Covert Communication with A Full-Duplex Receiver Based on Channel Distribution Information

Tingzhen Xu, Ling Xu, Xiaoyu Liu, Zaoyu Lu

1School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, Jiangsu, China

Emails:{tingzhen.xu, xuling, xiaoyu.liu}@njust.edu.cn, Lu_zaoyu@163.com

Abstract—In this work, we consider a system of covert communication with the aid of a full-duplex (FD) receiver to enhance the performance in a more realistic scenario, i.e., only the channel distribution information (CDI) rather than channel state information (CSI) is known to a warden. Our work shows that transmitting random AN can improve the covert communication with the infinite blocklength. Specifically, we jointly design the optimal transmit power and AN power by minimizing the outage probability at Bob, and we find that the outage probability decreases and then increases as the maximum allowable AN power increases. Intuitively, once AN exceeds an optimal value, the performance will become worse because of the self-interference. The simulation results also show that the performance behaviors of CDI and CSI are different. When Willie only knows CDI, there is an optimal AN power that minimizes Bob’s outage probability. However, when Willie knows CSI, the outage probability monotonically decreases with AN power.

Index Terms—full-duplex, artificial noise, channel distribution information.

I. INTRODUCTION

Privacy and security of information are vital in wireless communications since the information is transmitted through public links [1]–[3]. The most common method to ensure the security of information is protecting the content of messages like the traditional encryption technology [4]. However, sometimes exposing the location information can be deadly. For example, the commander’s position cannot be known to the enemy in a war, otherwise the army will lose a leader. So hiding the existence of the transmitter or communication has become significant. Such scenarios require covert communication to ensure the low probability of being detected by the warden.

The fundamental limits of covert communication in different channels, called the square root law (SRL), have been proved in [5]. The SRL gives the number of bits that can be transmitted. Besides the analysis of infinite blocklength, the effect of finite blocklength on covert communications was investigated in [6], [7].

A full-duplex (FD) receiver can help achieve a better performance of covert communication compared with adding an external jammer for the fact that a system with an external jammer may cause several issues, such as mobility [8]. The most works about covert communication are under the premise that the channel state information (CSI) of all channels are known to the transmitter. However, in practice, the warden cannot exactly know the channel information. For the reasons above, this work considers a system with a FD receiver to transmit the artificial noise (AN) to the warden Willie in a more realistic scenario (i.e., only the channel distribution information (CDI) is known to Willie) [9] and draws some conclusions.

II. SYSTEM MODEL

We consider a system of covert communication in Rayleigh fading channel. System model is shown in Fig. 1. Alice (a) tries to communicate with Bob (b) covertly and reliably under the supervision of Willie (w), who has to decide whether Alice is transmitting or not. We assume that Alice and Willie are equipped with a single antenna each, while Bob is equipped with two antennas, with one receiving messages and another transmitting AN in order to disturb Willie’s receive power. We assume that the average symbol transmit power of Bob $P_b$ is subject to a simple distribution, i.e., the uniform distribution. More complex distributions of $P_b$ will be discussed in future studies. The probability density function (PDF) of $P_b$ is given by.

\[
 f_{P_b}(y) = \begin{cases} 
 \frac{1}{P_{b_{\text{max}}}}, & 0 \leq P_b \leq P_{b_{\text{max}}}, \\
 0, & \text{otherwise},
\end{cases}
\]

where $P_{b_{\text{max}}}$ is the maximum allowable AN power.

In Rayleigh channel, we consider a more realistic situation. Assume that Willie only knows the CDI of Alice-Willie
channel, but we still assume that Alice and Bob know CSI of Alice-Bob channel. The receive signal of Willie is given by

$$y_w[i] = \begin{cases} \sqrt{P_a \sigma_{bw}^2} h_{bw} v_b[i] + n_w[i], & H_0, \\ \sqrt{P_a \sigma_{aw}^2} h_{aw} x[i] + \sqrt{P_b \sigma_{bw}^2} h_{bw} v_0[i] + n_w[i], & H_1. \end{cases}$$

(2)

where $P_a$ and $P_b$ are the transmit power at Alice and Bob, respectively, $h_j$ represents the channel, $j$ can be $ab, aw, bw, bb$. The mean value of $|h_j|^2$ is $E[|h_j|^2] = \lambda_j$, $x_a$ is the transmit signal at Alice satisfying $E[x_a[i] x_a[i]] = 1$, $i = 1, 2, \ldots, N$, where $i$ is the index of channel uses, $v_b$ is the AN transmitted by Bob satisfying $E[v_b[i] v_b[i]] = 1$, and $n_w[i] \sim CN(0, \sigma_w^2)$ is the AWGN at Willie with variance $\sigma_w^2$, $\sigma_{aw}^2$ and $\sigma_{bw}^2$ representing the distances of Alice-Willie and Bob-Willie, respectively, where $\alpha$ is the path loss exponent. When the number of channel uses $N \to \infty$, the average symbol received power is

$$T_w = \begin{cases} \sqrt{P_a \sigma_{bw}^2} |h_{bw}|^2 + \sigma_w^2, & H_0, \\ \sqrt{P_a \sigma_{aw}^2} |h_{aw}|^2 + \sqrt{P_b \sigma_{bw}^2} |h_{bw}|^2 + \sigma_w^2, & H_1. \end{cases}$$

(3)

Willie has to make a decision between $H_0$ and $H_1$, where null hypothesis $H_0$ means Alice does not transmit, the alternate hypothesis $H_1$ means Alice does transmit covert message to Bob.

### III. Detection Performance of Willie

We calculate the false alarm rate (FAR) $P_{FA} \triangleq P(D_1 | H_0)$ and miss detection rate (MDR) $P_{MD} \triangleq P(D_0 | H_1)$ as the metrics to measure the performance of Willie, where $D_0$ and $D_1$ are decisions made by Willie in favor of $H_0$ and $H_1$, respectively.

**Lemma 1:** The FAR and MDR at Willie are given by

$$P_{FA} = \begin{cases} 1, & \tau \leq \rho_1, \\ P_1, & \tau > \rho_1 \end{cases}$$

(4)

$$P_{MD} = \begin{cases} 0, & \tau \leq \rho_2, \\ P_2, & \tau > \rho_2 \end{cases}$$

(5)

where $P_1$ and $P_2$ are given by (7) and (8), respectively.

$$P_1 = \frac{\rho_1}{\lambda_{bw} P_b^{\text{max}}}, \quad \rho_1 = \sigma_w^2 + \frac{\lambda_{bw} P_b^{\text{max}} \alpha_{aw}}{N \sigma_{aw}^2},$$

(6)

$$P_2 = \frac{\rho_2}{\lambda_{aw} P_a^{\text{max}}}, \quad \rho_2 = \sigma_w^2 + \frac{\lambda_{bw} P_b^{\text{max}} \alpha_{bw}}{N \sigma_{bw}^2}.$$

**Proof:**

$$P_{FA} = P_y \left( \frac{P_a}{\rho_{bw}^2} |h_{bw}|^2 + \frac{\sigma_w^2}{\tau} > \gamma |H_0 \right)$$

$$= \int_0^{\rho_{bw}^2} \frac{1}{P_{bw}^{\text{max}}} \int_0^{\gamma} \frac{1}{\lambda_{bw}} e^{-\frac{1}{\lambda_{bw}} \tau} d\tau$$

$$= e^{-\gamma} \text{E}(\gamma) \triangleq P_1,$$

where $\gamma = \frac{(\sigma_w^2 - \tau) \rho_{bw}}{\lambda_{bw} P_b^{\text{max}}}$. $\text{E}(x) = \int_{-\infty}^{x} \frac{e^t}{t} dt$ is the exponential integral function.

$$P_{MD} = P_y \left( \frac{P_a}{\rho_{aw}^2} |h_{aw}|^2 + \frac{P_b}{\rho_{bw}^2} |h_{bw}|^2 + \sigma_w^2 < \gamma |H_1 \right)$$

$$= \int_0^{\rho_{bw}^2} \int_0^{\gamma} \frac{1}{\lambda_{bw}} e^{-\frac{1}{\lambda_{bw}} \tau} d\tau$$

$$= 1 - \frac{d}{g} \left( \frac{g d - \gamma}{d - \gamma} \right) \triangleq P_2,$$

where

$$d = \frac{\rho_{bw}^2}{\lambda_{bw} P_b^{\text{max}}}, \quad g = \frac{\rho_{aw}^2}{\lambda_{bw} P_a^{\text{max}}}.$$

(9)

with constraint

$$d > g.$$ 

The derivation of $\rho_1 \sim \rho_4$ please refer to Appendix $A$.  

**Theorem 1:** Consider the model and metrics above, the detection error probability at Willie is given by

$$\xi = \begin{cases} 1, & \tau \leq \rho_1, \\ P_1, & \rho_1 < \tau \leq \rho_2, \\ P_1 + P_2, & \tau > \rho_2. \end{cases}$$

(10)

The optimal threshold for Willie’s detection is

$$\tau^* = [\rho_2, +\infty).$$

(11)

**Proof:** As per (6), in order to represent $\xi$, we need to discuss the relationship between $\rho_1$ and $\rho_2$. When $\rho_1 < \rho_2$, we can easily get $\xi = 1 + P_2$ in interval $[\rho_2, \rho_1]$. Thus the situation of $\rho_1 > \rho_2$ is impossible. For $\rho_2 \geq \rho_1$, we have the expression as shown in (10).

For $\rho_1 < \tau \leq \rho_2$, $\xi$ decreases with $\tau$. When $\tau > \rho_2$, the first derivative of $\xi$ with respect to $\tau$ is

$$\xi'_\tau = dEi(d(\sigma_w^2 - \tau)) + d \ln \left( \frac{d}{d - g} \right) e^{g(\sigma_w^2 - \tau)}.$$

(12)

After some calculations and analysis, we can find $\xi = P_1 + P_2$ decreases and then increases as $\tau$ increases, thus the minimum $\xi$ is in the interval of $\tau > \rho_2$.  


IV. PERFORMANCE OF COVERT COMMUNICATION

Next, we analyze the performance of Bob. According to [10], we have the outage probability of Bob given by

$$P_{out} = 1 - \lambda_{ab} e^{-\frac{\sigma_w^2}{\lambda_{ab}} \ln \left( \frac{\mu h \lambda_{ab} P_{b}^{\text{max}} + \lambda_{ab}}{\mu h \lambda_{ab} P_{b}^{\text{max}}} \right) - \ln (\lambda_{ab})}$$

(13)

where $\mu = \frac{2}{N_0}$, $h$ is the self-interference cancellation coefficient at Bob, $R$ is the transmission rate from Alice to Bob. The problem that minimizes the outage probability $P_{out}$ under the covert constraint is given by

$$\begin{align*}
(P1) & \quad \min_{P_a, P_b^{\text{max}}} P_{out} \\
& \quad \text{s.t. } \xi^* \geq 1 - \epsilon,
\end{align*}$$

(14)

where $\xi^* = P_1 + P_2$. Here we use $\xi^*$ for the fact that the minimum $\xi$ is in $\{P_2, \infty\}$.

**Theorem 2:** For any given covert constraint $\epsilon$, the optimal $P_a$, for fixed $P_b^{\text{max}}$, to minimize the effective covert rate is

$$P_a^* = \frac{p_0^{\text{aw}}}{g_2 \lambda_{aw}},$$

(16)

And the globally optimal $P_b^{\text{max}}$ is

$$P_b^{\text{max}*} = \arg \min_{P_b^{\text{max}}} P_{out}^*,$$

(17)

where $g_2$ is given in [24], $P_{out}^*$ is explained later.

**Proof:** $P_{out}^*$ decreases with $P_a$, and $\xi^*$ first increases then decreases as $P_a$ increases. We omitted the specific proof due to the limited length of paper. Thus we have the optimal $P_a$ is the solution to $\xi^* = 1 - \epsilon$. We define

$$M = (\sigma_w^2 - \tau) d E \left( e^{(\sigma_w^2 - \tau) d} - e^{(\sigma_w^2 - \tau) d} - \epsilon \right),$$

(18)

then the equation $\xi^* = 1 - \epsilon$ becomes

$$- \frac{d e^{(\sigma_w^2 - \tau) d}}{g} \ln \left( \frac{d}{d - g} \right) = M,$$

(19)

For convenience of calculation and analysis, we approximate the exponential function and the logarithm function with the second and first order Taylor expansion, respectively. Then

$$- \frac{d}{g} \left[ 1 + (\sigma_w^2 - \tau) g + \frac{g^2 (\sigma_w^2 - \tau)^2}{2} \right] \times \frac{d}{d - g} = M$$

(20)

with constraint $2 P_b^{\text{max}} \lambda_{aw} r_a < P_a \lambda_{aw} r_a$. To ensure the equation have two positive real roots, it must satisfy

$$\begin{align*}
\Delta & \geq 0, \\
g_1 + g_2 & > 0, \\
g_1 \times g_2 & > 0,
\end{align*}$$

(21)

where

$$\Delta = M^2 - d^2 (\tau - \sigma_w^2) + M (4 - 2d \tau + 2d \sigma_w^2).$$

(22)

$g_1$, $g_2$ are the corresponding two roots. That is

$$\begin{align*}
M & < \min \left\{ \frac{1}{2} d^2 (\tau - \sigma_w^2)^2, d (\tau - \sigma_w^2)^2 \right\}, \\
M^2 - d^2 (\tau - \sigma_w^2)^2 + M (4 - 2d \tau + 2d \sigma_w^2) & \geq 0.
\end{align*}$$

(23)

Solve quadratic equation of (20), we get

$$g_{1, 2} = \frac{d^2 (\tau - \sigma_w^2)^2 - d M \pm \sqrt{\Delta}}{d^2 \sigma_w^2 (\sigma_w^2 - 2 \tau) + d^2 \tau^2 - 2 M},$$

(24)

As per [9], we have $P_a^1$, $P_a^2$ and $P_a^1 < P_a^2$. To achieve a larger $P_a$, we keep $P_a^2$ and get the optimal $P_a$ for fixed $P_b^{\text{max}}$ is $P_a^1 = P_a^2$. Substituting $P_a^1$ into $P_{out}^*$, we will obtain $P_{out}^1$. Then $P_b^{\text{max}*}$ is derived from (17).

V. SIMULATIONS AND DISCUSSIONS

In this section, we evaluate the performance of the whole analysis. For simplicity, we suppose all the distance $d$ are the same. It indicates that the transmission.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{fig2.png}
\caption{$P_{out}$ vs. $P_b^{\text{max}}$, where $\tau = 2$, $\epsilon = 0.2$, $\lambda_{aw} = 0.8$.}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{fig3.png}
\caption{$P_{out}^1$ vs. $P_b^{\text{max}}$ under CDI and CSI, where $\sigma_w^2 = \sigma_b^2 = 0$ dBm, $\epsilon = 0.3$, $R = 1$, $h = 0.1$, $\tau = 3$, $\lambda_{aw} = 0.5$.}
\end{figure}

Fig. 2 shows the curves of $P_{out}^1$ versus $P_b^{\text{max}}$ when Willie only knows CDI of Alice-Willie channel. It indicates that there indeed exits an optimal $P_b^{\text{max}}$ that minimizes the outage probability of Bob under the covert constraint. We observe that $P_{out}^1$ first decreases then increases with $P_b^{\text{max}}$ since the AN is helpful for the transmission at first, but when the AN is too large, the performance will be worse due to the self-interference. It also shows that $P_b^{\text{max}*}$ increases as $\sigma_w^2$ increases due to the fact that increasing $\sigma_w^2$ means Alice can transmit more power which leads to the larger $P_b^{\text{max}*}$ to cover the transmission.

To show the differences between the cases that Willie only knows CDI and CSI, we plot Fig. 3 $P_{out}$ versus $P_b^{\text{max}}$.
for Willie knows CSI. From Fig. 3, we know that $P_{\text{out}}^1$ monotonically decreases with $P_b^{\text{max}}$ for the fact that the increasing of $P_b^{\text{max}}$ will only benefits Bob’s performance when there is no uncertainty at Willie. At the same time, $P_{\text{out}}^1$ decreases with $\epsilon$ because that the larger $\xi$ at Willie means the better performance at Bob. By comparing the two figures, we can easily known that under the same conditions, the outage probability at Bob is smaller in the scenario that Willie only knows CDI than the scenario that Willie knows CSI. It means that the former is more beneficial than the latter.

VI. Conclusions

In this work, we mainly analyze the performance of covert communication under CDI with the aid of a FD receiver. We jointly design $P_a$ and $P_b^{\text{max}}$ to minimize the outage probability. We first optimize $P_a$ by fixing $P_b^{\text{max}}$ and then substitute this $P_a$ into the objective function to obtain $P_b^{\text{max}}$. Our work shows that transmitting random AN can help improve the covert performance in the case of infinite blocklength. We have found that $P_b^{\text{max}}$ increases with $\sigma_w^2$, i.e., if the receive noise variance $\sigma_w^2$ at Willie increases, then Alice can increase its transmit power $P_a$. This will require that the AN power transmitted by Bob should increase accordingly. Besides, the performance of CDI and CSI is compared. It’s consistent with our intuition, i.e., the scenario that Willie only knows CDI performs better than the scenario that Willie knows CSI for covert transmission.

Appendix A

Derivation of $\rho_1, \rho_2$

Apparently, when Willie’s detection threshold is smaller than the minimum power of interference-plus-noise, the $P_{FA}$ equals to one according to the definition of false alarm rate, i.e.,

$$\tau \leq \sigma_w^2 + \frac{P_b^{\text{max}}(\min(|h_{bw}|^2))}{P_{bw}}$$

(25)

We set

$$Z = \min\{|h_1|^2, |h_2|^2, \ldots, |h_N|^2\}$$

(26)

where random variable $X = \{|h_i|^2, 1 \leq i \leq N\}$, each $|h_i|^2$ is independent and identically distributed. $X \sim E(\lambda)$ and $\lambda = \frac{1}{\lambda_{bw}}$. So we have

$$F_X(x) = \begin{cases} 0, & x < 0, \\ 1 - e^{-\lambda x}, & x \geq 0. \end{cases}$$

(27)

Then we get

$$F_Z(z) = P(Z \leq z) = 1 - P(Z > z) = 1 - \prod(1 - P(|h_i|^2 \geq z)) \cdots P(|h_N|^2 \geq z)$$

$$= 1 - \prod(1 - P(|h_i|^2 \leq z)) \cdots [1 - P(|h_N|^2 \leq z)]$$

$$= 1 - [e^{-\lambda z}]^N$$

(28)

So the PDF is

$$f_Z(z) = N \lambda (e^{-\lambda z})^N$$

(29)

The expectation is

$$E(z) = \int_0^{+\infty} z N \lambda (e^{-\lambda z})^N dz = \frac{1}{\lambda N}$$

Finally, $\rho_1$ is derived. And the derivation of $\rho_2$ is similar to $\rho_1$.

References

[1] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, “Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays,” IEEE Access, vol. 5, pp. 1658–1667, Jan. 2017.
[2] F. Shu, X. Wu, J. Hu, J. Li, R. Chen, and J. Wang, “Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array,” IEEE J. Sel. Areas Commun., vol. 36, no. 4, pp. 890–904, Apr. 2018.
[3] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, “Covert communication achieved by a greedy relay in wireless networks,” IEEE Trans. Wireless Commun., vol. 17, no. 7, pp. 4766–4779, Jul. 2018.
[4] J. H. Cheon and J. Kim, “A hybrid scheme of public-key encryption and somewhat homomorphic encryption,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 5, pp. 1052–1063, May 2015.
[5] B. A. Bash, D. Goeckel, and D. Towsley, “Limits of reliable communication with low probability of detection on AWGN channels,” IEEE J. Sel. Areas Commun., vol. 31, no. 9, pp. 1921–1930, Sept. 2013.
[6] S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, “Delay-intolerant covert communications with either fixed or random transmit power,” IEEE Trans. Inf. Forensics Security, vol. 14, no. 1, pp. 129–140, Jan. 2019.
[7] S. Yan, B. He, Y. Cong, and X. Zhou, “Covert communication with finite blocklength in AWGN channels,” in Proc. IEEE ICC, May 2017, pp. 1–6.
[8] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, “Covert communication in the presence of an uninform jammer,” IEEE Trans. Wireless Commun., vol. 16, no. 9, pp. 6193–6206, Sept. 2017.
[9] S. Lee and R. J. Baxley, “Achieving positive rate with undetectable communication over AWGN and rayleigh channels,” in Proc. IEEE ICC, Jun. 2014, pp. 780–785.
[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,” in Proc. IEEE ICC, May 2018, pp. 1–6.