An Effective Cooperative Jamming-based Secure Transmission Scheme for a Mobile Scenario

Haidong Huang[1], Yan Huo[1], Qinghe Gao[1], Tao Jing[1], Zhiwei Yang[2]

[1] Beijing Jiaotong University, Beijing 100044, China
{22120063, yhuo,qhgao, tjing}@bjtu.edu.cn
[2] Tianjin Hailiang Information Technology CO,LTD., Tianjin 300021, China
yangzhiwei@hylanda.com a

Abstract. Physical Layer Security (PLS) is becoming a hot topic in wireless communications research. The application of artificial noise can reduce the eavesdropping ability of illegal eavesdroppers without affecting legitimate users. Most current PLS schemes only consider static scenarios without taking mobility into account. Some Cooperative Jamming (CJ) schemes analyse the security performance in mobile scenarios, but do not exploit the handoff and cooperation of friendly jammers. To address the above challenge, we propose a CJ scheme for soft-handoff-based cooperative jamming (CJSH) in mobility scenarios. We first consider a common scenario where a base station communicates with a mobile legitimate user alongside a mobile passive eavesdropper. Some friendly jammers with multiple antennas are chosen to emit artificial noise. Next, we design two corresponding thresholds for jammer entry and exit and measure the values based on the Secrecy Outage Probability (SOP). We then define the Power Average Security Gain (PASG) as the system performance to balance security and energy consumption. Finally, numerical simulation results are provided to verify the rationality of the proposed handoff scheme and demonstrate that it effectively improves the system security performance and jamming power consumption.

Keywords: Physical layer security, Mobility, Handoff scheme, Cooperative jamming.

1 Introduction

As a complement to cryptography-based security mechanisms, physical layer security (PLS) is a promising technique that directly exploits the unique properties of the wireless channels to improve the security of wireless networks. The typical type of anti-eavesdropping PLS technique, Cooperative Jamming (CJ), exploits the characteristic differences between legitimate and eavesdropping channels [1]. Essentially, a legitimate node can be chosen to act as a friendly jammer and transmit artificial noise (AN) continuously or intermittently, degrading in the channel quality for eavesdroppers while ensuring that legitimate users are not affected [2, 3]. Existing CJ schemes improve the secure performance by optimizing various aspects such as secrecy capacity maximization [4], power allocation

optimization [5], beamforming vector optimization [6], and precoding matrix design [7]. These schemes, which only focus on CJ design in static scenarios, are inconsistent with the dynamics of real wireless mobile systems, such as those used in Internet of Things (IoT) applications. Therefore, there is an urgent need for the design of an effective PLS scheme for dynamic network scenarios.

Mobility is one of the distinguishing features of a large number of wireless communication scenarios. There has been a gradual increase in research interest in mobile models. In some works, the most commonly used spatial node distributions of the Random Way-point Mobility (RWP) model and the Random Direction (RD) model have been used for security analysis [8]. In contrast to modeling the randomness of the position and number of moving nodes as a homogeneous two-dimensional Poisson point process (PPP), other work specifically analyses the difference between point-based mobility and traceable mobility in [9]. The authors claim that the RWP and RD models can better capture the strong coupling between the underlying movement mode and the trajectory of moving nodes.

The secrecy properties of mobile scenarios are gaining attention, while many PLS schemes are being adopted. It is usually assumed that eavesdroppers do not intend to move. However, even with the help of friendly jammers, the disadvantage of reducing the jamming effectiveness of stationary jammers becomes apparent when the intelligent eavesdropper tries to move away from the jammer. For example, [10] calculated the average bit error rate of different resource allocation schemes over the TeraHertz frequency band. The authors in [8] investigated the SOP and ergodic secrecy capacity of mobile users following the RWP and RD models under the Rayleigh fading channel. Furthermore, the authors in [11] extended to the secrecy capacity under Nakagami-m channels and considered the interference from multiple other base stations. Security analyses involving multiple mobile eavesdroppers have been carried out in the context of unmanned aerial vehicle jitter in air-to-ground communication studies [12]. Several works have begun to focus on the application of friendly jammers and AN design. In [13], a central base station with multiple antennas is used for the simultaneous emission of AN and communication signals. Building on this research, the same authors in [14] further selected the best CJ node to support the security of industrial wireless networks using edge devices. To explore the mobility of different types of nodes, including eavesdroppers and jammers, the authors in [15] considered the impact of multiple node mobility on security performance for different scenarios. Two secrecy enhancement strategies were proposed based on the location information of different wireless nodes. The handoff-based cooperative jamming scheme is proposed in [16] but still overlooks the sudden degradation of secrecy performance during handoff interruptions. However, these studies are limited in considering the effects of other wireless devices, such as legitimate jammers. The CJ schemes of PLS in mobility scenarios still offer promising research prospects.

To address the above challenges, in this paper, we further propose a soft-handoff-based cooperative jamming scheme (CJSH), which is characterized by intermittent cooperation among multiple jammers in the mobility scenario. On

the other hand, in response to the demand for low power consumption, our scheme defines an equilibrium and achieves maximum performance between jamming energy consumption and secrecy. We summarize the main contributions of the paper as follows.

- We describe a PLS model for an intelligent mobile eavesdropper and study the secrecy performance using CJ methods. We then propose a soft handoff-based cooperative jamming scheme with multiple multi-antenna jammers to overcome the challenge of secrecy loss during jammer handoff.
- We define two handoff thresholds related to the secrecy outage probability (SOP) to characterize the cooperation of jammers. And the new performance metric, power average security gain (PASG), is proposed to characterize the trade-off between secrecy and power consumption.
- We optimize the values of two handoff thresholds in the proposed CJSH scheme. Numerical simulation results demonstrate that the optimized thresholds can effectively improve the utilization of jamming power.

The rest of this paper is organized as follows. In Section 2, we introduce the mobility model with an intelligent mobile eavesdropper and declare the secrecy performance indicators used. Then, we propose the optimization problem and design the corresponding solutions in Section 3. Analysis of numerical results is provided in Section 4, and the conclusion is organized in Section 5.

2 System Model

2.1 Network Model and Mobility Scenarios

The proposed down-link transmission is shown in the Fig. 1. Alice is the central base station with a signal coverage area Ω with radius r. There are one legitimate user Bob, one passive eavesdropper Eve, and N_J known friendly jammers Carol in Ω. Alice intends to communicate with Bob, while Eve tries to keep on eavesdropping passively. In order to reduce Eve's eavesdropping ability, several Carols will selectively send AN in accordance with the proposed handoff scheme.

Relates to the mobility of network nodes, Bob is a mobile user and Eve attempts to move for improving the effectiveness of eavesdropping. The behavior patterns of Eve will be introduced below. To prevent Eve from getting too close to Alice, there is a secrecy guard area of Alice with radius r_G to ensure that the distance d_{AE} from Eve to Alice is $d_{AE} \geq r_G$. This assumption is reasonable [8], for example, it is difficult for Eve to approach the base station if it is installed on the roof of a large tower or building.

Eve's Intelligent Eavesdropping Mobile (IEM) Model: Assuming that Eve knows Alice's location without position of Carols. Eve in IEM model only chooses to roam the borders of the secrecy guard area. And because of the intelligence, Distinct from staying, Eve rather tries to move randomly to get rid of the interference from Carols, which confirms the point that CJ scheme by multiple friendly jammers can effectively prevent security performance degradation caused by the movement attempt of Eve.

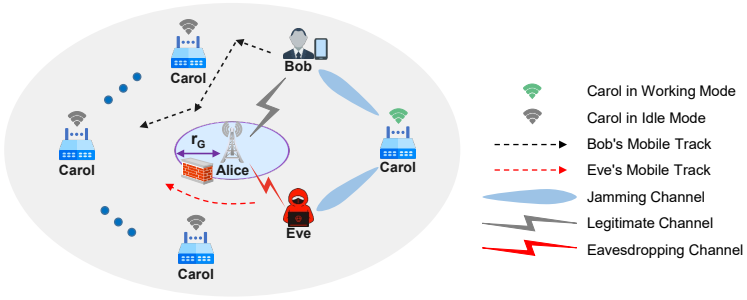


Fig. 1. System model for cooperative jamming of multiple Carols

2.2 Proposed Cooperative Jamming Scheme

Soft-Handoff-Based Cooperative Jamming (CJSH) Scheme: The handoff and cooperation of Carols can effectively improve security by dealing with mobile eavesdroppers. Referring to the idea of the soft handoff mechanism [17] for guaranteeing the quality of service in mobile communication, it is judged whether replacement and cooperation of multiple Carols is needed according to the security performance metrics $\mathbb{P}_{\mathrm{SO}}^{k}, \forall k \in N_J$. The definition of $\mathbb{P}_{\mathrm{SO}}^{k}$ is specifically reflected in Section 3. Carols in the working state will emit AN at the same time, which is received by Eve and Bob. This proposed soft handoff scheme can ensure that there are always one or more Carols in working states and avoid the interruption problem caused by the hard handoff of Carol.

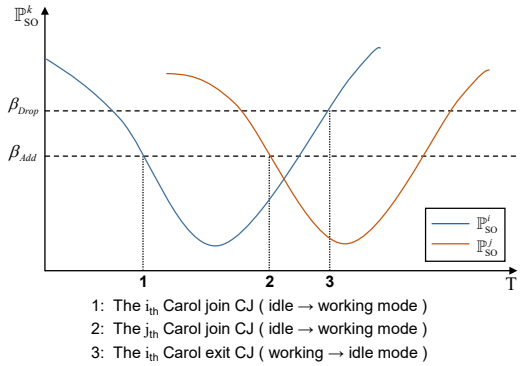


Fig. 2. The cooperate jamming processes in mobility scenarios

In the CJSH described, the soft-handoff process is shown in Fig. (2). Two SOP related thresholds are used to realize the process and defined as the join threshold β_{Add} and the exit threshold β_{Drop}, respectively. The idle Carol with

good jamming performance (low $\mathbb{P}_{\mathrm{SO}}^{k}$) will be changed to the working state causing lower SOP. The working Carol with downgrading poor safety quality (high $\mathbb{P}_{\mathrm{SO}}^{k}$) will be changed to the idle state for preventing low energy efficiency. As a result, it is possible to realize the continuous joining and exiting of good and poor effectual Carols during the communication process and effectively avoid the problem of interruption.

2.3 Mathematical Formulation and Performance Metrics

Assuming that one or more of Carols are chosen to send AN against the eavesdropping. Multiple antenna scenario is adopted that k_{th} ($\forall k \in N_J$) Carols is equipped with N_{C_k} antennas. All other nodes Alice, Bob and Eve are equipped with only single antenna. Then the received signals at Bob and Eve can be represented as:

$$\mathrm{y}_B = \sqrt{PL_{AB}} h_{AB} \mathrm{x}_A + \sum_{i=1}^{N_J} \left(\varphi_k \sqrt{PL_{kB}} \mathbf{H}_{kB}^{\dagger} \mathbf{x}_k \right) + n_B \tag{1}$$

$$\mathrm{y}_E = \sqrt{PL_{AE}} h_{AE} \mathrm{x}_A + \underbrace{\sum_{i=1}^{N_J} \left(\varphi_k \sqrt{PL_{kE}} \mathbf{H}_{kE}^{\dagger} \mathbf{x}_k \right)}_{\text{AN from Carols}} + n_E \tag{2}$$

In (1) and (2), x_A and $\mathbf{x}_k$ are signals transmitted by Alice and k_{th} Carol. h_{Ab}, $b \in \{B, E\}$ is the channel response from Alice to the receivers (Bob, Eve). The channel response matrix from k_{th} Carol to b is assumed to be independent and denoted by $\mathbf{H}_{kb} \in \mathbb{C}^{N_{C_k} \times 1}$, and each element follows Rayleigh fading with a complex Gaussian random variable of zero-mean and unit variance. The symbol $(.)^{\dagger}$ represents the transposition of $(.)$. The binary variable $\varphi_k \in \{0, 1\}$ determine the participation of k_{th} Carol. $n_b \sim \mathcal{CN}(0, N_0^2)$ represents independent zero mean complex additive Gaussian white noise (AWGN) at receivers with variance N_0^2. PL_{ab}, $a \in \{A, k\}$ is the corresponding path loss of the channel from a to b, which can be expressed as $PL_{ab} = \eta d_{ab}^{-\alpha}$ and $\eta = 10^{-3.24} f^{-2}$ according to [18], where d_{ab} (Km) is the distance from the transmitters to the receivers, f (MHz) is transmission frequency. And the path loss coefficient $\alpha \in [2, 6]$ is determined by the propagation environment.

To construct the AN-aided transmit signal for security, zero-forcing constraints are used in signal design. Let P_A and P_k denote the total transmission power of Alice and Carols. The transmit signal can be formulated as:

$$\mathrm{x}_A = \sqrt{P_A} s \ , \ \mathbf{x}_k = \sqrt{\frac{P_k}{N_{C_k} - 1}} \mathbf{W}_k \mathbf{z}_k \tag{3}$$

Alice transmits the legal signal $s \sim \mathcal{CN}(0, 1)$. For Carol, AN signals $\mathbf{z}_k \in \mathbb{C}^{\left(N_{C_k}-1\right) \times 1}$ is also the Gaussian noise vector with probability distribution $\mathbf{z}_k \sim \mathcal{CN}\left(\mathbf{0}, \mathbf{I}_{N_{C_k}-1}\right)$. Matrices $\mathbf{W}_{\mathrm{k}} \in \mathbb{C}^{N_{C_k} \times \left(N_{C_k}-1\right)}$ denotes an orthogonal basis for

null space of $\mathbf{H}_{kB}^{\dagger}$. According to the mathematical expression of the received signal from (1) and (2), the signal-to-interference-plus-noise ratio (SINR) of Bob and Eve can be expressed as γ_B and γ_E as follows:

$$\gamma_B = \frac{|h_{AB}|^2 \eta P_A d_{AB}^{-\alpha}}{N_0^2}\ ,\ \gamma_E = \frac{|h_{AE}|^2 \eta P_A d_{AE}^{-\alpha}}{\sum\limits_{k=1}^{N_J} \varphi_k \frac{\left\|\mathbf{H}_{kE}^{\dagger}\mathbf{W}_k\right\|^2 \eta P_k}{\left(N_{C_k}-1\right) d_{kE}^{\alpha}} + N_0^2} \tag{4}$$

We design Carol's handoff cooperative jamming scheme in a mobility scenario with the goal of meeting the security requirements of legitimate links while reducing the energy consumption of the system. Therefore, it is necessary to find not only a security performance metric, but also a metric that can achieve a balance between security and energy consumption as a measure of the effectiveness of the proposed scheme.

1) The Secrecy Outage Probability (SOP): The SOP is the probability of achieving a non-negative target secrecy rate, which is one of the most commonly used security performance metrics in the presence of an eavesdropper. SOP is defined as the probability that the SINR at Eve is below the threshold γ_{th}:

$$\mathbb{P}_{\mathrm{SO}} = \Pr(\gamma_E \geq \gamma_{th}) \tag{5}$$

2) Power Average Security Gain (PASG): More cooperative jamming generally satisfies better secrecy performance but consumes more energy. Therefore we need to trade off between energy consumption and security when optimizing the thresholds β_{Add} and β_{Drop} for soft handoff. Based on the above considerations, this paper designs a new performance metric PASG, with the aim of comparing the CJ scheme with the case of no friendly jamming to characterize the effect of SOP enhancement for the jamming power. We define $\mathbb{P}_{\mathrm{SO,non}}$ as SOP without CJ and $\bar{P}_{total}$ as the average total energy consumption. PASG is represented as:

$$\varpi = \frac{\mathbb{P}_{\mathrm{SO,non}} - \bar{\mathbb{P}}_{\mathrm{SO}}}{\bar{P}_{total} - P_A} = \lim_{T\to\infty} \int_0^T \frac{\mathbb{P}_{\mathrm{SO,non}} - \mathbb{P}_{\mathrm{SO}}(t)}{\sum\limits_{k=1}^{N_J} \varphi_k(t) P_k} dt \tag{6}$$

In the following sections, we will express the above performance metrics mathematically.

3 Analysis and Optimization of Security

3.1 Problem Formulation

With the goal of trade-off between energy consumption and security performance, We compute the SOP for the case where a single Carol interferes with Eve and as the safety performance that this Carol can provide. The the thresholds β_{Add} and β_{Drop} are mathematically characterized by using the values of the

SOP for Carol to join and exit the cooperative jamming. Subsequently, there establishing the following optimization problem $\mathcal{P}1$.

$$\mathcal{P}1: \quad \max_{\beta_{Add},\beta_{Drop}} \quad \varpi \tag{7a}$$

$$\text{s.t.} \quad 0 < \beta_{Drop} < 1 \tag{7b}$$

$$0 < \beta_{Add} < 1 \tag{7c}$$

$$\beta_{Drop} - \beta_{Add} \geq \epsilon \tag{7d}$$

Problem $\mathcal{P}1$ determines the maximized PASG by optimizing β_{Add} and β_{Drop}. (7b) and (7c) bound the range of values of β_{Add} and β_{Drop} based on the probability SOP, respectively. For secrecy, a lower SOP corresponds to a Carol with a better jamming effect, so a Carol should join at a low threshold and exit at a high, corresponding to the constraints in (7d), where ϵ is the difference between two thresholds that need to be met.

3.2 Analysis and Optimization of Security

We first must explore the mathematical expression of performance parameters. For the sake of simplicity without loss of generality, at most 2 Carols are involved in CJ simultaneously in the soft handoff scenario studied in this paper. Under the above assumptions, SOP can be expressed in (4) and (5) as:

$$\mathbb{P}_{\mathrm{SO}} = \Pr\left(\frac{|h_{AE}|^2 \eta P_A d_{AE}^{-\alpha}}{\varphi_i \frac{\left\|\mathbf{H}_{iE}^{\dagger}\mathbf{W}_i\right\|^2 \eta P_i}{(N_i-1)d_{iE}^{\alpha}} + \varphi_j \frac{\left\|\mathbf{H}_{jE}^{\dagger}\mathbf{W}_j\right\|^2 \eta P_j}{(N_j-1)d_{jE}^{\alpha}} + N_0^2} \geq \gamma_{th} \right) \tag{8}$$

The serial number $i \in N_J$ and $j \in N_J$ represent corresponding Carol participating in CJ. To simplify the representation, new variables are defined as follows:

$$X = \frac{|h_{AE}|^2 \eta P_A}{d_{AE}^{\alpha} N_0^2}, \; Y_k = \frac{\left\|\mathbf{H}_{C_k E}^{\dagger}\mathbf{W}_{C_k}\right\|^2 \eta P_{C_k}}{(N_{C_k}-1) d_{kE}^{\alpha} N_0^2}, \; \forall k \in N_J \tag{9}$$

The conclusions that $X \sim \mathrm{Exp}(\lambda_0)$, $Y_k \sim \Gamma(\mu_k, \lambda_k)$ have been adopted by some existing works [19], where $\mu_k = N_{C_k} - 1$, $\lambda_0 = \frac{N_0^2 d_{AE}^{\alpha}}{\eta P_A}$, $\lambda_k = \frac{\mu_k N_0^2 d_{kE}^{\alpha}}{\eta P_k}$. Then the SOP can be simplified and solved as follows.

Theorem 1. *The SOP in (8) has a simplified form as:*

$$\mathbb{P}_{\mathrm{SO}} = \Pr\left(\frac{X}{1 + \varphi_i Y_i + \varphi_j Y_j} \geq \gamma_{th} \right) \tag{10}$$

1) When $\varphi_i = 1$ and $\varphi_j = 0$, the i_{th} Carol individually emits AN to assist Alice in communicating with Bob. The SOP can be expressed as:

$$\mathbb{P}_{\mathrm{SO}}^{i} = \Pr\left(\frac{X}{1+Y_i} \geq \gamma_{th}\right) = \left(\frac{\lambda_i}{\lambda_i + \lambda_0 \gamma_{th}}\right)^{\mu_i} e^{-\lambda_0 \gamma_{th}} \tag{11}$$

2) When $\varphi_i = 1$ and $\varphi_j = 1$, one good effect j_{th} Carol joins the cooperative jamming so that two Carols will work together to help secure communications. The SOP can be expressed after convolution and integration operations as:

$$\mathbb{P}_{\mathrm{SO}}^{ij} = \Pr\left(\frac{X}{1+Y_i+Y_j} \geq \gamma_{th}\right) = \left(\frac{\lambda_i}{\lambda_i + \lambda_0\gamma_{th}}\right)^{\mu_i} \left(\frac{\lambda_j}{\lambda_j + \lambda_0\gamma_{th}}\right)^{\mu_j} e^{-\lambda_0\gamma_{th}} \quad (12)$$

Based on position of Carol available to participate in CJSH, the range of SOP can be determined to tighten optimization constraints. We define r_k as the distance between Alice and k_{th} Carol. For Carol, the jamming effect is worst when the location satisfies $d_{kE,\max} = r_k + r_G$, and is conversely best when it satisfies $d_{kE,\min} = r_k - r_G$. To narrow down the value range of (7b) and (7c), the upper bound β_{ub} and lower bound β_{lb} can be derived as:

$$\beta_{ub} = \max_{k \in N_J} \left\{ \left(\frac{\lambda_{k, d_{kE} = d_{kE,\max}}}{\lambda_{k, d_{kE} = d_{kE,\max}} + \lambda_0\gamma_{th}} \right)^{\mu_k} e^{-\lambda_0\gamma_{th}} \right\} \quad (13)$$

$$\beta_{lb} = \min_{k \in N_J} \left\{ \left(\frac{\lambda_{k, d_{kE} = d_{kE,\min}}}{\lambda_{k, d_{kE} = d_{kE,\min}} + \lambda_0\gamma_{th}} \right)^{\mu_k} e^{-\lambda_0\gamma_{th}} \right\} \quad (14)$$

Then $\mathcal{P}1$ can be rewritten as the problem with stricter constraints:

$$\mathcal{P}2: \quad \max_{\beta_{Add}, \beta_{Drop}} \quad \varpi \quad (15a)$$

$$\text{s.t.} \quad \beta_{lb} + \epsilon \leq \beta_{Drop} \leq \beta_{ub} \quad (15b)$$

$$\beta_{lb} \leq \beta_{Add} \leq \beta_{ub} - \epsilon \quad (15c)$$

$$\beta_{Drop} - \beta_{Add} \geq \epsilon \quad (15d)$$

Algorithm 1: Calculate the solution β_{Add} and β_{Drop} of $\mathcal{P}2$

Input: $\beta_{ub}, \beta_{lb}, \epsilon, N_\beta$
Initialization $\delta = (\beta_{ub} - \beta_{lb} - \epsilon)/N_\beta$;
for $i = 0, 1, \cdots, N_\beta$ **do**
  for $j = i, i+1, \cdots, N_\beta$ **do**
    Let $\beta_{Add} = \beta_{lb} + i \times \delta$; $\beta_{Drop} = \beta_{lb} + \epsilon + j \times \delta$;
    Reset system time $T = 0$;
    while ϖ *not converge* **do**
      Compute ϖ with $\beta_{Add}, \beta_{Drop}$; Let $T = T + 1$;
    end
    if $\varpi > \varpi^*$ **then** Let $(\varpi^*, \beta_{Add}^*, \beta_{Drop}^*) = (\varpi, \beta_{Add}, \beta_{Drop})$;
  end
end
Output: *Optimal solution* $(\varpi^*, \beta_{Add}^*, \beta_{Drop}^*)$

According to PASG in (6), we regard the time period experienced by the whole system process from the beginning to the stabilization as an integral path.

With the help of the curve integrals with SOP as the product function, we can get PASG by calculating the integral formula. Since the handoff and cooperation of Carol in CJSH affect the SOP drastically, the integral function in the formula is not a smooth curve, which makes it difficult to derive the closed expressions of and PASG.

In order to solve problem $\mathcal{P}2$ with low complexity, we use the idea of differentiation to calculate integrals and discretize the solution space into N_β intervals and use the Exhaustive Attack Method, as summarized in Algorithm 1. For the given system model parameters, β_{Add} and β_{Drop} can be obtained computationally by equation (13) and (14) as input. Based on each set of solutions $(\beta_{Add}, \beta_{Drop})$, converged ϖ can be obtained after a sufficiently long time of T. Thus, the corresponding solutions $\left(\beta^*_{Add}, \beta^*_{Drop}\right)$ for $\varpi^* = \max \varpi$ can be solved.

4 Simulation

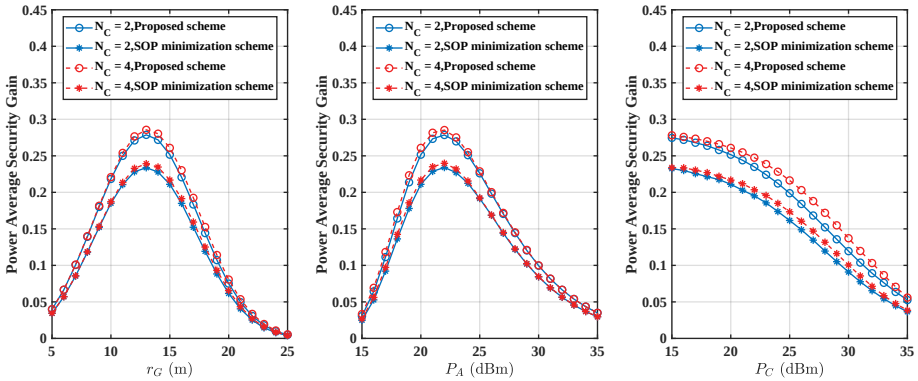
The Cartesian coordinate system is established with Alice as the origin, where the positions of Carol are randomly selected as $(-40, -40)$, $(35, -40)$, $(-25, 50)$ and $(40, 45)$(m), respectively. In the legend of simulation results, the CJSH scheme is always used in this paper. The number of antennas is assumed to be the same $N_C = N_{C_k}$ $(\forall k \in N_J)$ for all Carols. The proposed scheme is the optimal solution to $\mathcal{P}2$, while the SOP minimization scheme is another solution of thresholds only for the best security. The main simulation parameters are shown in Tab. 1.

Table 1. Simulation Parameters

Simulation parameters	value
The Alice coverage radius r (m)	100
The Path loss coefficient α	3
The Number of the jammers Carol	4
The Cost for security γ_{th}	3
The Transmission frequency f (MHz)	2000
The Noise power N_0^2 (dBm)	-27

The effect of the parameters of the system model on the PASG is shown in Fig. 3. An appropriate r_G and P_A can result in an effectively improved PASG in Fig. 3(a) and Fig. 3(b). Because lower r_G and higher P_A results in weakness of jamming effects. In contrast, higher r_G and lower P_A can give a small SOP. Both of the above make the change in SOP insignificant and causing low PASG. The situation is different at lower P_A in Fig. 3(c), because the rate of P_C reduction is more pronounced compared to SOP enhancement, resulting in higher values of PASG. By using CJSH, the proposed solution based on the optimization problem $\mathcal{P}2$ possesses a significant improvement in PASG compared to the SOP minimization solution focusing only on security, reflecting the optimal trade-off

between security and energy consumption. On the other hand, multiple antennas can have a positive but insufficient effect on the optimization of security and energy consumption. Under the same power constraints, more antennas can make jamming signal more concentrated and thus cause lower SOP and higher PASG.



(a) Secrecy guard zone. (b) Transmit power of Alice. (c) Transmit power of Carol.

Fig. 3. Impact of different parameters on PASG

Fig. 4 show the PASG of the system using the CJSH scheme for different values of β_{Add} and β_{Drop}. It is indicated that the values of PASG do not vary monotonically with β_{Add} and β_{Drop}. Instead, there exists a pole that corresponds to the optimal solution of the problems. The location of the solution is interestingly close to the boundary where $\beta_{Drop} = \beta_{Add} + \epsilon$, which means that these two thresholds corresponding to Carol's entry and exit are very close under constraints. From the objective of $\mathcal{P}1$ maximizing PASG, the scenario of two-jammer cooperation should occur as much as possible when a single jammer works poorly, and due to the limitation of power consumption, the CJ will not last long, so the time interval from the beginning of the new one joining to the exit of the old jammer is very short, and thus β_{Add} and β_{Drop} are very close.

5 Conclusion

In this paper, we propose a soft-handoff-based cooperative jamming scheme in mobility scenarios. We study the secrecy performance of a mobile user and a passive eavesdropper within the coverage of the base station. Friendly jammers with multiple antennas are used to select the transmitting AN for security. We rationally design the mathematical expression of the two handover thresholds and optimize the values. The result of the optimization is that the two thresholds are usually set to approximately equal values while satisfying the constraint

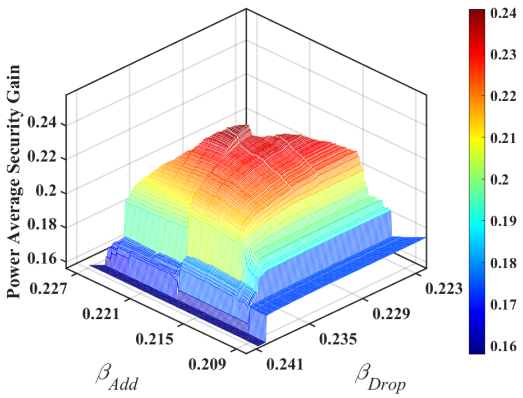


Fig. 4. The three-dimension grid image reflecting the impact of joining and exiting thresholds on PASG under the conditions of $N_C = 2$, $r_G = 15$m, $P_A = P_C = 20$dBm, $\epsilon = 0.01$. The optimal solution is $\left(\beta^*_{Add}, \beta^*_{Drop}\right) = (0.223, 0.233)$.

requirements. We then define and measure the PASG as a performance metric under the CJSH scheme. The simulation results have verified the improvement of security by multiple antennas. At the same time, we show that the CJSH scheme effectively satisfies the system requirements of high security and low power consumption.

Acknowledgments. This work was supported in part by the Fundamental Research Funds for the Central Universities under Grant 2019JBZ001 and the National Natural Science Foundation of China under Grant 62202035 and Grant 61931001.

References

1. Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, "Jamming strategies for physical layer security," *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148–153, 2018.
2. J. M. Moualeu, P. C. Sofotasios, D. B. da Costa, S. Muhaidat, W. Hamouda, and U. S. Dias, "Physical-layer security of simo communication systems over multipath fading conditions," *IEEE Transactions on Sustainable Computing*, vol. 6, no. 1, pp. 105–118, 2021.
3. Q. Gao, Y. Huo, T. Jing, L. Ma, Y. Wen, and X. Xing, "An intermittent cooperative jamming strategy for securing energy-constrained networks," *IEEE Transactions on Communications*, vol. 67, no. 11, pp. 7715–7726, 2019.
4. Y. Wen, L. Liu, J. Li, X. Hou, N. Zhang, M. Dong, M. Atiquzzaman, K. Wang, and Y. Huo, "A covert jamming scheme against an intelligent eavesdropper in cooperative cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 10, pp. 13 243–13 254, 2023.
5. Y. Huo, X. Fan, L. Ma, X. Cheng, Z. Tian, and D. Chen, "Secure communications in tiered 5g wireless networks with cooperative jamming," *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, pp. 3265–3280, 2019.

6. Q. Li and L. Yang, "Beamforming for cooperative secure transmission in cognitive two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 130–143, 2020.
7. J. Tang, Y. Zhao, W. Feng, X. Zhao, X. Y. Zhang, M. Liu, and K.-K. Wong, "Cross-layer optimization for industrial internet of things in noma-based c-rans," *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 16 962–16 975, 2022.
8. J. Tang, M. Dabaghchian, K. Zeng, and H. Wen, "Impact of mobility on physical layer security over wireless fading channels," *IEEE Transactions on Wireless Communications*, vol. 17, pp. 7849–7864, 2018.
9. J. Tang, H. Wen, H. Song, T. Zhang, and K. Qin, "On the security–reliability and secrecy throughput of random mobile user in internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 635–10 649, 2020.
10. M. Alzard, S. Althunibat, K. Umebayashi, and N. Zorba, "Resource allocation in thz-based subcarrier index modulation systems for mobile users," in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 01–06.
11. N. Cao, Y. Chen, and Z. Yang, "Secrecy outage probability with randomly moving interferers in nakagami-m fading," *IEEE Communications Letters*, vol. 23, no. 1, pp. 76–79, 2018.
12. H. Wu, H. Li, Z. Wei, N. Zhang, and X. Tao, "Secrecy performance analysis of air-to-ground communication with uav jitter and multiple random walking eavesdroppers," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 572–584, 2021.
13. T. Zhang, H. Wen, J. Tang, H. Song, R. Liao, Y. Chen, and Y. Jiang, "Analysis of the physical layer security enhancing of wireless communication system under the random mobile," *IET Communications*, vol. 13, no. 9, pp. 1164–1170, 2019.
14. T. Zhang, H. Wen, J. Tang, H. Song, and F. Xie, "Cooperative jamming secure scheme for iwns random mobile users aided by edge computing intelligent node selection," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 4999–5009, 2021.
15. K. Yu, J. Yu, and A. Dong, "Cooperative communication and mobility for securing urllc of future wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 5, pp. 5331–5342, 2022.
16. D. Shen, Y. Huo, and Q. Gao, "A friendly jamming handover scheme for a conscious mobile eavesdropper in iot systems," *Procedia Computer Science*, 2022.
17. R. P. Narrainen and F. Takawira, "Performance analysis of soft handoff in cdma cellular networks," *IEEE Transactions on Vehicular Technology*, vol. 50, no. 6, pp. 1507–1517, 2001.
18. Y. Wen, Y. Huo, L. Ma, T. Jing, and Q. Gao, "A scheme for trustworthy friendly jammer selection in cooperative cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3500–3512, 2019.
19. L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219–228, 2018.