $\lambda_{u_i}$. Moreover, we adopt the CIPC at U1 and U2 to achieve the signal decoding at Bob, in which the transmit power varies as per $h_{u_i}$ such that $P_{u_i} h_{u_i}^2$ is a fixed value, $l \in \{1, 2\}$, i.e.

$$Q_l = \frac{P_{u_l} |h_{u_l}|^2}{\lambda_{u_l}},$$

where $P_{u_l}$ denotes U1’s transmit power, and $Q_l$ denotes the power control parameter of U1.

Detection performance at willie: In order to evaluate communication covertness, we need to analyse the detection performance at Willie. The detection error probability at Willie can be expressed as [7]

$$P_{D} = P \left[ \frac{|\sum_{i=1}^{n} y_{i}|^2}{\sum_{i=1}^{n} |x_{i}|^2} = \frac{1}{\lambda_{u_i}} |h_{u_i}|^2 \right] = \frac{1}{\lambda_{u_i}} \lambda_{u_i} Q_{\lambda_{u_i}}, \quad \tau > \lambda_{u_i}^2,$$

where $\lambda_{u_i}$ is the given threshold, and $\mathcal{D}$ and $\mathcal{D}_0$ are the binary decisions Willie made in favour of U1 transmits or not, respectively. Considering the case of $n \to \infty$ as [7, 10], $T_u$ can be written as

$$T_u = \frac{P_{u_2} |h_{u_2}|^2 + \alpha^2}{P_{u_1} |h_{u_1}|^2 + \alpha^2}, \quad \mathcal{H}_0,$$

or

$$T_u = \frac{P_{u_1} |h_{u_1}|^2 + \alpha^2}{P_{u_2} |h_{u_2}|^2 + \alpha^2}, \quad \mathcal{H}_1.$$

The detection performance at Willie is

$$\xi = \alpha + \beta,$$

where $\alpha = P \left[ \mathcal{D}_1 | \mathcal{H}_1 \right]$ is the false alarm probability and $\beta = P \left[ \mathcal{D}_0 | \mathcal{H}_0 \right]$ is the miss detection probability.

From (4) and (5), the false alarm probability $\alpha$ is derived as

$$\alpha = P \left[ T_u > \tau | \mathcal{H}_0 \right] = P \left[ \frac{|\sum_{i=1}^{n} y_{i}|^2}{\sum_{i=1}^{n} |x_{i}|^2} > \frac{1}{Q_2} \left( \tau - \alpha^2 \right) \right],$$

where

$$T_u = \frac{P_{u_1} |h_{u_1}|^2 + \alpha^2}{P_{u_2} |h_{u_2}|^2 + \alpha^2}, \quad \tau = \alpha^2,$$

or

$$T_u = \frac{P_{u_2} |h_{u_2}|^2 + \alpha^2}{P_{u_1} |h_{u_1}|^2 + \alpha^2}, \quad \tau = \alpha^2.$$
Similarly, the miss detection probability $\beta$ is derived as
\[
\beta = \mathbb{P}[T_1 < t] = \mathbb{P}\left[ \frac{Q_1|h_{1w}|^2}{|h_{1b}|^2} + \frac{Q_1|h_{2w}|^2}{|h_{2b}|^2} < t - \sigma_b^2 \right]
\]  
(7)

Since $h_{1w}$, $h_{1b}$, $h_{2w}$, and $h_{2b}$ are independent, $X_1 \overset{d}{=} \frac{Q_1|h_{1w}|^2}{|h_{1b}|^2}$ and $X_2 \overset{d}{=} \frac{Q_1|h_{2w}|^2}{|h_{2b}|^2}$ are still independent. Similar to (6), the cumulative distribution function (CDF) of $X_j$, $j \in \{1, 2\}$, is derived as
\[
F_{X_j}(x) = \mathbb{P}[X_j < x] = \begin{cases} \lambda_{a,w}^x, & x \geq 0, \\ 0, & \text{otherwise}, \end{cases}
\]  
(8)

and the corresponding probability density function (PDF) is derived as
\[
f_{X_j}(x) = \frac{dF_{X_j}(x)}{dx} = \begin{cases} \frac{Q_1\lambda_{a,w}\lambda_{a,b}}{Q_1\lambda_{a,w} + \lambda_{a,b}}, & x > 0, \\ 0, & \text{otherwise}. \end{cases}
\]  
(9)

As per (7) and (9), $\beta$ is derived as
\[
\beta = \int_0^{\tau - \sigma_b^2} \int_0^{\tau - \sigma_b^2 - x} f_{X_1}(y) f_{X_2}(x+y) \, dy \, dx
= \int_0^{\tau - \sigma_b^2} \int_0^{\tau - \sigma_b^2 - x} \frac{Q_1\lambda_{a,w}\lambda_{a,b}}{Q_1\lambda_{a,w} + \lambda_{a,b}} \left(\frac{Q_1\lambda_{a,w} + \lambda_{a,b}}{Q_1\lambda_{a,w} + \lambda_{a,b}}\right)^y \, dy \, dx
= K_1 K_2 \int_0^{\tau - \sigma_b^2} \left(\frac{1}{K_1 + y} - \frac{1}{K_1 + K_3}ight) \, dy
= K_3 \int_0^{\tau - \sigma_b^2} \left(\frac{1}{K_1 + y} - \frac{1}{K_1 + K_3}ight) \, dy
= \begin{cases} \frac{K_3}{K_1 + K_3}, & \tau > \sigma_b^2, \\ 0, & \text{otherwise}, \end{cases}
\]  
(10)

where $K_1 \overset{d}{=} \frac{Q_1|h_{1w}|^2}{|h_{1b}|^2}$, $K_2 \overset{d}{=} \frac{Q_1|h_{2w}|^2}{|h_{2b}|^2}$, and $K_3 \overset{d}{=} \tau - \sigma_b^2$.

Following (6) and (10), $\xi$ can be derived as
\[
\xi = \frac{K_2}{K_1 + K_2 + K_3} + \frac{K_3}{K_1 + K_2 + K_3} = \frac{K_1 K_2 \ln \left(\frac{K_2 + K_3}{K_1 + K_3}\right)}{K_1 K_2} = \frac{K_1 K_2 \ln \left(\frac{K_2 + K_3}{K_1 + K_3}\right)}{K_1 K_2} = \tau \geq \sigma_b^2,
\]  
(11)

From a conservative point of view, Willie has the ability to adopt an optimal detection threshold to achieve the minimum detection error probability. The optimal choice of the threshold to minimize the detection error probability is given by
\[
\tau^* = \text{argmin}_{\tau} \xi(\tau).
\]  
(12)

Since $\xi$ is a non-convex function of $\tau$, it is hard to give a closedform of the optimal Willie’s detection threshold $\tau^*$. We can solve this problem by the method of efficient one-dimension numerical search and obtain $\tau^*$. Substituting $\tau^*$ into (11), we can acquire the corresponding minimum detection error probability $\xi^*$. It is worth mentioning that $\xi^*$ is the function of $Q_1$ and $Q_2$, considering the worst-case, it is assumed that $Q_1$ and $Q_2$ are known by Willie.

Communication performance analysis and optimization: To decode the superimposed signals from U1 and U2, we handle U2’s signal first during the successive interference cancellation (SIC) process [8, 9]. The signal-to-interference-plus-noise-ratio (SINR) used to decode $x_{u_1}$ is given by
\[
y_{u_1} = \frac{P_{u_1} |h_{1w}|^2}{P_{u_1} |h_{1w}|^2 + \sigma_b^2} = \frac{Q_2}{Q_1 + \sigma_b^2},
\]  
(13)

and the corresponding channel capacity of U2 is given by $C_{u_2} = \log_2 \left(1 + \frac{Q_2}{Q_1 + \sigma_b^2}\right)$. It is noted that the outage event occurs when the SIC process fails during the decoding process. In order to guarantee the success of SIC at Bob, it needs to meet the condition as
\[
\log_2 \left(1 + \frac{Q_2}{Q_1 + \sigma_b^2}\right) \geq R_{u_2},
\]  
(14)

where $R_{u_2}$ is the predetermined transmission rate of U2. As per (13) and (14), we find that there exists the inherent limitation of $Q_1$ and $Q_2$, which is given by
\[
0 \leq Q_1 \leq \frac{Q_2}{2Q_{\sigma_b^2} - 1} - \sigma_b^2.
\]  
(15)

After SIC, we eliminate the interference from the public user, the signal-to-noise-ratio (SNR) used to decode $x_{u_1}$ is expressed as
\[
y_{u_1} = \frac{P_{u_1} |h_{1w}|^2}{\sigma_b^2} = \frac{Q_2}{\sigma_b^2},
\]  
(16)

and the corresponding communication rate of U1 is given by
\[
R_{u_1} = \log_2 \left(1 + y_{u_1}\right) = \log_2 \left(1 + \frac{Q_2}{\sigma_b^2}\right).
\]  
(17)

It is worth mentioning that U1 can achieve the maximum transmission rate under the requirement of successfully SIC when $Q_1 = \frac{Q_{\sigma_b^2}}{2Q_{\sigma_b^2} - 1} - \sigma_b^2$.

Furthermore, as per (11) and (15), under the limitation of covertness requirement, the problem of choosing the optimal power control parameters to maximize the covert rate is given by
\[
\max_{0 \leq Q_1 \leq Q_{\sigma_b^2}} R_{u_1} \quad \text{s.t.} \quad c_1 : \xi^*(Q_1, Q_2) \geq 1 - \varepsilon, \\
c_2 : 0 \leq Q_1 \leq \min \left(Q_{\sigma_b^2}^{\max}, \frac{Q_{\sigma_b^2}}{2Q_{\sigma_b^2} - 1} - \sigma_b^2\right), \\
c_3 : 0 \leq Q_2 \leq Q_{\sigma_b^2}^{\max},
\]  
(18)

where $\xi^*$ denotes the minimum detection error probability, $\varepsilon$ denotes the covert constraint, and $Q_{\sigma_b^2}^{\max}$ and $Q_{\sigma_b^2}^{\min}$ are the maximum value of $Q_1$ and $Q_2$, respectively, $c_1$ is the covertness requirement, $c_2$ and $c_3$ are the feasible condition of $Q_1$ and $Q_2$, respectively, and as per (15), $Q_1 \leq \frac{Q_{\sigma_b^2}}{2Q_{\sigma_b^2} - 1} - \sigma_b^2$ is the success of SIC requirement.

From (15) and (17), it is obviously that $R_{u_1}$ is an increasing function of $Q_1$ and the feasible condition of $Q_1$ is $0 \leq Q_1 \leq \min(Q_{\sigma_b^2}^{\max}, \frac{Q_{\sigma_b^2}}{2Q_{\sigma_b^2} - 1} - \sigma_b^2)$. Moreover, $\xi^*$ increases as $Q_2$ increases, which will be verified in the numerical results. Thus, $Q_2 = Q_{\sigma_b^2}^{\max}$ is the optimal choice to obtain the maximum covert rate, since higher $Q_2$ leads to higher detection error probability at Willie and larger feasible condition of $Q_1$.

The optimal choice of $Q_2$ is given by
\[
Q_2^* = \min Q_2 \left(\left(Q_2, Q_{\sigma_b^2}^{\max}, \frac{Q_{\sigma_b^2}}{2Q_{\sigma_b^2} - 1} - \sigma_b^2\right),
\]  
(19)

where $Q_2^*$ is the solution of $\xi^* = 1 - \varepsilon$. The corresponding maximum covert rate is given by
\[
R_{u_1}^* = \log_2 \left(1 + \frac{Q_2^*}{\sigma_b^2}\right).
\]  
(20)

Remark 1. It is noted that $R_{u_1}^*$ is restricted by the covertness requirement $\xi^* \geq 1 - \varepsilon$ and the success of SIC requirement $0 \leq Q_1 \leq \frac{Q_{\sigma_b^2}}{2Q_{\sigma_b^2} - 1} - \sigma_b^2$. 

361
As per (19), we can observe that the covertness requirement is the primary influence factor of $R^\ast_2$ when $Q^{\text{max}}$ is small (i.e. $Q^* = Q^1$), while the success of SIC requirement (i.e. reliability requirement) dominates $R^\ast_2$ when $Q^{\text{max}}$ is large enough (i.e. $Q^* = Q^{\text{max}} - \sigma^2_c$). Since the constraint $c_2$ is looser than $c_1$ when the value of $Q_2$ is small, while $c_1$ is looser than $c_2$ when $Q_2$ is relatively large. In other words, the interference between the two users leads to the SIC failure, which restricts the covert rate in case of the public user's transmit power is relatively large. The following simulation also verifies this conclusion.

**Numerical results:** In the following, we provide numerical results to evaluate performances in the considered covert communication system, where $\sigma^2_c = \sigma^2 = -10$ dBm, $\lambda_{\text{w}} = \lambda_{\text{b}} = 1$, and $\lambda_{\text{wb}} = 0.5$.

Figure 1 illustrates the minimum detection error probability $\xi^\ast$ at Willie versus $Q_2$ with different values of $Q_1$. We can first observe that when $Q_2$ is a fixed value, $\xi^\ast$ is a monotonically increasing function of $Q_1$ and converges to 1. It is due to the fact that a high value of $Q_2$ means a higher transmit power used to shield the covert link. As expected, we also observe that $\xi^\ast$ decreases as $Q_1$ increases. Since the transmit power of $U_1$ increases as $Q_1$ increases, which leads to larger exposure risk of the wireless transmit behaviour.

Figure 2 demonstrates the maximum covert rate $R^\ast_2$ at Bob versus $Q^{\text{max}}$ subject to different covert constraints $\epsilon$ with a fixed value of $R_{\text{w}} = 3$. It is clearly shown that $R^\ast_2$ is a monotonically increasing function of $Q^{\text{max}}$ and $\epsilon$. Moreover, when $Q^{\text{max}}$ is relatively large, $R^\ast_2$ coincides with the curve of the special case $Q_1 = \frac{Q^{\text{max}} - \sigma^2_c}{\lambda_{\text{w}} - \sigma^2_c}$ in (15), which means that the SIC error takes the lead role of $R^\ast_2$, rather than the covert constraint.

**Conclusion:** In this paper, we investigated CIPC aided covert communications in an uplink NOMA system and analysed the corresponding covertness performance. We derived the closed-form expression of the detection error probability and obtained the optimal choice of the power control parameters to acquire the maximum covert rate. The conducted analysis and numerical results illustrate that the covertness requirement is the main influence factor of covert rate when the public user's CIPC parameter is small, while the interference between two users restricts the covert rate when the public user’s CIPC parameter is relatively large.

**Acknowledgement:** This work has been supported by the National Natural Science Foundation of China (no. 62071486 and no. 61771487).

One or more of the Figures in this Letter are available in colour online.

© 2021 The Authors. Electronics Letters published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

Received: 14 December 2020  Accepted: 16 February 2021
doi: 10.1049/ell2.12132

**References**

1. Liu, Y., et al.: Non-orthogonal multiple access for 5G and beyond. *Proc. of IEEE* **105**(12), 2347–2381 (2017)
2. Sun, X., et al.: Secure transmissions in millimeter wave SWIPT UAV-based relay networks. *IEEE Wireless Commun. Lett.* **3**, 1–1 (2019)
3. Xiang, Z., et al.: Secure transmission design in HARQ assisted cognitive NOMA networks. *IEEE Trans. Inf. Forensics Security* **15**, 2526–2541 (2020)
4. Xiang, Z., et al.: Secure transmission in HARQ-assisted non-orthogonal multiple access networks. *IEEE Trans. Inf. Forensics Security* **15**, 2171–2182 (2020)
5. Yan, S., et al.: Low probability of detection communication: Opportunities and challenges. *IEEE Wireless Commun.* **26**(5), 19–25 (2019)
6. Bash, B.A., Goecckel, D., Towsley, D.: Limits of reliable communication with low probability of detection on AWGN channels. *IEEE J. Sel. Areas Commun.* **31**(9), 1921–1930 (2013)
7. Sobers, T.V., et al.: Covert communication in the presence of an unformed jammer. *IEEE Trans. Wireless Commun.* **16**, 6193–6206 (2017)
8. Tao, L., et al.: Covert communication in downlink NOMA systems with random transmit Power. *IEEE Wireless Commun. Lett.* **9**(11), 2000–2004 (2020)
9. Jiang, Y.E., et al.: Covert communications in D2D underlaying cellular networks with power domain NOMA. *IEEE Syst. J.* **14**(3), 3717–3728 (2020)
10. Hu, J., et al.: Covert wireless communications with channel inversion power control in rayleigh fading. *IEEE Trans. Veh. Technol.* **68**(12), 12135–12149 (2019)

![Figure 1](image1.png)  
*Fig. 1 Minimum detection error probability $\xi^\ast$ versus $Q_2$ with different values of $Q_1$*

![Figure 2](image2.png)  
*Fig. 2 Maximum covert rate $R^\ast_2$ versus $Q^{\text{max}}$ subject to different covert constraints with a fixed value of $R_{\text{w}} = 3$*