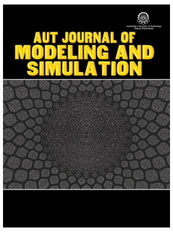

AUT Jouranl of Modeling and Simulation

AUT J. Model. Simul., 52(1) (2020) 31-38
DOI: 10.22060/miscj.2019.15496.5135

Covert Transmission with Antenna Selection and Using an External Jammer

Morteza Sarkheil[1], Paeiz Azmi[1*], Moslem Forouzesh[1], Ali Kuhestani[2]

[1] Department of ECE, Tarbiat Modares University, Tehran, Iran
[2] Department of ECE, Qom University of Technology, Qom, Iran

ABSTRACT: This paper adopts the antenna selection technique to enhance the covert rate in a wireless communication network comprised of a source, a destination, an external jammer and an eavesdropper. In the covert communication, the level of transmit power is low and hence a source with multiple antennas can be adopted to send the information toward the single antenna destination while concurrently, the jammer transmits an artificial noise signal. For this system model, we consider a scenario where the source is forced to select one or several of its antennas to transmit its confidential information due to its limited RF chains. Furthermore, we consider two different jamming scenarios to support our covert communication: 1) The destination is unable to cancel the jamming signal; 2) The destination can subtract the jamming signal. For such a communication network, our aim is to maximize the covert rate subject to power constraint and covert communication requirement. In the first scenario, the optimization problem is non-convex, and hence, it can be solved through using Difference of Convex function (DC) method while the optimization problem of the second scenario is intrinsically convex. Our numerical results show that the higher the number of selected antennas at the transmitter, the higher the covert rate will be achieved.

Review History:

Received: Dec. 30, 2018
Revised: Apr. 10, 2019
Accepted: May, 25, 2019
Available Online: Jun. 15, 2020

Keywords:

Covert communication
antenna selection
external jammer.

1- INTRODUCTION

Security is a critical and important subject in wireless communications networks. This is because the broadcast nature of wireless networks permits to the unauthorized nodes to access the contents of the confidential messages [1]. Physical layer security as a new solution to enhance the confidentiality of wireless communications has attracted a lot of interest [2]--[4]. Physical layer secure transmission is provisioned by intelligently exploiting the time varying properties of fading channels, instead of relying on conventional cryptographic techniques. This approach uses signal processing and encoding techniques at the physical layer, to improve the quality of the received signal at illegitimate receivers compared with the unauthorized users. Toward this end, the jamming signal can be used to enhance the physical layer security. Typically, there are two main types of jamming signal to enhance the security of wireless networks [4], [5]: 1) Friendly jamming (FJ) scenario where the jamming signal is known at the legitimate receiver, 2) Gaussian noise jamming (GNJ) where the jamming signal is unknown at the legitimate receiver[5]-[7]. It should be noted that FJ provides better secrecy performance compared with GNJ because when FJ is used, legitimate receiver can cancel the jamming signal. However, GNJ is more simple compared with FJ scenario. This reveals the trade-off between secrecy performance and complexity of the network.

In some communication networks, low probability of detection (LPD) or covert communication is essential for information transmission over electromagnetic and acoustic channels [8]. For military applications, LPD is interest when the transmitter wishes to remain undetected, or when the knowledge of communication may point to the presence of a receiver. As such, in covert communication only the detection capability of an eavesdropper is considered, i.e., an eavesdropper need not be able to actually decode the communication signal. In other words, the covert communication keeps military forces from possible attacks [9]. In recent years, some few works have investigated the covert communication in different wireless communication networks [9]--[14].

In this paper, we take into account the power allocation problem of a wireless communication network, where a multiple antenna source transmits its confidential message to a single antenna destination in the presence of a passive eavesdropper. To covert the communication against the eavesdropping attack, a single antenna external jammer is employed. For this communication network, we investigate two different jamming scenarios to support covert communication: 1) The destination is unable to cancel the jamming signal, i.e., we have FJ, 2) The destination can subtract the jamming signal, i.e., we have GNJ. We consider

*Corresponding author's email: pazmi@modares.ac.ir

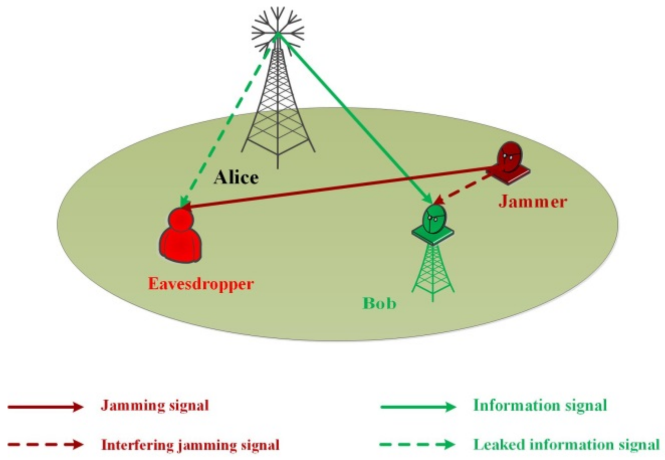

Fig.1. Our MISO system model in the presence of an external jammer and a passive eavesdropper

a realistic scenario where the number of RF chains at the source may be fewer than the number of source's antennas. Instead of selecting the antennas randomly, we propose to select the best antennas to transmit the information signal toward the destination. For such a network, we formulate the power allocation between the source and jammer that maximizes the instantaneous covert rate while concurrently hiding the communication against the passive eavesdropping attack. Since the optimization problem of GNJ scenario is non-convex, we exploit difference of concave (DC) approach to convert it to a convex optimization problem. For the FJ scenario, we observe that the optimization problem is convex. We also obtain closed-form solutions for the optimal power threshold from the eavesdropper's viewpoint. Our numerical examples show that by increasing the number of selected antennas at the transmitter the covert rate is increased. Furthermore, the impact of the distance between the transmitter and the eavesdropper on the achievable covert rate is more than the impact of the distance between the transmitter and the receiver.

2- SYSTEM MODEL

As shown in Fig. 1, the system model under consideration is a multi-input single-output (MISO) wireless network consisting of an MT antenna transmitter (Alice), a single antenna jammer, a single antenna receiver (Bob), and a single antenna eavesdropper (Eve). For this system model, assume Alice selects several antennas to send information signal. In this system model, we consider two scenarios for sending jamming signal. 1) FJ, in this scenario, Bob has the ability to cancel the jamming signal. 2) GNJ, in this scenario, Bob does not know the jamming signal and then cannot cancel the jamming signal. In this scenario, we assume the communication channels follow the slow fading. Moreover, the fading coefficients have Rayleigh distribution. Alice is unaware of Eve's channel state information (CSI) and only knows the distance between itself and Eve and its channel distribution information (CDI). We also assume that the jammer knows the distance between itself and Eve. The distance between Alice and Bob, Alice and Eve, the jammer and Bob and the jammer and Eve are defined as D_{ab} , D_{ae} , D_{jb} and D_{je} , respectively. The information signal and the jamming signal denoted by $\mathbf{x_s} = \left[x_s^{\,1}, x_s^{\,2}, .., x_s^{\,m}\right]$ and $\mathbf{x_j} = \left[x_j^{\,1}, x_j^{\,2}, .., x_j^{\,m}\right]$, respectively, where m shows the number of transmit symbols in each time slot.

3- COVERT COMMUNICATION

In the covert communication, our aim is to send a message from Alice to Bob secretly such that Eve will not be notified of this communication, i.e., based on the level received energy. The Eve decides about the presence or absence of signal transmission by Alice. In this scenario, notation Ω_0 states that Alice does not transmit the information signal to Bob, while Ω_1 states that the Alice transmits the information signal to Bob. Notation P_{MD} is the probability that Alice sends its information signal but Eve decides on the absence of communication. Furthermore, P_{FA} is the probability that Alice is silent but Eve decides on the presence of communication between Alice and Bob. The covert communication between Alice and Bob is established when the following condition holds [9]

$$\underset{m\to\infty}{P_{FA}} + P_{MD} \geq 1-\varepsilon, \tag{1}$$

where $1-\epsilon$ is the lower bound of the probability of detection error at Eve. The received signal at node $k \in Bob, Eve$, is as follows

$$y_k = \begin{cases} \dfrac{\sqrt{p_j}\, h_{jk} x_j}{D_{jk}^{\beta/2}} + n_k, & \Omega_0, \\ \dfrac{\sqrt{p_j}\, h_{jk} x_j}{D_{jk}^{\beta/2}} + \dfrac{\sqrt{p_s}\, w^H h_{ak} x_s}{D_{ak}^{\beta/2}} + n_k, & \Omega_1, \end{cases} \tag{2}$$

where $\mathrm{p_s}$ and p_j are the allocated power for the information signal and the jamming signal, respectively, such that $p_s = \alpha P_{total}$ and $p_s = \alpha P_{total}$, where α is the power allocation factor. It is worth noting that the total power consumption constraint provides a guideline for the power allocation of the Alice and the jammer. This approach has been widely exploited in the literature for both performance analysis and network optimization design [7], [11], [14]. Furthermore, in (3), β is the path-loss exponent and the complex Gaussian channel vector from Alice to node k and jammer to node k are defined by $\mathbf{h_{ak}}$, and h_{jk}, respectively. Note that $\mathbf{w} = \frac{\mathbf{h_{ab}}}{\backslash \mathbf{h_{ab}} \backslash}$ represents the maximum ratio transmission (MRT) beamformer coefficients at the source in which $\mathbf{h_{ab}}$ is the channel coefficient between Alice and Bob}. n_k is the white Gaussian noise received at node k with the distribution of $n \sim CN(0, \sigma_k^2)$. The decision of Eve is based on the energy of the received signal. Eve decides on the state Ω_1 if $\frac{Y_e}{m} \geq V$. Otherwise, Eve decides on the state Ω_0. V is the threshold of decision and Y_e is the energy of the received signal which is $Y_e = \sum_{l=1}^{m} |y_k^l|^2$ Accordingly, P_{FA} and P_{MD} can be written, respectively, as

$$\begin{aligned} P_{FA} &= P((\sigma_e{}^2 + \gamma)\frac{\chi^2{}_{2m}}{m} \geq V \mid \Omega_0), \\ P_{MD} &= P((\sigma_e{}^2 + \gamma)\frac{\chi^2{}_{2m}}{m} \leq V \mid \Omega_1), \end{aligned} \tag{3}$$

where χ_{2m}^2 is a random variable with chi-squared distribution with \$2m\$ degrees of freedom. For large number of transmit symbols in each time slot, $m \longrightarrow \infty$, we have $\frac{\chi_{2m}^2}{m} \to 1$. Therefore, (3) and (4) can be simplified as

$$\begin{aligned} P_{FA} &= P((\sigma_e{}^2 + \gamma) \geq V \mid \Omega_0), \\ P_{MD} &= P((\sigma_e{}^2 + \gamma) \leq V \mid \Omega_1). \end{aligned} \tag{4}$$

We note that the received signal has the distribution of $y_k^l \sim CN(0, (\sigma^2 + \gamma))$, where γ is defined as follows

$$\gamma = \begin{cases} \frac{P_j}{D_{ae}^{\beta}} |h_{je}|^2, & \Omega_0, \\ \frac{P_j}{D_{je}^{\beta}} |h_{je}|^2 + \frac{P_s}{D_{ae}^{\beta}} \|w^H h_{ae}\|^2, & \Omega_1. \end{cases} \tag{5}$$

In (5), $\mathrm{h_{je}}$ and h_{ae} are zero-mean Gaussian random variables with unit variances. Thus, $|h_{je}|^2$ has an exponential distribution with the parameter $\lambda = 1$. Therefore, for the assumption of Ω_0, γ has an exponential distribution with the parameter of $\lambda = \frac{1}{\phi_0}$. According to [15], the summation of two exponential distributions x and y with parameters λ_1 and λ_2 is given by

$$f_{x+y}(\gamma) = \frac{\lambda_1 \lambda_2}{\lambda_2 - \lambda_1}[e^{-\lambda_1 \gamma} - e^{-\lambda_2 \gamma}]U(\gamma) \tag{6}$$

where $U(\gamma)$ is the step function. Furthermore, since the channel coefficients have complex Gaussian distribution, according to [16], γ has the following distribution

$$f(\gamma) = \begin{cases} \frac{1}{\phi_0} e^{-\frac{\gamma}{\phi_0}}, & \gamma \geq 0 \quad \Omega_0, \\ \frac{1}{\phi_0 - \phi_1}(e^{-\frac{\gamma}{\phi_0}} - e^{-\frac{\gamma}{\phi_1}}), & \gamma \geq 0 \quad \Omega_1, \end{cases} \tag{7}$$

where $\phi_1 = \frac{P_s}{D_{ae}^{\beta}}$ and $\phi_0 = \frac{P_j}{D_{je}^{\beta}}$. By combining (4), (5), (6) and (7), we obtain

$$P_{FA} = \begin{cases} e^{-\frac{(V - \sigma_e^2)}{\phi_0}}, & V - \sigma_e^2 \geq 0, \\ 1, & V - \sigma_e^2 \leq 0, \end{cases} \tag{8}$$

and

$$P_{MD} = \begin{cases} \Gamma, & V - \sigma_e^2 \geq 0, \\ 0, & V - \sigma_e^2 \leq 0, \end{cases} \tag{9}$$

where $\Gamma = \frac{1}{\phi_0 - \phi_1}(\phi_1 e^{-\frac{(V - \sigma_e^2)}{\phi_1}} - \phi_0 e^{-\frac{(V - \sigma_e^2)}{\phi_0}} + \phi_0 - \phi_1)$.

3-1- Eavesdropper's error

The Eve's error is defined as $\mathrm{P_{MD}} + \mathrm{P_{FA}}$. In this scenario, we consider the worst case scenario where Eve has an optimal threshold. The optimal threshold of Eve is minimum decision error. Therefore, we can write

$$P_{MD} + P_{FA} = \begin{cases} e^{-\frac{(V - \sigma_e^2)}{\phi_0}} + \Lambda_1, & V - \sigma_e^2 \geq 0, \\ 1, & V - \sigma_e^2 \leq 0, \end{cases} \tag{10}$$

where $\Lambda_1 = \frac{1}{\phi_0 - \phi_1}(\phi_1 e^{-\frac{(V - \sigma_e^2)}{\phi_1}} - \phi_0 e^{-\frac{(V - \sigma_e^2)}{\phi_0}} + \phi_0 - \phi_1)$. The minimum Eve's error i.e., $\min_V(P_{FA} + P_{MD})$ is calculated in Appendix A.

3-1- Cover rate

The covert rate at Bob is defined as

$$R = \log(1 + \frac{\alpha P_{total} |h_{ab}|^2 D_{jb}^{\beta}}{D_{jb}^{\beta} D_{ab}^{\beta} \sigma_b^2 + (1 - \alpha) P_{total} |h_{jb}|^2 D_{ab}^{\beta}}). \tag{11}$$

Algorithm 1 Iterative power allocation algorithm

```
1: Initialization: Set $\mu = 0$ ( is the iteration number) and initialize to $\alpha(0)$
2: Set $\alpha = \alpha(\mu)$ ,
3: Solve (21) and set the result to $\alpha(\mu+1)$
4: If $|\alpha(\mu+1) - \alpha(\mu)| \le \theta$
       stop
   else
       set $\mu = \mu + 1$ and go back to step 2
```

Our goal is to increase the covert rate. To this end, from the M_T antennas, N_D of antennas with the highest channel coefficients between Alice and Bob are selected to send the information. As such, the corresponding antennas are selected based on the following criterion

$$h_{ab} = \mathrm{X}_{N_D}(sort(H_{M_T \times 1})), \tag{12}$$

where $\mathrm{sort}(v)$ arranges the v elements in descending order and $\mathrm{X}_i(u)$ selects first i elements of u. According to (12), we can increase the covert rate by selecting appropriate antennas for sending information signal1[1]. The proposed antenna selection technique, not only increases the covert rate, but also reduces the hardware equipment at Alice, including amplifiers and mixers, and also reduces the network complexity and overhead.

4- OPTIMIZATION PROBLEM

In this paper, our goal is to maximize the covert rate subject to the limitation of transmit power and the covert communication condition. Moreover, in the following, we investigate two different scenarios of FJ and GNJ.

4-1- Gaussian Noise Jamming Scenario

In this scenario, it is assumed that Bob cannot cancel the jamming signal. Therefore, we have the following optimization problem

$$\begin{aligned} &\max_{\alpha}\{R = \log(1 + \frac{\alpha P_{total}\|h_{ab}\|^2 D_{jb}^{\beta}}{D_{jb}^{\beta} D_{ab}^{\beta}\sigma_b^2 + (1-\alpha)P_{total}|h_{jb}|^2 D_{ab}^{\beta}})\}, \\ &s.t \quad C_1 : 0 < \alpha < 1, \\ &\qquad C_2 : \min_{V}(P_{FA} + P_{MD}) \ge 1 - \varepsilon. \end{aligned} \tag{13}$$

After formulating the constraint C_2 (See Appendix B), (13) can be rewritten as follows

$$\begin{aligned} &\max_{\alpha}\{R = \log(1 + \frac{\alpha P_{total}\|h_{ab}\|^2 D_{jb}^{\beta}}{D_{jb}^{\beta} D_{ab}^{\beta}\sigma_b^2 + (1-\alpha)P_{total}|h_{jb}|^2 D_{ab}^{\beta}})\}, \\ &s.t \quad C_1 : 0 < \alpha < 1, \\ &\qquad C_2 : \frac{(1-\alpha)D_{je}^{\beta}}{\alpha D_{je}^{\beta} - (1-\alpha)D_{ae}^{\beta}}\ln(\frac{(1-\alpha)D_{ae}^{\beta}}{\alpha D_{je}^{\beta}}) < ln\varepsilon. \end{aligned} \tag{14}$$

Since the optimization problem (14) is a non-convex one, we rewrite the objective function as Follows

$$\Sigma(\alpha) - \Psi(\alpha) \tag{15}$$

where

$$\begin{cases} \Sigma(\alpha) = log(D_{jb}^{\beta} D_{ab}^{\beta}\sigma_b^2 + (1-\alpha)P_{total}D_{ab}^{\beta}|h_{jb}|^2 \\ \qquad + \alpha P_{total}D_{jb}^{\beta}\|h_{ab}\|^2) \\ \Psi(\alpha) = \log(D_{jb}^{\beta} D_{ab}^{\beta}\sigma_b^2 + (1-\alpha)P_{total}D_{ab}^{\beta}|h_{jb}|^2) \end{cases} \tag{16}$$

To solve the optimization problem, we use the DC method and propose iterative algorithm I. As such, we approximate $\Psi(\alpha)$ as follows [16-19]

$$\Psi(\alpha) \approx \tilde{\Psi}(\alpha) = \Psi(\alpha(\eta-1)) + \nabla^T \Psi(\alpha(\eta-1))(\alpha - \alpha(\eta-1)) \tag{17}$$

where ∇ is the gradient operator and η demonstrates the iteration number. $\nabla^T \Psi(\alpha(\eta-1))$ is calculated as follows

$$\nabla^T \Psi(\alpha(\eta-1)) = \frac{-P_{total}D_{ab}^{\beta}|h_{jb}|^2}{D_{jb}^{\beta} D_{ab}^{\beta}\sigma_b^2 + (1-\alpha(\eta-1))P_{total}D_{ab}^{\beta}|h_{jb}|^2}. \tag{18}$$

[1] In many practical scenarios the eavesdropper is passive, hence, we assume its channel state information (CSI) is not available and Alice has only its channel distribution information (CDI). With this assumption, we do not consider the antenna selection criterion from the eavesdropper viewpoint.

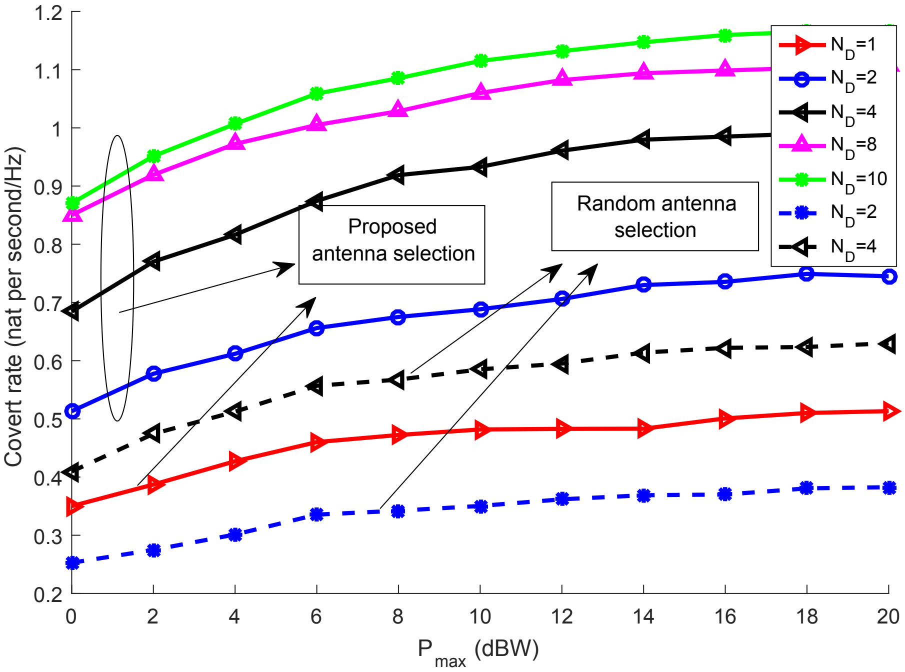

Fig. 2. Covert rate versus the total transmit power.

Finally, (11) can be rewritten as $\Sigma(\alpha)-\tilde{\Psi}(\alpha)$ which is a concave function. C_2 can be convex by using the change of value $T=(1-\alpha)D_{ae}^{\beta}-\alpha D_{je}^{\beta}$. Therefore, we have

$$\begin{aligned}
&\max_{\alpha}\ \Sigma(\alpha)-\tilde{\Psi}(\alpha)\\
&s.t\ C_1: 0<\alpha<1,\\
&\quad C_2: (1-\alpha)D_{ae}^{\beta}\ln(\frac{(1-\alpha)D_{ae}^{\beta}}{\alpha D_{je}^{\beta}})<Tln\varepsilon,\\
&\quad C_3: \alpha D_{je}^{\beta}-(1-\alpha)D_{ae}^{\beta}<T.
\end{aligned} \tag{19}$$

As we mentioned before, we use the DC method to solve the optimization problem. Therefore, (21) is in fact the approximate of (17) after applying the DC method. The optimization problem in (19) is convex because the objective function is concave, C_1 and C_3 are linear, and C_2 is convex[1]. Hence, we can use the available software such as CVX solver to solve the convex optimization problem.

4-1- Friendly Jamming Scenario

In this scenario, it is assumed that Bob can cancel the jamming signal. Hence, we have the following optimization problem

$$\begin{aligned}
&\max_{\alpha}\left\{R=log(1+\frac{\alpha P_{total}\backslash h_{ab}\backslash^{2}}{D_{ab}^{\beta}\sigma_b^2})\right\},\\
&s.tC_1,C_2.
\end{aligned} \tag{20}$$

In (22), the objective function is convex. Therefore, we can use the CVX solver to solve it. In addition, we can convert constraints C_1 and C_2 to convex constraints as in the previous scenario.

5- SIMULATION RESULTS

In this section, our aim is to evaluate the secrecy performance of the proposed secure transmission scheme. For simplicity and without loss of generality, we assume that Alice, Bob, the jammer and the passive Eve are located at the positions (-2.5, 2.5), (2.5, 2.5), (2.5,-2.5) and (-2.5,-2.5), respectively. Unless otherwise stated, the network parameters are: number of antennas at Alice M_T=10, number of antenna at Alice that are selected N_D=6, $\varepsilon=0.1$, $1-\varepsilon s$ is lower bound of error detection probability, and the path-loss exponent $\beta=2$.

Fig. 2 shows the effect of the transmit power sent by Alice on the covert rate. According to simulation results, if the transmit power increases, the covert rate increases. However, as can be seen, the covert rate ceiling is appeared at high transmit powers. This is because when the transmit power increases, jammer transmits jamming signal with higher power, hence, Alice can transmit information signal with higher power which leads to increase covert rate. Furthermore, we observe that by increasing the number of the best selected antennas for signal transmission, the achievable

[1] The left side of C_2 is convex because its second-order derivative is positive for $0<\alpha<1$ and the right side of C_2 is linear, hence, it is clear that the difference of convex and linear functions is convex

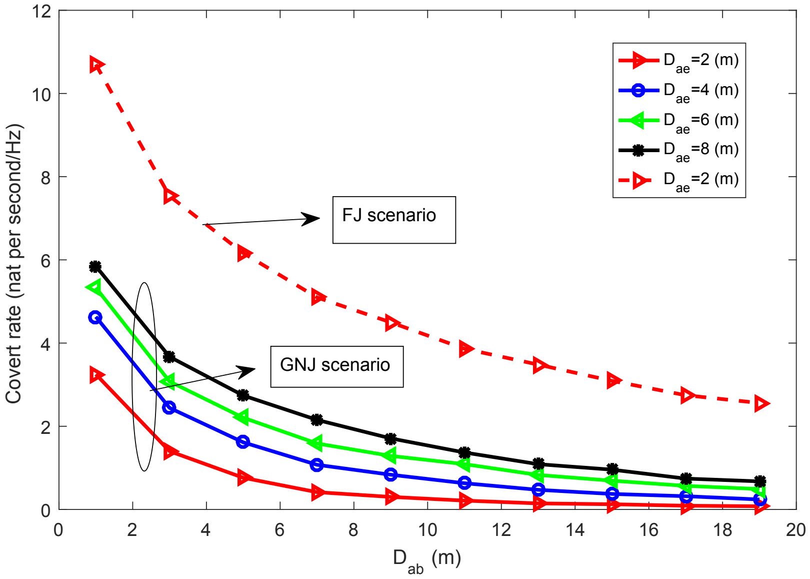

Fig. 3. Covert rate versus the distance between Alice and Bob. We set $P_{total}=5W$.

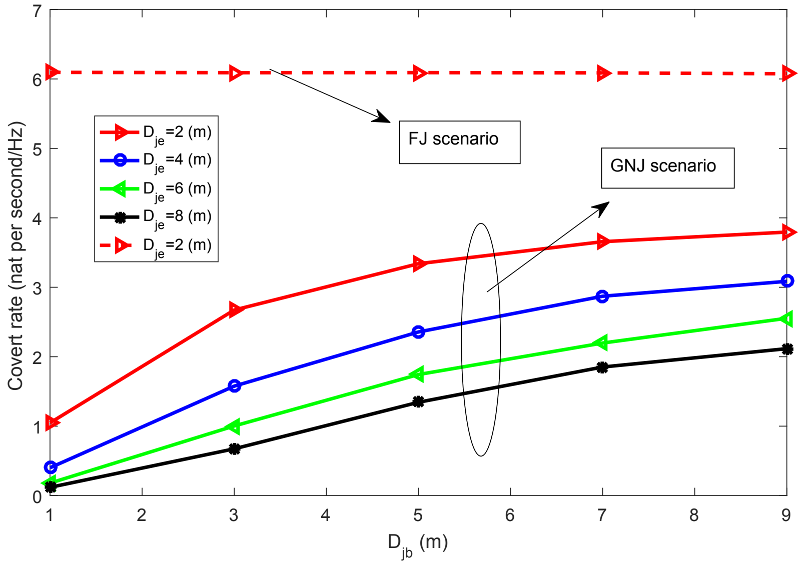

Fig. 4. Covert rate versus the distance between the jammer and Bob. We set $P_{total}=5W$.

covert rate improves. For example, if the transmit power is constant and the number of antennas which are selected for sending information signal is doubled, the covert rate is reduced 27%. However, the simulation results show that the associated number of antennas should not be larger than 6 in order to balance the performance gain and implementation cost. If the number of antennas exceeds 6, in addition to Bob's condition, the Eve conditions will also improve for detection, which will make our hidden rate not change significantly. Since allocating large number of antennas for signal transmission imposes more hardware equipment (RF chains), higher latency and more much overhead to the network. Moreover, this figure compares random antenna selection and proposed antenna selection. It is necessary to note that random antenna selection with $N_D=4$ has more efficiency with respect to proposed method with $N_D=1$ and less efficiency with respect to proposed method with $N_D=2$. The reason is when the number of antennas increase diversity gain increases. But the proposed method with less diversity gain has more efficiency with respect to random antenna selection with higher diversity gain. The Fig. 2 shows proposed method enhances the covert rate approximately 2 times.

As we can see in Fig. 3, the lower the distance between Alice and Bob, the higher the covert rate. In addition, the lower the distance between Alice and Eve, the lower the covert rate. Given Fig. 3, if the distance between Alice and Bob is increased by 6 meters, the covert rate reduces about

62%. Now, if the distance between Alice and Eve increases the same amount, the cover rate increases about 4.7 times. Thus, the impact of the distance between Alice and Eve is more important than the distance between Alice and Bob. Also, as shown in Figure 3, when the Bob can cancel the jamming signal, the covert rate increases dramatically. For example, if the distance between Alice and Jammer is 2 meters and Bob cancels the jamming signal, the covert rate is 5.6 times more.

Also, in Fig. 4, we can see the effect of the distance between the jammer and Bob and Eve on the covert rate. According to simulation results, when Bob cannot cancel the jamming signal, the lower the distance between the jammer and Bob, the lower the covert rate. For example, if the distance between the jammer and Bob from 3 to 9 meters, the covert rate will increase 40%. Since the jamming signal treats as interference in Bob, by reducing the distance between the jammer and Bob, the covert rate is reduced. Moreover, the distance between the jammer and Eve is effective. If their distance is 6 meter high, the covert rate will decrease 63% . Also, when the jamming signal is canceled, increasing of the distance between Bob and jammer does not change the covert rate, and this parameter does not effect on the covert rate.

6- CONCLUSION

In the covert communication, the level of transmit power is low which lead to low SINR hence we aim to exploit from method without increasing the transmit power increase the covert rate. Our strategy to increase the covert rate is choosing the appropriate antenna in the transmitter to send the information. For this purpose, we proposed a system with a multi-antenna transmitter, a single-antenna jammer, a single-antenna receiver, and a single antenna eavesdropper. In this scenario, we encountered the optimization problem, which we use to solve the method of DC. Moreover, we investigated two different scenarios: 1) GNJ where Bob is unable to cancel the jamming signal, 2) FJ scenario where Bob is able to cancel the jamming signal. As the simulation results show, by increasing the number of antennas which are selected in the transmitter and choosing an appropriate antenna for sending the information, it causes an increase in the covert rate. Furthermore, the distance between transmitter and the eavesdropper has more impact on the cover rate compared with the distance between the transmitter and the receiver.

7- APPENDIX

7-1 Appendix A

It is simple to show that $\mathrm{P}_{\mathrm{FA}}+\mathrm{P}_{\mathrm{MD}}$ is convex. In order to calculate the minimum value of $\mathrm{P}_{\mathrm{FA}}+\mathrm{P}_{\mathrm{MD}}$, we derivative $\mathrm{P}_{\mathrm{FA}}+\mathrm{P}_{\mathrm{MD}}$ with respect to V and then we find the root of it. Following this, we obtain the optimum value of V as follows

$$V^{*}=\frac{\phi_0\phi_1}{\phi_1-\phi_0}Ln\frac{\phi_1}{\phi_0}+\sigma_e^2.$$

By substituting V^{*} into (13), we have

$$\min_{V}(P_{FA}+P_{MD})=e^{-\frac{\phi_1 A}{\phi_1-\phi_0}}+\Lambda_2,$$

where $\Lambda_2=\frac{1}{\phi_0-\phi_1}(\phi_1 e^{-\frac{\phi_0}{\phi_1-\phi_0}A}-\phi_0 e^{-\frac{\phi_1}{\phi_1-\phi_0}A}+\phi_0-\phi_1)$ and $A=Ln\frac{\phi_1}{\phi_0}$.

7-2 Appendix B

For the constraint C_2, we can write

$$\frac{\alpha D_{je}^{\beta}}{(1-\alpha)D_{ae}^{\beta}-\alpha D_{je}^{\beta}}\times\left[e\frac{(1-\alpha)D_{je}^{\beta}}{(1-\alpha)D_{ae}^{\beta}-\alpha D_{je}^{\beta}}ln(\frac{\alpha D_{je}^{\beta}}{(1-\alpha)D_{ae}^{\beta}})-\right.$$
$$\left.e\frac{\alpha D_{je}^{\beta}}{(1-\alpha)D_{ae}^{\beta}-\alpha D_{je}^{\beta}}ln(\frac{\alpha D_{je}^{\beta}}{(1-\alpha)D_{ae}^{\beta}})\right] \quad (21)$$
$$=\frac{\alpha D_{je}^{\beta}}{(1-\alpha)D_{ae}^{\beta}-\alpha D_{je}^{\beta}}\times e^{\frac{(1-\alpha)D_{ae}^{\beta}}{(1-\alpha)D_{ae}^{\beta}-\alpha D_{je}^{\beta}}^{ln(\frac{\alpha D_{je}^{\beta}}{(1-\alpha)D_{ae}^{\beta}})}}\times\left[1-e^{ln(\frac{\alpha D_{je}^{\beta}}{(1-\alpha)D_{ae}^{\beta}})}\right]>-\varepsilon$$

Therefore, we can rewrite the inequality (21) as

$$e^{\frac{(1-\alpha)D_{ae}^{\beta}}{(1-\alpha)D_{ae}^{\beta}-\alpha D_{je}^{\beta}}ln(\frac{\alpha D_{je}^{\beta}}{(1-\alpha)D_{ae}^{\beta}})}<\varepsilon.$$

which is equivalent to the constraint C_2.

REFERENCE

[1] Y. Liang, H. V. Poor, and L. Ying, “Wireless broadcast networks: reliability, security, and stability,” Inf. Theory and App. Work. , USA, pp. 249-255, Feb. 2008.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: A survey,” IEEE Commun. Surveys Tuts. , Vol. 16, no. 3, pp. 1550-1573, Feb. 2014.

[3] A. Kuhestani, A. Mohammadi and M. Mohammadi “ Joint Relay Selection and Power Allocation in Large-Scale MIMO Systems With Untrusted Relays and Passive Eavesdroppers,” IEEE Trans. Inf. Foren. Sec., vol. 13, no. 2, pp. 341-355, Feb. 2018.

[4] M. Tatar Mamaghani, A. Kuhestani and K.-K. Won “Secure Two-Way Transmission via Wireless-Powered Untrusted Relay and External Jammer,” IEEE Trans. Veh. Tech., pp. 1-1, Jul. 2018.

[5] A. Kuhestani, A. Mohammadi and P. L. Yeoh, “Optimal power allocation and secrecy sum rate in two-way untrusted relaying networks with an external jammer,” IEEE Trans. Commun. ,Vol. 66, no.6, pp. 2671-2684, Jun. 2018 .

[6] A. Yener and S. Ulukus, “Wireless physical-layer security: Lessons learned from information theory,” Proc. IEEE, Vol. 103, no. 10, pp. 1814-1825, Oct. 2015.

[7] E. Tekin and A. Yener, “The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” IEEE Trans. Inf. Theory ,Vol. 54, no. 6, pp. 2735-2751, Jun. 2008 .

[8] R. Diamant and L. Lampe, “Low Probability of Detection for Underwater Acoustic Communication: A Review,” IEEE Access, Vol. 6, pp. 19099-19112, Mar. 2018.

[9] K. Shahzad, X. Zhou, and S. Yan, “Covert Communication in Fading Channels under Channel Uncertainty,” IEEE 85th Veh. Tech.Conf. (VTC Spring), Sydney, NSW, Australia, pp. 1-5, Nov. 2017.

[10] A. Abdelaziz and C. Emre Koksal, “Fundamental Limits of Covert Communication over MIMO AWGN Channel,” IEEE Conf. on Commun. and Net. Security (CNS), Las Vegas, NV, USA, pp. 1-9, Dec. 2017.

[11] M. Forouzesh, P. Azmi, N. Mokari, and K.-K. Wong,” Covert Communications Versus Physical Layer Security,” arXiv: 1803.06608.

[12] J. Zhang and M. C. Gursoy, “Collaborative relay beamforming for secure broadcasting,” IEEE Wireless Commun. and Net. Conf. (WCNC), Sydney, NSW, Australia, pp. 1-6, Apr. 2010.

[13] J. Hu, S. Yan, X. Zhou, F. and J. Wang, “Covert Communication in Wireless Relay Networks,” IEEE GLOBECOM 2017, Singapore, pp. 1-6, Jan. 2018.

[14] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, “Hiding Information in Noise: Fundamental Limits of Covert Wireless Communication,” IEEE Commun. Magazine, Vol. 53, no. 12, pp. 26-31, Dec. 2015.

[15] P. E. Oguntunde, O.A. Odetunmibi and A.O. Adejumo, “On the Sum of Exponentially Distributed Random Variables: A Convolution Approac”,’ European Journal of Statistics and Probability, Vol. 1, no. 2, pp. 1-8, Dec 2013.

[16] M. Forouzesh, P. Azmi, and A. Kuhestani, “Secure transmission with covert requirement in untrusted relaying networks”, arXiv: 1809.00312 [cs.CR], 2018.

[17] S. Boyd and L. Vandenberghe, “Convex Optimization”, Cambridge University Press, 2004.

[18] M. Moltafet, P. Azmi, M.R. Javan, and A.Mokdad, “Optimal and fair energy efficient resource allocation for energy harvesting-enabled-PD-NOMA-based HetNets”, IEEE Transactions on Wireless Communications, Vol. 17, no. 3, pp. 2054-2067, Mar. 2018.

[19] D. T. Ngo, S. Khakurel, T. Le-Ngoc, “Joint subchannel assignment and power allocation for OFDMA femtocell networks”, IEEE Transactions on Wireless Communications, Vol. 13 no. 1, pp. 342-355, Jan. 2014.

HOW TO CITE THIS ARTICLE

M. Sarkheil, P. Azmi, M. Forouzesh, A. Kuhestani, Covert Transmission with Antenna Selection and Using an External Jammer, AUT J. Model. Simul., 52(1) (2020) 31-38.

DOI: 10.22060/miscj.2019.15496.5135