JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 35, 1029-1044 (2019)
DOI: 10.6688/JISE.201909_35(5).0006

Cooperative Jamming for Secrecy of Wireless Communications

BAIHE MA, ZHIHONG LIU, YONG ZENG, ZHUO MA,
HUI ZHANG AND JIANFENG MA
School of Cyber Engineering
Xidian University
Xi'an, Shaanxi, 710126 P.R. China
E-mail: liuzhihong@mail.xidian.edu.cn

This paper investigates cooperative jamming for security in wireless networks. No location information of eavesdropper is available and no constraint on the number of eavesdroppers is presupposed. A cooperative jamming strategy is proposed for jamming the eavesdroppers anywhere in the network, even if they are located quite close to the sender or the receiver. The basic ideas behind the strategy are to defeat eavesdroppers by a divide and conquer strategy, and exploit the helpful interference from the sender and the receiver to circumvent the nearby eavesdropper problem. Analysis and simulation results reveal that cooperative jamming can improve the secure performance and can be employed to establish initial connections in wireless networks.

Keywords: physical layer security, wireless communications, cooperative jamming, network security, machine learning

1. INTRODUCTION

Embedded, mobile, and wireless cyber-physical systems are becoming ubiquitous and are used in many applications. Due to the open wireless medium, security is an important issue in wireless systems. A careful trade-off between security properties, functionality and cryptographic primitives must be addressed carefully. For example, resource-constrained nodes should receive less computationally intensive tasks, and the lack of tamper-resistance implies that long-term secrets should not reside in nodes [1].

Existing work on cooperative jamming for physical-layer security focused primarily on the simple model with single sender-receiver pair and single eavesdropper, investigating the security from the information-theoretic perspective. In practice, it is hard to achieve secure communication with eavesdroppers in any location of the network. To solve this situation, in this paper, we consider a scenario in which a sender communicates with a receiver in the presence of multiple eavesdroppers anywhere, even if they are located near the sender or the receiver, and have no constrict on the number of eavesdroppers.

As depicted in Fig. 1, suppose a node S wants to communicate securely with a receiver D, but they do not share any secret credentials and cannot run computationally intensive tasks (such as RSA or DH key exchange algorithm) to establish a session key due to their limited computational resources. In this occasion, they can employ cooperative jamming to setup an initial secret key to protect their communications. At first, both S and D agree on a code, and setup two thresholds γ and γ_e, where the receiver D is able

Received October 19, 2018; revised December 3, 2018; accepted January 10, 2019.
Communicated by Xiaohong Jiang.

to decode the message if and only if it received Signal-to-Interference-plus-Noise Ratio (SINR) γ_{SD} is greater than the threshold γ_t, whereas the SINR γ_{SE} at potential eavesdroppers E is below another (lower) threshold γ_e. Each jammer can impair the eavesdroppers located within its jamming region[1]. A jammer at different location should be tuned to proper jamming power to satisfy the defined threshold γ_t, thus its jamming region is different.

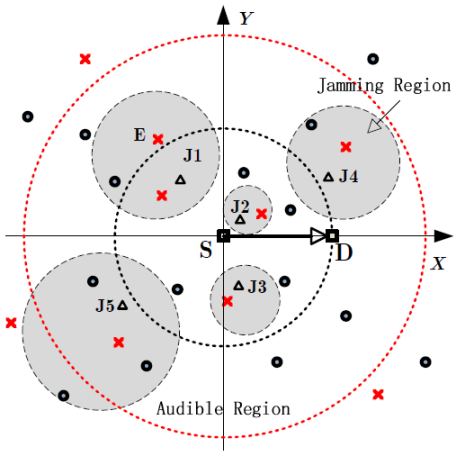


Fig. 1. The network model. ×, Δ, and ◦ denote eavesdropper, jammer, and legitimate nodes, respectively. The shaded disc is the jamming region of a jammer. Any eavesdropper E located within a jamming region will have its $\gamma_{SE} < \gamma_e$.

To thwart the eavesdroppers located in the communication region, one can choose legitimate nodes to act as jammers by introducing interference to the eavesdroppers. However, all eavesdroppers cannot be jammed at the same time, since it is likely that the induced noise may also hurt the legitimate receiver. We address this issue by a method, which requires the sender to divide the message into multiple packets, and send packets in separate transmissions. In each transmission, we select a jammer to inject noise with certain power to degrade the signal quality at eavesdroppers near the jammer.

2. RELATED WORK

Existing work on cooperative jamming focused primarily on the simple model with single sender-receiver pair and single eavesdropper, investigating the security from the information-theoretic perspective. In practice, it is hard to achieve secure communication with eavesdroppers in any location of the network. In [2], Goel *et al*. considered multiple eavesdroppers of unknown location, using artificial noise and multi-user diversity to enhance the security, but their scheme can only tolerate the number of eavesdroppers whose growth is sub-linear in the number of system nodes. Zhou *et al*. [3] used a multi-antenna transmitter to implement jamming. Furthermore, many works presupposed that the eavesdroppers cannot be arbitrarily close to the sender. In 2012, Çapar *et al*. [4] supposed that the probability that any pair of nodes does not have eavesdroppers in their

[1] The *Audible region* in Fig. 1 is the region where any eavesdropper E located inside it will have $\gamma_{SE} > \gamma_e$ when no jammer is introduced, and the *jamming region* of a jammer J is the region where any eavesdropper E located inside it will have $\gamma_{SE} < \gamma_e$ due to the jamming signal of J.

vicinity is arbitrarily close to 1, and in [5], the sender is assumed to know *a priori* whether there is any eavesdropper within some neighborhood or not. As shown in [6, 7], to enable covert communications, Soltani *et al*. employed friendly jammers to generate artificial noise in order to impair wardens' ability to detect transmissions. Reference [8] considered a physical layer network including single-antenna nodes and multiple eavesdroppers. Additionally, they proposed a condition to realize a positive secrecy rate at the destination and solved the secrecy rate maximization problem. A method was presented in [9] to solve the problem of reliability and secrecy enhancement for wireless content sharing between nodes with the model of multiple nodes and multiple eavesdroppers. Additionally, they also presented a method of jammer node selections to maximize the worst-case ergodic secrecy rate. In their model, they employed the more practical case in which only statistical channel statistic information knowledge is known.

In this paper, we consider a scenario in which a sender communicates with a receiver in the presence of multiple eavesdroppers anywhere, even if they are located near the sender or the receiver, and have no constraint on the number of eavesdroppers, which is as realistic as possible.

The basic idea first appears in [10, 11]. In [11], jammer placement algorithms targeted towards optimizing the total number of jammers are introduced. The work in [10] presupposed that, if the eavesdroppers are located farther away than the receiver, there exists a positive secrecy transmission capacity between the sender and the receiver, and the secure communication is deemed possible. The methodology does not consider noise and fading in wireless channels, and only consider the occasion that eavesdroppers locate within the region $B(S, d_{SD})$[2]. It presupposes that, if the eavesdroppers are located farther away than the receiver, there exists a positive secrecy transmission capacity between the sender and the receiver, and the secure communication is deemed possible. However, in practice this assumption is not applicable. In this paper, we do not have such limitations. We consider a scenario in which a sender communicates with a receiver in the presence of multiple eavesdroppers anywhere, even if they are located near the sender or the receiver, and have no constraint on the number of eavesdroppers.

3. SYSTEM MODEL

Consider a configuration with a sender S, a receiver D, multiple legitimate nodes and eavesdroppers. Let $\Phi_l = \{x_i\}_{i=1}^{\infty} \subset \mathbb{R}^2$ be the set of legitimate nodes, and $\Phi_e = \{e_i\}_{i=1}^{\infty} \subset \mathbb{R}^2$ be the set of eavesdroppers. Nodes in Φ_l and Φ_e are distributed according to independent Poisson Point Processes (PPP) with intensities nodes are assumed to be static, and the eavesdroppers are passive, operating independently of each other. We assume that each legitimate node can work as a jammer, and each jammer is able to set its power to a static value that is determined by the environment's geometry.

We assert transmission success to be determined by SINR lying above a specified threshold. For a message sent by S to be securely received at D in the presence of an eavesdropper E, we require the SINR at the eavesdropper γ_{SE} to be smaller than the SINR at the receiver D γ_{SD}. Furthermore, we require $\gamma_{SD} \geq \gamma_l$ and $\gamma_{SE} < \gamma_e$, where $\gamma_e (< \gamma_l)$ can be arbitrarily small. Thus the secrecy capacity of the link S-D is $\mathbf{C}_{SD}(E) = [\log_2(1 + \gamma_{SD}) -$

[2] $B(S, d_{SD})$ denotes a disc of radius d_{SD} centered at the node S. d_{SD} is the Euclidean distance between S and D, *i.e.*, $d_{SD} = S - D$.

$\log_2 (1 + \gamma_{SE})]^+$, and both S and D can agree on a code with secrecy rate $\mathbf{R}_{SD}$. Communication is secure if the secrecy capacity $\mathbf{C}_{SD}$ is higher than the secrecy rate $\mathbf{R}_{SD}$.

4. COOPERATIVE JAMMING PROTOCOL

4.1 Smart Jamming

Although the eavesdroppers cannot be thwarted at the same time, we can defeat them one by one. To gain an advantage over eavesdroppers, we generate multiple packets for a single message such that the message can only be decoded if all packets are received, otherwise no information about the message can be gained. Then packets are sent in separate transmissions, for each transmission, a jammer generates jamming signal to keep the eavesdroppers in its jamming region from getting the packet. Therefore, with enough jammers, the eavesdropper anywhere in the network is guaranteed to miss some nonempty subset of the packets. The smart jamming protocol can be expressed as follows,

Stage 1: Initialization The sender S and the receiver D agree on a code and parameters γ_l and γ_e. Then S selects t legitimate nodes in the audible region to act as jammers (how to determine the value t will be discussed later). For each jammer J, the sender S broadcasts a pilot signal with transmit power P_S, and the jammer J tunes its jamming power PJ until the SINR at the receiver D γ_{SD} is slightly higher than the threshold γ_l.

Stage 2: Packet Construction Suppose the length of the secret message M be b bits. S generates $t - 1$ random b-bit packets $M_1, \ldots, M_{t-1}$, then sets M_t to satisfy $M = M_1 \oplus M_2 \oplus \ldots \oplus M_t$, where $\oplus$ denotes bit-wise XOR operation.

Stage 3: Packet Transmission The sender S transmits each packet one by one. When one packet is being delivered, a jammer J injects jamming signal with jamming power P_J simultaneously. This procedure continues until t packets are sent.

The receiver D can easily reconstruct the secret message M if D has received all packets $M_1, \ldots, M_t$ correctly. According to the Crypto Lemma [12], the eavesdropper missing at least one packet cannot get any information about the message M. Furthermore, if the audible region is covered completely by jamming regions of t jammers, the communication is secure provided that both S and D agree on a wiretap code with secrecy rate $\mathbf{C}_{SD} = \log_2(1 + \gamma_l) - \log_2(1 + \gamma_e)$ at each round of separate transmissions. Therefore, the final secrecy rate the protocol can achieve is $R_{SD} = 1/t \cdot \mathbf{C}_{SD}$.

4.2 Cooperative Jamming

Insecure transmission is mainly due to the presence of eavesdroppers close to the sender (or the receiver). As illustrated in Fig. 2, if the eavesdroppers locate near the region near S and D, they are hard to be jammed.

By recruiting the receiver to do cooperative jamming and a helper to relay in a two stage jamming strategy, the nearby eavesdroppers can be defeated. Given the S-D channel and an eavesdropper within close proximity of the receiver D, we can choose a helper H near D to jam E. The protocol consists of the following two stages:

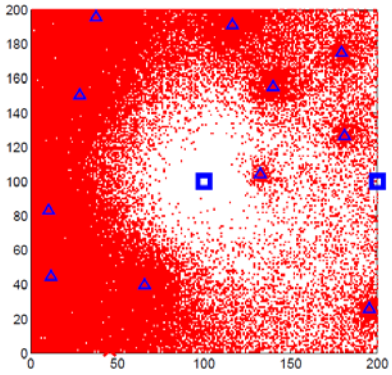


Fig. 2. Example of smart jamming strategy in fading channels. S is located at (100, 100), D at (200, 100), Δ denotes jammer, the red area represents the jamming region. Here P_S/N_0 = 90dB, λ = 0.0003, λ_E = 0.00005, α = 3, R = 100m, γ_1 = 10dB, and γ_e = −10dB. All links experience unit mean Rayleigh fading.

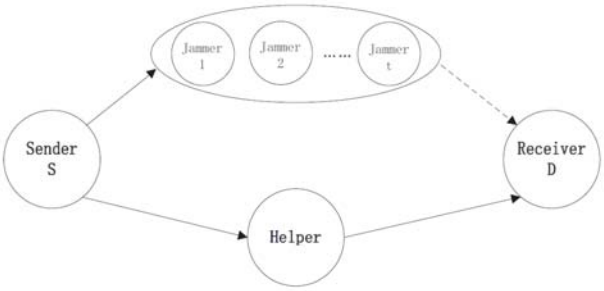


Fig. 3. The cooperative jamming strategy.

Stage 1: the receiver D transmits jamming signal X_D while the sender S transmitting signal X_S. The signal received by a helper H is Y_H which is a mixture of X_S and X_D.

Stage 2: the helper H transmits signal $X_H = \beta Y_H$, where β is the amplification factor in Amplify-and-Forward transmission.

Since node D has perfect knowledge of the signal X_D it transmitted in Stage 1, it can cancel the jamming signal X_D from X_H while an eavesdropper cannot achieve this. An eavesdropper E will wiretap two noisy versions of the signal and must select the one with higher signal quality to decode.

In order to efficiently thwart the eavesdroppers in the whole audible region, we can employ the helper-based scheme in opposite direction to jam the eavesdroppers near the sender, *i.e.*, he receiver D transmits signal while S injects noise. Next we present the cooperative jamming strategy as follows (shown in Fig. 3):

Stage 1: Initialization The sender S and the receiver D agree on a code and parameters γ_1 and γ_e, then S select t jammers and tunes jammers' power to satisfy the parameters. Beside, we choose two helpers d for the transmission from S to D and H_{sd} for the transmission from D to S (how to select helpers will be explained later).

Stage 2: Random Number Exchange

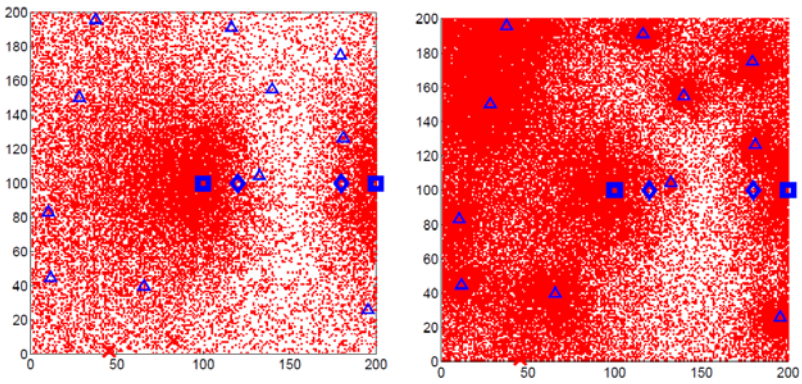
Random Number from D to S: D generates a random number M_D, sends it to S using the helper-based two-stage scheme with the aid of H_{ds}, and S acts as the jammer.

Random Number from S to D: S generates a random number M_S, sends it to D using the helper-based two-stage scheme with the aid of H_{sd}, and D acts as the jammer.

Stage 3: Packet Construction Let M be the b-bit message to be delivered from S to D. S generates $t-1$ random b-bit packets $M_1, \ldots, M_{t-1}$ and then sets M_t to satisfy $M = (M_D \oplus M_S) \oplus M_1 \oplus M_2 \oplus \ldots \oplus M_t$. where $\oplus$ denotes bit-wise XOR operation.

Stage 4: Packet Transmission S then sends $M_1, \ldots, M_t$ to D packets one by one. When one packet is delivering, a jammer J injects jamming signal with jamming power P_J simultaneously. This procedure continues until t packets are sent.

D can reconstruct the message M because D knows M_D and has received M_S, $M_1, \ldots, M_t$ from S. Any eavesdropper missing at least one block cannot get any information about M. Fig. 4 presents an example of simulation results on different jamming schemes. Compared to Fig. 2, the helper-based two-stage scheme can defeat eavesdroppers near S and D, the cooperative jamming, combining the helper-based scheme and smart jamming scheme, can achieve a better performance.



(a) Helper-based jamming. (b) Cooperative jamming.

Fig. 4. Examples of jamming strategies in fading channels. S is located at (100, 100), D at (200, 100), Δ denotes jammer, $\Diamond$ denote helper, and the red area represents the jamming region. Here $P_S/N_0 = 90$dB, $\lambda = 0.0003$, $\lambda_E = 0.00005$, $\alpha = 3$, $R = 100$m, $\gamma_t = 10$dB, and $\gamma_e = -10$dB. All links experience unit mean Rayleigh fading.

5. PERFORMANCE ANALYSIS

5.1 Smart Jamming Protocol

5.1.1 Secrecy outage probability

Wireless channel is modeled by large-scale fading with path loss exponent α ($\alpha > 2$). The instantaneous SINRs at the receiver D and the eavesdropper E are

$$\gamma_{SD} = \frac{\varepsilon_S d_{SD}^{-\alpha}}{1+\varepsilon_J d_{JD}^{-\alpha}} = \gamma_l, \gamma_{SE} = \frac{\varepsilon_S d_{SE}^{-\alpha}}{1+\varepsilon_J d_{JE}^{-\alpha}} = \gamma_e \tag{1}$$

where $\varepsilon_S = P_S/N_0$ and $\varepsilon_J = P_J/N_0$ are the transmit SNR of the sender S and the jammer J, respectively. Then we have

$$\left(\frac{d_{JE}}{d_{JD}}\right)^2 \le \left(\frac{\gamma_e}{\gamma_l} \cdot \frac{\varepsilon_S d_{SD}^{-\alpha} - \gamma_l}{\varepsilon_S d_{SE}^{-\alpha} - \gamma_e}\right)^{2/\alpha}.$$

Given an eavesdropper E_i at (x_i, y_i), its *masking region*[3] A_{E_i} is

$$\left(x - \frac{x_i - aR}{1-a}\right)^2 + \left(y - \frac{y_i}{1-a}\right)^2 \le \frac{a[(x_i - R)^2 + y_i^2]}{(1-a)^2},$$

where $a = (\frac{\gamma_e}{\gamma_l} \cdot \frac{\varepsilon_S R^{-\alpha} - \gamma_l}{\varepsilon_S (x_i^2 + y_i^2)^{-\alpha/2} - \gamma_e})^{2/\alpha}$, $R = \|S - D\|$ is the distance between S and D.

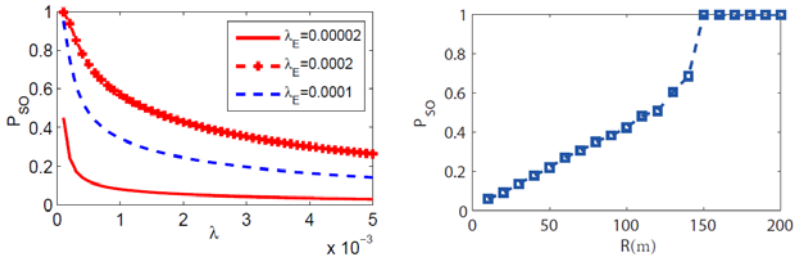
Let $\mathbb{B}_E = B(S, R_E)$ be the audible region, where $R_E = (\frac{\varepsilon_S}{\gamma_e})^{1/\alpha}$ be the radius of the audible region, then the secrecy outage probability P_{SO} is

$$\mathbb{P}_{SO} = 1 - \prod_{E_i \in \mathbb{B}_E} (1 - e^{-\lambda S_{E_i}}),$$

where $S_{E_i} = \pi \frac{a[(x_i - R)^2 + y_i^2]}{(1-a)^2}$. Therefore we can estimate the expectation of the secrecy outage probability as follows

$$\begin{aligned}\mathbb{E}(\mathbb{P}_{SO}) &= 1 - \mathbb{E}\left[\prod_{E_i \in \mathbb{B}_E} (1 - e^{-\lambda S_{E_i}})\right] \\ &= 1 - \exp\left[-\int_{\mathbb{B}_E} e^{-\lambda S_{E_i}} \lambda_E \mathrm{d}E_i\right].\end{aligned}$$

Fig. 5 shows the secrecy outage probability that given λ_E the secrecy outage probability decreases with λ. Given λ, higher λ_E results in higher outage probability. If λ is large enough, the secrecy outage probability can be arbitrarily approximated to 0.



(a) (b)

Fig. 5. Secrecy outage probability vs. (a) λ (R = 50m), and (b) R (λ = 0.0001, λ_E = 0.00002). Here ε_S = 97dB, γ_l = 10dB, and γ_e = −3dB.

[3] A masking region of an eavesdropper E is a region that any jammer located inside it with transmit power satisfying $\gamma_{SD} > \gamma_l$ will result in $\gamma_{SE} < \gamma_e$, *i.e.*, it can successfully impair the ability of the eavesdropper E to decode the message.

5.1.2 Secrecy coverage

Intuitively, if the jamming regions of t jammers can cover the audible region $B(S, R_E)$ in t separate transmissions, the communication from S to D is secure, no matter how many eavesdroppers locate within $B(S, R_E)$.

Given a jammer J_i at (x_i, y_i), according to Eq. (1), $\varepsilon_J = \dfrac{\varepsilon_E R^{-\alpha} - \gamma_t}{\gamma[(x_i - R)^2 + y_i^2]^{-\alpha/2}}$, the jamming region A_{J_i} of J_i contains all the points (x, y) which satisfy

$$\varepsilon_S(x^2+y^2)^{-\alpha/2} < \gamma_e + \gamma_e\varepsilon_J[(x-x_i)^2 + (y-y_i)^2]^{-\alpha/2}.$$

It is hard to derive the closed-form of coverage ratio[4], so we present some numerical results via simulations. Fig. 6 shows the coverage ratio as the function of λ. From the figures, the coverage ratio increases with λ, and given λ and the transmit SNR ε_S, it decreases with the distance R. If D locates near the border of the audible region, the coverage ratio decreases fast and eventually equals 0. This result in fact is explicable, because closer to the border of the audible region, lower SNR Bob experiences, implying that less interference of jammers can be involved to jam eavesdroppers in case of $\gamma_{SD} < \gamma$.

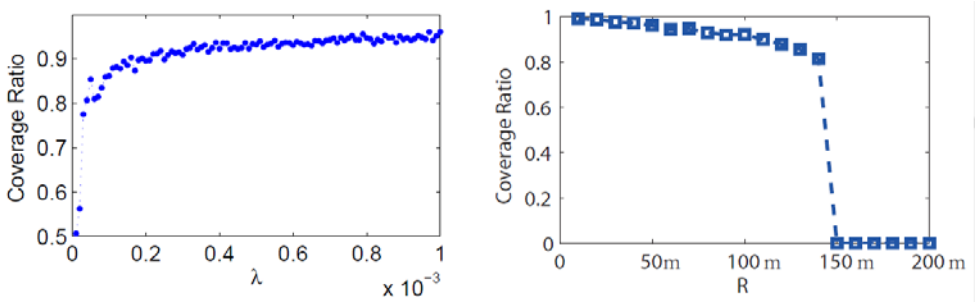


Fig. 6. Coverage ratio vs. (a) λ (R = 80m, ε_S = 92dB), and (b) R (λ = 0.0001, ε_S = 97dB). Here γ = 10dB, γ_e = –3dB.

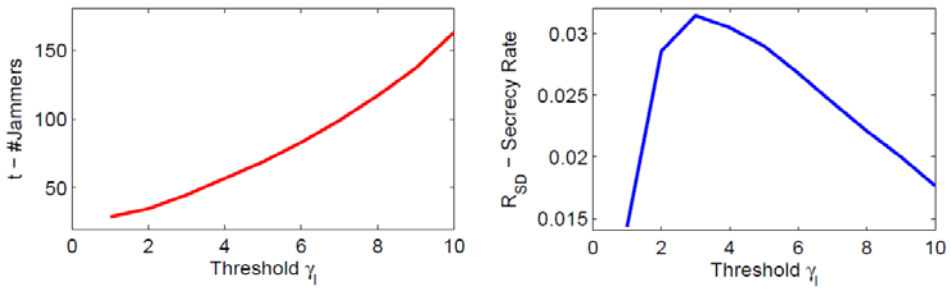


Fig. 7. Smart jamming; (a) Number of jammers vs the threshold γ; (b) The secrecy rate $\mathbf{R}_{SD}$ that can be achieved. Here R = 100m, γ_e = –3dB, λ_E = 0.00002, ε_S = 90dB, and the secrecy outage probability P_{SO} < 0.1.

[4] Coverage ratio is a ratio that measures the proportion of the audible region covered by jamming regions.

5.1.3 Secrecy rate maximization

Theoretically speaking, if there are t legitimate nodes in the audible region, the most secure method is to divide the message into t blocks，and send each block in a separate transmission with a different node as jammer. However, more rounds of transmission will lead to less secrecy rate $\mathbf{R}_{SD} = \frac{1}{t}[\log_2(1+\gamma_l) - \log_2(1+\gamma_e)]$. Hence there is a trade-off between secrecy rate and security.

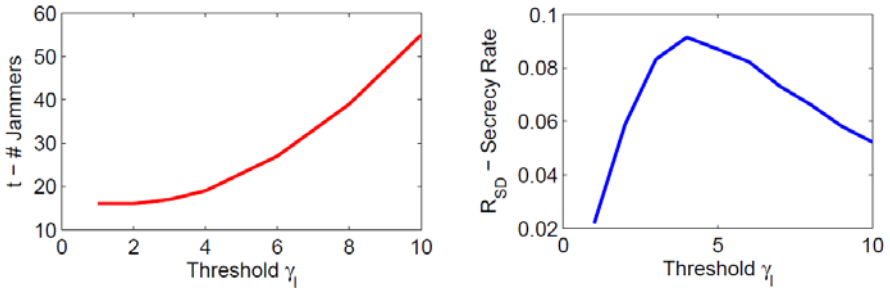
In practice, if we code message into t packet, only t jammers $B(S, R_E)$ are chosen randomly. This thinning procedure transforms the PPP of legitimate nodes with density λ into a PPP with density $\lambda' = \frac{t}{\pi R_E^2}$ (where R_E is the radius of the audible region). The expectation of the secrecy outage probability in this occasion is

$$\mathbb{E}(P_{SO}) = 1 - \exp[-\int_{\mathbb{B}_E} e^{-\frac{t}{\pi R^2} S_{E_i}} \lambda_E \mathrm{d}E_i]. \tag{2}$$

According to discussion, given $\mathbb{E}(P_{SO}) \to \varepsilon (0 < \varepsilon < 1)$ and γ_e, we can determine $\mathbf{R}_{SD}$ as follows:

$$\begin{aligned} \text{Maximize} \quad & \mathbf{R}_{SD} = \frac{1}{t}[\log_2(1+\gamma_l) - \log_2(1+\gamma_e)] \\ \textbf{s.t.} \quad & t < \pi R_E^2 \lambda \\ & \exp[-\int_{\mathbb{B}_E} e^{-\frac{t}{\pi R^2} S_{E_i}} \lambda_E \mathrm{d}E_i] > 1 - \varepsilon \end{aligned}$$

As illustrated in Fig. 7, given ε and γ_e, higher γ_l requires a larger number of jammers t, the Secrecy rate $\mathbf{R}_{SD}$ increases with the threshold γ_l at first then decreases. When $\gamma_l = 3$ in this setting, the achievable secrecy rate reaches its maximal value. To obtain the proper parameters γ_l and γ_e to achieve the maximal secrecy rate, a feasible method is leveraging a simplified machine learning algorithm [13] to derive their suboptimal values.



(a) t (b) $\mathbf{R}_{SD}$

Fig. 8. Cooperative jamming. (a) Number of jammers vs the threshold γ_l; (b) The secrecy rate $\mathbf{R}_{SD}$ that can be achieved. Here R = 100m, γ_e = −3dB, λ_E = 0.00002, ε_S = 90dB, and the secrecy outage probability $P_{SO} < 0.1$.

5.2 Cooperative Jamming Protocol

Since an exact expression for secrecy outage probability of cooperative jamming is hard to obtain, Monte Carlo simulations are conducted in different network configurations. As shown in Fig. 7, when we choose $\gamma_l = 3$ in smart jamming, the achievable secrecy rate reaches its maximal value, and we have to choose more than 50 jammers to satisfy the given secrecy outage probability. The main reason is due to the eavesdroppers near the sender and the receiver. Because the jamming region of the jammer near S or D is quite small, we need more jammers and rounds to jam the eavesdroppers in close proximity. We apply a helper-based two-stage scheme to jam the nearby eavesdroppers, the number of jammers can decrease significantly. As illustrated in Fig. 8, given the secrecy outage probability ε, the number of jammers in the cooperative jamming is less than the number of jammers in smart jamming, and the secrecy rate increases accordingly. For the network setting in the figure, when $\gamma_l = 4$, we need to choose less than 20 jammers to take part in cooperative jamming, and the achievable secrecy rate reaches its maximal value which is higher than the achievable secrecy rate of smart jamming protocol.

6. DISCUSSIONS

6.1 Network Scenarios

Physical-layer security approaches can provide solutions to some problems that can not be solved by conventional cryptography, such as quantum attacks, wireless communication with low probability of detection [14]. The purpose of the cooperative jamming protocol is designed to tackle the initial key establishment problem. Although this protocol is costly, it is not a frequently-used session key establishment method, only used in the initial stage of network establishment. The cooperative jamming protocol has a stronger security performance compared to conventional cryptography, and can be regarded as a supplement to traditional methods.

6.2 Parameter Selection

In practice, we can use a suboptimal method to determine the desired number of legitimate nodes to act as jammers t. The basic idea is that we treat the legitimate nodes in the audible region as reference points. If all the legitimate nodes in audible region are jammed, *i.e.*, they experience $SINR < \gamma_e$ when a packet is transmitted in the packet transmission stage, we regard the communication is secure and stop jamming with a new jammer. For example, let M be the message to deliver, Alice first sends a random number M_1 with a legitimate node as jammer meanwhile other legitimate nodes in the audible region measure SINR they see. If a node k experiences $SINRk < \gamma_e$, it reports to Alice. This process continues until all legitimate nodes in the audible region have been jammed and recorded by Alice. Then Alice transmits $M_{t+1} = M \oplus (M_1 \oplus \ldots \oplus M_t)$ (where M_i is the random number transmitted at ith round) to Bob. In this way, Alice can easily determine how many jammers should be chosen. In a dense network, the results of this method are quite similar to the analysis results.

A feasible method is leveraging a simplified machine learning algorithm to derive a suboptimal value. To reduce the resource consumption of nodes, we choose the nearest neighbor algorithm [15] which has quick convergence speed and low computational complexity to obtain the proper parameters. It is easily fails into local optimum rather than global optimum results. To solve this problem and reduce the computation complexity, we then use a simplified genetic algorithm [16] to approach the global optimum.

The basic idea is that: Firstly, to set the initial parameters, any potential sender utilizes the newest neighbor algorithm to learn two parameters γ_I and γ_e from his neighbors. Then, for any sender S, he selects n nodes among his one-hop neighbors. From each one-hop neighbor such as $node_k$, the sender S selects one of $node_k$'s neighbors whose communication power and corresponding receiver's SNR are most similar to him. He utilizes the nearest neighbor algorithm to optimize the parameters γ_I and γ_e by learning the parameters from these two-hop neighbors. Finally, we employ t and $RSD = 1/t\ [\log_2(1+\gamma_I) - \log_2(1+\gamma_e)]$ as two fitness functions to select the better parameters γ_I and γ_e by using a genetic algorithm. To reduce computational and storage complexity, we only use the mutation of the genetic algorithm. Every pair of parameters γ_I and γ_e changes on a small scale to create more possibilities. By iterating this method several times, node S can obtain a more optimal solution in the global scale. The parameters selection strategy can be described as follows:

Stage 1: Initial parameters settings First we install suboptimal (or empirical) parameters to a few nodes chosen randomly among the network, denoted $Node_1, \ldots, Node_n$. These nodes broadcast their γ_I, γ_e communication power and corresponding receiver's SNR to their neighbors. On receiving those broadcast parameters, other node, for instance, $Node_k$, learns the parameters $(\gamma_{I(k)}, \gamma_{e(k)})$ from $Node_1, \ldots, Node_n$ whose communication power and corresponding receiver's SNR are most similar to $Node_k$. $Node_k(\gamma_{I(k)}, \gamma_{e(k)})$ denotes $Node_k$ with the parameters γ_I and γ_e. The similarity between two nodes can be calculated by the Euclidean distance between their communication power and corresponding receiver's SNR. $Node_k(\gamma_{I(k)}, \gamma_{e(k)})$ generates $\gamma'_{I(k)}$ and $\gamma'_{e(k)}$ by changing on a smll scale, $(\gamma_{I(k)}, \gamma_{e(k)})$ by $\gamma'_{I(k)} = \gamma_{I(k)} \cdot \theta$, $\gamma'_{e(k)} = \gamma_{e(k)} \cdot \theta$. Here, θ denotes a random number in (0.9, 1.1) which is an empirical interval to realize the change of the parameters.

Stage 2: Parameter optimization For node S with parameters $(\gamma_{I(S)}, \gamma_{e(S)})$, he chooses n nodes randomly from his neighbors, and for each neighbor, node S chooses his two- hop neighbors whose communication power and corresponding receiver's SNR are most similar to S. He selects a pair of parameters $(\gamma_{I(best)}, \gamma_{e(best)})$ which achieves the highest R_{SD} in these two-hop neighbors and calculates corresponding t of this pair. By comparing $(\gamma_{I(best)}, \gamma_{e(best)})$ with $(\gamma_{I(S)}, \gamma_{e(S)})$, S then selects and stores the better parameters to act as his new $(\gamma_{I(S)}, \gamma_{e(S)})$. Finally, $(\gamma_{I(S)}, \gamma_{e(S)})$ changes on a small scale to generate a different pair of parameters $(\gamma'_{I(S)}, \gamma'_{e(S)})$ and node S computes t based on $(\gamma'_{I(S)}, \gamma'_{e(S)})$. S updates his parameters with the better parameters which can achieve a higher R_{SD}.

Algorithm 1 illustrates the detail of our parameters selection algorithm. Fig. 9 presents an example of simulation results on the parameter optimization strategy. 1,000 nodes are deployed randomly in a field to form a stationary Poisson point process Π on the plane $\subset \mathbb{R}_2$ in the simulation. From the figure, after each S communicates with D for

20 times, γ_I converges to 31, γ_e converges to −8.5, t converges to 4, and R_{SD} converges to 2. When S wants to communicate with D, S only needs 1 broadcast and a few unicasts to optimize the parameters ($\gamma_{I(S)}$, $\gamma_{e(S)}$).

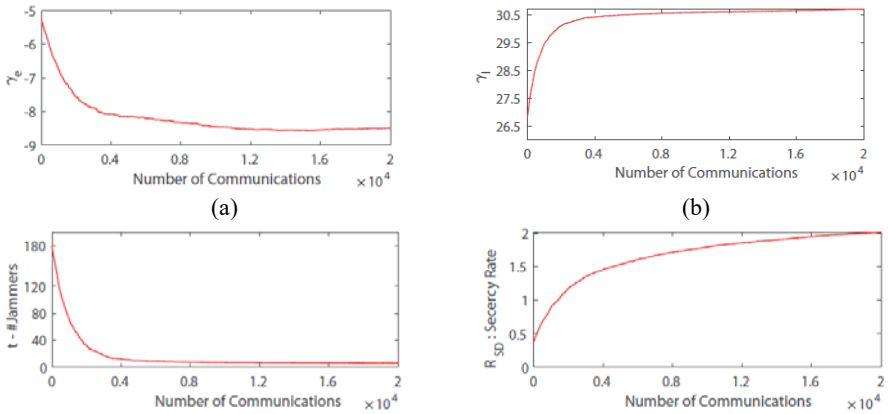


Fig. 9. Parameters Selection; (a)γ_e; (b) γ_I; (c) Average number of jammers; (d) The average secrecy rate $\mathbf{R}_{SD}$ that can be achieved. Here $R_{average}$ = 100m, choose 10 neighbors of each S, manual set (γ_I, γ_e) = {(30, −10), (30, −3), (10, −10), (10, −3)}, α = 3, λ = 0:00025, $\varepsilon_{S_{average}}$ = 80dB, each node communicates 20 times on average.

6.3 Collusive Attackers

The design of cooperative jamming is to defeat independent eavesdroppers located anyway in the network. As discussed in [10] (Lemma 1), if we choose one jammer to emit interfering signal at each round of transmission, the outage of probability of each round of jamming will be minimized. However, one jammer at each round of transmission does not have a strong ability to resist collusive attack because the jamming region at each round of jamming concentrates on a locally smaller area. To defeat several collusive attackers, the viable solution is to using multiple jammers at each round of transmission and increases the number of jamming rounds. This will be left as one of our future work.

7. CONCLUSIONS

Cooperative jamming emerges as a powerful tool to increase the security of wireless networks at the physical layer. In this paper we propose a cooperative jamming protocol that can deal with eavesdroppers anywhere in the network, even it locates close to the sender or the receiver. The results show that the proposed strategy can improve the secure performance and can be employed to establish initial connections in wireless networks. Additionally, considering the ability of each IoT nodes, we present an algorithm by using a simple machine learning and the idea of genetic algorithm to calculate the parameters of cooperative jamming. In our method, when S wants to communicate with D, S only needs 1 broadcast and a few unicasts to optimize the parameters ($\gamma_{I(S)}$, $\gamma_{e(S)}$).

ACKNOWLEDGEMENTS

This work was supported by the National Key Research and Development Program of China (2016YFB0800601), the National Natural Science Foundation of China (61671360) and Joint Funds of the National Natural Science Foundation of China (Key Program) (U1764263), in part by China 111 Project (B16037).

REFERENCES

1. L. B. Oliveira, F. M. Q. Pereira, R. Misoczki, D. F. Aranha, F. Borges, and J. Liu, "The computer for the 21st century: Security privacy challenges after 25 years," in *Proceedings of the 26th International Conference on Computer Communication and Networks*, 2017, pp. 1-10.
2. S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, Vol. 7, 2008, pp. 2180-2189.
3. X. Zhou and M. R. McKayr, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, Vol. 59, 2010, pp. 3831-3842.
4. Çağatay Çapar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proceedings of IEEE INFOCOM*, 2012, pp. 1152-1160.
5. O. Koyluoglu, C. Koksal, and H. E. Gamal, "On the secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, Vol. 58, 2012, pp. 3000-3015.
6. R. Soltani, B. Bash, D. Goeckel, S. Guha, and D. Towsley, "Covert single-hop communication in a wireless network with distributed artificial noise generation," in *Proceedings of the 52nd Annual Allerton Conference on Communication*, *Control*, *and Computing*, 2014, pp. 1078-1085.
7. R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *CoRR*, Vol. abs/1709.07096, 2017. http://arxiv.org/abs/1709.07096.
8. W. Mallat, W. H. Alouane, H. Boujemaa, and F. Touati, "Secure two-user af relaying networks using cooperative jamming," in *Proceedings of the 14th International Wireless Communications Mobile Computing Conference*, 2018, pp. 741-746.
9. L. Wang, H. Wu, and G. L. Stüber, "Cooperative jamming-aided secrecy enhancement in p2p communications with social interaction constraints." *IEEE Transactions on Vehicular Technology*, Vol. 66, 2017, pp. 1144-1158.
10. J. Liu, Z. Liu, Y. Zeng, and J. Ma, "Cooperative jammer placement for physical layer security enhancement," *IEEE Network*, Vol. 30, 2016, pp. 56-61.
11. Z. Liu, J. Liu, N. Kato, J. Ma, and Q. Huang, "Divide-and-conquer based cooperative jamming: Addressing multiple eavesdroppers in close proximity," in *Proceedings of the 35th Annual IEEE International Conference on Computer Communications*, 2016, pp. 1-9.
12. M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, Cambridge, UK, 2011.

13. J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Networks*, Vol. 61, 2015, pp. 85-117.
14. B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Communications Magazine*, Vol. 53, 2015, pp. 26-31.
15. J. M. Keller, M. R. Gray, and J. A. Givens, "A fuzzy *k*-nearest neighbor algorithm," *IEEE Transactions on Systems*, *Man*, *and Cybernetics*, Vol. SMC-15, 1985, pp. 580-585.
16. D. Beasley, D. R. Bull, and R. R. Martin, "An overview of genetic algorithms: Part 1, fundamentals," *University Computing*, Vol. 15, 1993, pp. 56-69.

Baihe Ma (马佰和) received his B.Sc. degree from Xidian University in 2016, and pursuing his M.S. Degree in Xidian University.

Zhihong Liu (刘志宏) received his B.Sc. degree from National University of Defense Technology (NUDT), China, in 1989, his M.S. degree in Computer Science from Air Force Engineering University, China, in 2001, and his Ph.D. degree in Cryptography from Xidian University in 2009. Now he is with the School of Cyber Engineering at Xidian University. His research areas include mobile computing and information security. (liuzhihong@mail.xidian.edu.cn)

Yong Zeng (曾勇) received his B.Sc, M.S., and Ph.D. degrees from Xidian University in 2000, 2003, and 2008, respectively. Since 2007 he has been with Xidian University as an Associate Professor. His research interests include cryptography, physical-layer security, and complex networks. (yzeng@mail.xidian.edu.cn)

Zhuo Ma (马卓) received his B.Sc., M.S., and Ph.D. degrees from Xidian University in 2003, 2006, and 2010, respectively. Since 2010 he has been with Xidian University as an Associate Professor. His research interests include physical-layer security, security protocol, and theory of trusted computing. (mazhuo@mail.xidian.edu.cn)

Hui Zhang (张辉) received his B.Sc. degree from Xidian University in 2016, and pursuing his M.S. degree in Xidian University.

Jianfeng Ma (马建峰) received the B.S. degree in Mathematics from Shaanxi Normal University, Xian, China, in 1985, and the M.S. and the Ph.D. degrees in Computer Software and Telecommunication Engineering from Xidian University, Xian, in 1988 and 1995, respectively. From 1999 to 2001, he was a Research Fellow with the Nanyang Technological University of Singapore, Singapore. He is currently a Professor and the Ph.D. Supervisor with the Department of Computer Science and Technology, Xidian University. His current research interests include information and network security, wireless and mobile computing systems, and computer networks.

Algorithm 1: Parameters Selection Algorithm

Require:

Set parameters $(\gamma_{I(1)}, \gamma_{e(1)})$, …, $(\gamma_{I(i)}, \gamma_{e(i)})$ to a few nodes $Node_1$, …, $Node_i$

Ensure:

The parameters of every nodes (γ_I, γ_e).

1: **for** node *Nodek* **do**

2: **for** $Node_1$ to *Nodei* **do**

3: Calculate the similarity, *i.e.*, $Distance_1$, …, $Distance_i$, between $Node_k$ and ($Node_1$, …, $Node_i$)

end for
Node$_k$($\gamma_{l(k)}$, $\gamma_{e(k)}$) learns the parameters from the node with min(*Distance*$_1$, …, *Distance*$_i$)
Generate the ($\gamma'_{l(k)}$, $\gamma'_{e(k)}$) by changing ($\gamma_{l(k)}$, $\gamma_{e(k)}$) on a small scale with a random number θ
Node$_k$ updates the parameters ($\gamma_{l(k)}$, $\gamma_{e(k)}$) with ($\gamma'_{l(k)}$, $\gamma'_{e(k)}$) and calculates the t in the situation of ($\gamma'_{l(k)}$, $\gamma'_{e(k)}$).
Choose n nodes (*Node*$_{Neib(1)}$, …, *Node*$_{Neib(n)}$) from the neighbors of *Node*$_k$ randomly
for *Node*$_{Neib(1)}$ to *Node*$_{Neib(n)}$ **do**
    In each *Node*$_{Neib}$'s neighbors, choose a two-hop neighbor *Node*$_{two\text{-}hop}$ whose communication power and corresponding receiver's SNR are most similar to *Node*$_k$
    Compare the R_{SD} of each node *Node*$_{two\text{-}hop}$, select the best two-hop neighbors *Node*$_{best}$($\gamma_{l(best)}$, $\gamma_{e(best)}$) who has the highest R_{SD}
end for
if R_{SD}($\gamma_{l(best)}$, $\gamma_{e(best)}$) > R_{SD}($\gamma_{l(k)}$, $\gamma_{e(k)}$) **then**
    $\gamma_{l(k)} = \gamma_{l(best)}$
    $\gamma_{e(k)} = \gamma_{e(best)}$
end if
($\gamma_{l(k)}$, $\gamma_{e(k)}$) changes in a small scale to generate the ($\gamma_{l(chang)}$, $\gamma_{e(change)}$) and calculate t of the two parameter pairs
if R_{SD} ($\gamma_{l(change)}$, $\gamma_{e(change)}$) > R_{SD} ($\gamma_{l(k)}$, $\gamma_{e(k)}$) **then**
    $\gamma_{l(k)} = \gamma_{l(change)}$
    $\gamma_{e(k)} = \gamma_{e(change)}$
end if
Node$_k$ save the parameters ($\gamma_{l(k)}$, $\gamma_{e(k)}$)
end for