Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 1832051, 11 pages
https://doi.org/10.1155/2017/1832051

Research Article

A Location Prediction-Based Helper Selection Scheme for Suspicious Eavesdroppers

Yan Huo,[1] Yuqi Tian,[1] Chunqiang Hu,[2,3] Qinghe Gao,[1,3] and Tao Jing[1]

[1]*School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing, China*
[2]*School of Computer Science, Chongqing University, Chongqing, China*
[3]*Department of Computer Science, The George Washington University, Washington, DC, USA*

Correspondence should be addressed to Yan Huo; yhuo@bjtu.edu.cn

Received 20 July 2017; Revised 14 October 2017; Accepted 31 October 2017; Published 4 December 2017

Academic Editor: Chaokun Wang

This paper aims to improve security performance of data transmission with a mobile eavesdropper in a wireless network. The instantaneous channel state information (CSI) of the mobile eavesdropper is unknown to legitimate users during the communication process. Different from existing work, we intend to reduce power consumption of friendly jamming signals. Motivated by the goal, this work presents a location-based prediction scheme to predict where the eavesdropper will be later and to decide whether a friendly jamming measure should be selected against the eavesdropper. The legitimate users only take the measure when the prediction result shows that there will be a risk during data transmission. According to the proposed method, system power can be saved to a large degree. Particularly, we first derive the expression of the secrecy outage probability and set a secrecy performance target. After providing a Markov mobile model of an eavesdropper, we design a prediction scheme to predict its location, so as to decide whether to employ cooperative jamming or not, and then design a power allocation scheme and a fast suboptimal helper selection method to achieve targeted and efficient cooperative jamming. Finally, numerical simulation results demonstrate the effectiveness of the proposed schemes.

1. Introduction

As a promising technology, an Internet of Things (IoT) network offers opportunities to directly transform physical things into information world without human interventions [1–3]. It may be composed of billions of low-end devices that connect everyday objects and surrounding environments. These devices equipped with various sensors and actuators can be connected to the Internet via heterogeneous wireless networks. We can exploit the devices to collect meaningful and suitable data conveniently to achieve information sharing, computing, and controlling remotely. Obviously, these data contain sensitive and private information such as social relationships and financial transactions [4]. As a result, the security of IoT networks is of critical importance for the wide deployment and acceptance of big data services in the future.

Due to properties of broadcast communication and signal superposition in wireless networking scenarios, it is difficult to shield transmitted signals from unauthorized receivers as well as protect legitimate receivers from unintended overlapping of multiple signals. These facts make security become a vital issue, especially in the openness of the wireless medium. As a result, many works have been done to meet security requirements. These works mainly exploit cryptographic techniques at the upper layers of wireless networks [5–7]. As a complement to the measures at the upper layers, the idea of physical layer security (PLS) is proposed and has been widely discussed in recent years. To be specific, PLS is to exploit channel characteristics to enhance secure performance of data transmission, which means the inherent randomness of the noise and communication channels are used to limit the amount of information to be extracted by unauthorized receivers [8]. A number of studies in this field propose to address the problem of either active or passive attacks in wireless networks [9]. As for passive attacks, eavesdropping is a well-known security risk in the whole

communication process. The strategies of antieavesdropping, as Wyner described in his classic wiretap channel model [10], have recently regained substantial research attention [11–15].

To the best of our knowledge, many studies aiming at eavesdropping usually design different schemes to ensure secure transmission according to whether the channel state information (CSI) of the eavesdropper is known to legitimate users. For one thing, it is possible to design a targeted and efficient security scheme when the CSI of the eavesdropper is known to legitimate users, which means the exact location of the eavesdropper is known. Because of knowing the eavesdropper's CSI, the equation of the secrecy performance metric can be deduced into a convex optimization problem that can be solved. For another, however, the design of a secure scheme becomes challenging if the CSI of the eavesdropper is partially or even totally unknown to legitimate users. The general solution is to guarantee the robust secrecy performance in the worst case and to design a suboptimal algorithm. Also, there exist other tactical methods, such as the artificial noise alignment schemes [16] that do not use the knowledge of the eavesdroppers channel gains. Among these schemes, few of them consider a network model with a mobile eavesdropper, whose CSI is unknown to legitimate users because of the unexpected movement.

A mobile eavesdropper is like an unexpected risk to the communication process of legitimate users. Due to the continuous random movement in the network all the time, it is difficult to decide when the eavesdropper will move close to the legitimate transmitter and start to wiretap information. This kind of wiretapping exists widely in our real life, especially mobile social networks. Data transmission among legitimate users should be kept from information stealing by an unauthorized passerby. Regarding this issue, many PLS-based security schemes are designed by transmitting jamming signals during the whole communication process. With enough and accurate CSI of an eavesdropper, these schemes are achievable and effective at the expense of a large amount of power consumption. Different from these schemes, we want to deal with this secure issue in a more practical situation. The legitimate users do not have to act in a defensive way during the whole communication period. They only have to take a security measure against the eavesdropper when they find out the risk of privacy disclosure. Such behavior can save system power to a great degree.

To address these challenges, we have proposed a novel risk prediction scheme in our conference paper [17]. This scheme is aimed at the network model with a mobile eavesdropper, whose CSI is unknown to the legitimate users. After studying the mobile eavesdropping model, we analyze the network model and derive an expression of the secrecy outage probability as the security metric and set a target secrecy outage probability for the risk decision in this paper. Considering the mobile path prediction of the eavesdropper, next, a Markov chain is exploited to set up a Markov mobile model of the eavesdropper. According to the mobile model, we perform the prediction by exploiting the history movement information of the eavesdropper. After predicting the location where the eavesdropper will be, we exploit the prediction results to decide whether the eavesdropper might be harmful to data transmission later or not. If it will be, the corresponding security measures will be taken against it, and the power allocation scheme is designed to achieve maximum secrecy capacity. At last, this paper also demonstrates the effectiveness of our scheme via a series of simulations. The main contributions of this paper can be summarized as follows:

(i) We propose a Markov chain-based location prediction scheme for a mobile eavesdropper by its history movement information.

(ii) Based on prediction results, we formulate an optimization problem to allocate power for transmitter and helper so as to obtain the maximum achievable secrecy rate after selecting a suitable helper.

(iii) In order to enhance the friendly jamming efficiency of a helper, we design a fast suboptimal helper selection algorithm that takes into account both algorithm complexity and secrecy performance.

The rest of the paper is organized as follows. The related works are described in Section 2. We present the system model and derive the expression of the secrecy outage probability in Section 3, followed by the detailed illustration of our location prediction-based helper selection scheme in Section 4. Moreover, the numerical simulation is shown and analyzed in Section 5. Finally, we conclude this article in Section 6.

2. Related Work

Jamming is generally treated as an unfavorable factor in wireless communications [18]. It may overlap with information signals, which finally impacts decoding performance. In spite of the negative side, some studies suggested that friendly jamming can be used as an effective tool to protect information signals from malicious adversaries. From the perspective of the wiretap channel model, perfect secrecy can be achieved when channel condition of legitimate users is better than that of eavesdroppers. Accordingly, the basic idea of friendly jamming strategies is to degrade the wiretap channel quality of eavesdroppers.

This idea was first introduced in [19]. Negi and Goel attempted to exploit artificially generated noise to degrade the eavesdroppers channel but not to affect the information signals. They discussed the secrecy capacity over the multiple transmit antennas scenario and the multiple helpers scenario. Following this work, a number of studies have been performed. Wang et al. proposed a targeted jamming scheme against the eavesdropper in [20]. In the work, they designed an asymptotic power allocation method to solve an achievable secrecy rate maximization problem. Besides, they provided a jammer selection method to make a decision for reducing the abuse rate of jammers. Similarly, Zhang et al. also investigated secure communications for cooperative cognitive radio networks in [21]. They studied a joint time and power allocation scheme to achieve the maximum secrecy rate for relay-jammer scenario and then presented a weight and time allocation strategy for cluster-beamforming

scenario. All these proposed schemes are designed under the assumption that the eavesdropper channel condition is known. In that case, the jammer among legitimate users can make target jamming and optimizing power allocation is possible to achieve.

Yet, a more practical assumption is the unknown CSI of eavesdroppers. Obviously, it is more difficult to achieve target jamming and performance. Some researchers exploited the secrecy outage probability and ϵ-outage secrecy capacity to describe the system secrecy performance. According to the above two indicators, a series of suboptimal algorithms were studied. In [22], Li and Ma considered a worst-case robust secrecy rate maximization problem with incomplete Eve's CSI. They presented a suboptimal but safe solution to an outage-constrained robust secrecy rate maximization problem. In [23], Jiang et al. derived closed-form expressions of secrecy indicators for unknown CSI of eavesdroppers. Also, they developed a joint zero-forcing and successive interference cancellation method to analyze the individual secrecy performance for a multiple access wiretap channel. A friendly cooperative jamming strategy for IoT networks with imperfect eavesdropper's CSI was also investigated in [24]. The authors in [24] transformed this challenge into the worst-case eavesdropper's CSI and formulated a two-stage robust optimization problem to find the optimal solution.

Although there still exist numerous studies on the unknown or imperfect CSI of eavesdroppers [25–27], all of these only focused on the wiretap by static eavesdroppers. The more general case is that eavesdroppers may have other behaviors. For instance, they can still wiretap information signals when they are in mobile state. In that case, the CSI of mobile eavesdroppers may be changeable with the changing location. In this paper, we intend to analyze and predict the mobility of eavesdroppers. With the mobility prediction, we can decide whether it may steal the information via the legitimate channel. In terms of the prediction of the mobile path, the Markov chain is a good way to realize it. In [28], Fazio and Marano employed a distributed set of hidden Markov chains to predict the probable cells that a mobile node may visit in the future. Besides, [29] also formulated a Markov-history model for realistic mobility of nodes in a network. All these studies inspire us to predict the location (i.e., CSI) of a mobile eavesdropper. According to this, a power allocation and jammer selection scheme is put forward. To the best of our knowledge, this work is the first one to investigate the PHY layer security issue in the mobile eavesdroppers scenario.

3. System Model

Considering a typical wireless wiretapping network, there exists a legitimate transceiver pair (called Alice and Bob), an eavesdropper (Eve), and several helpers, shown in Figure 1. Each of them in the network is equipped with a single omnidirectional antenna. Alice sends its message to Bob via a legitimate channel h_{ab}. At that time, Eve, a random mobile passive adversary, is likely to come within the area around Alice to wiretap Alice's message through a wiretapping channel h_{ae}. To prevent this wiretapping attack, a helper

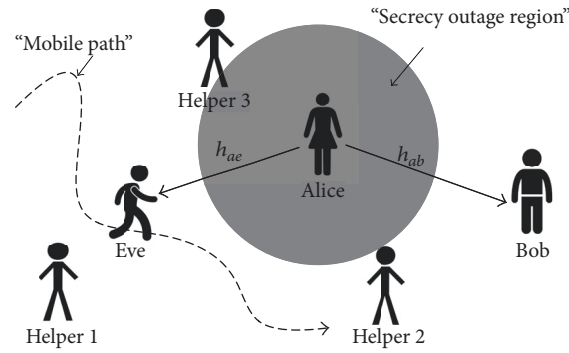

Figure 1: Description of the network layout.

may be selected to broadcast jamming signals (e.g., artificial noises) to degrade the reception quality of Eve, which is also called a friendly jamming strategy.

In this scenario, we define d_{ab} as the distance between Alice and Bob and d_{ae} as the distance between Alice and Eve. The legitimate channel (from Alice to Bob) is denoted by h_{ab}, and the wiretap channel (between Alice and Eve) is denoted by h_{ae}. We assume both channels are modeled as Rayleigh fading channels. Signal to interference plus noise ratio (SINR) of both legitimate and unauthorized users is decided by path-loss and fading effects [30]. Then, we can first characterize channel vectors as follows:

$$h = L \cdot f(G), \tag{1}$$

where L is the path-loss coefficient and $f(G)$ is the channel power fading coefficient. Here, L can be characterized by the path-loss exponent α and the distance d between two communicating parties; that is,

$$L = \frac{c}{d^{\alpha}}, \tag{2}$$

where c is the path-loss constant. In addition, $f(G)$ follows exponential distribution; that is,

$$f(G) = \lambda e^{-\lambda G}. \tag{3}$$

Without loss of generality, the coefficient G is modeled as a random variable with unit mean, and hence $\lambda = 1$.

When Alice selects a helper to be the friendly helper to preserve its privacy transmission to Bob, the received signals of Bob and Eve are

$$\begin{aligned} y_{ab} &= \sqrt{P_s} h_{ab} s + \sqrt{P_J} \omega_J^H h_{jb} s + n_{ab}, \\ y_{ae} &= \sqrt{P_s} h_{ae} s + \sqrt{P_J} \omega_J^H h_{je} s + n_{ae}, \end{aligned} \tag{4}$$

respectively, where P_s and P_J are information signal power and jamming signal power, respectively. ω_J^H is the beamforming vector at Alice to transmit the jamming signal, which is used to eliminate the interference of the jamming signal at Bob. n_{ab} and n_{ae} are the additive white Gaussian noise (AWGN) with zero mean and variance σ_n^2 at Bob and Eve,

respectively. The SINR at Bob and at Eve can be, respectively, presented as

$$\mathrm{SINR}_{ab} = \frac{P_s \left\| h_{ab} \right\|^2}{\sigma_n^2 + P_J \omega_J^H h_{jb} h_{jb}^H \omega_J},$$
$$\mathrm{SINR}_{ae} = \frac{P_s \left\| h_{ae} \right\|^2}{\sigma_n^2 + P_J \omega_J^H h_{eb} h_{eb}^H \omega_J}. \tag{5}$$

Accordingly, the secrecy capacity at Bob can be deduced as follows, which is defined as the difference between the mutual information of the legitimate channel and that of the wiretap channel.

$$\begin{aligned} C_s &= \left[I\left(s; y_{ab}\right) - I\left(s; y_{ae}\right) \right]^+ \\ &= \left[\log_2\left(1 + \mathrm{SINR}_{ab}\right) - \log_2\left(1 + \mathrm{SINR}_{ae}\right) \right]^+, \end{aligned} \tag{6}$$

where $\{z\}^+ = \max[z, 0]$. $I(s; y_{ab})$ and $I(s; y_{ae})$ denote the mutual information of the channels between Alice and Bob and between Alice and Eve, respectively. Secrecy capacity is the maximum achievable rate between the legitimate transmitter and receiver that can guarantee perfect secrecy. It gives the upper bound of the transmission rate subject to constraints of unauthorized users. Obviously, the communication link is secure when $C_s > 0$. On the contrary, it has the risk of information leakage because Eve experiences a better channel condition than Bob.

However, it is hard for Alice to be aware of the channel information of Eve, h_{ae}, in a passive eavesdropping mode. As a result, we can characterize the secrecy outage probability. It is the probability that the instantaneous secrecy capacity is less than a target secrecy rate R_s:

$$P_{\mathrm{out}}\left(R_s\right) = P\left(C_s < R_s\right). \tag{7}$$

According to [31], we get the following expression:

$$P_{\mathrm{out}}\left(R_s\right) = 1 - \frac{\mathrm{SINR}_{ab}}{\mathrm{SINR}_{ab} + 2^{R_s}\mathrm{SINR}_{ae}} e^{-(2^{R_s}-1)/\mathrm{SINR}_{ab}}. \tag{8}$$

Here, P_{out} is a function of SINR_{ab} and SINR_{ae}. Since SINR is a function of d as shown in (1) to (3), we can deduce that $P_{\mathrm{out}}(R_s)$ is a function of d_{ab} and d_{ae}. Taking the locations of Alice, Bob, and Eve into account, the secrecy outage regions corresponding to different secrecy outage probabilities should be calculated.

Since Alice and Bob are communicating with their locations settled, secrecy outage probabilities of other locations in the network can be calculated. If we can predict the location where the randomly moving eavesdropper will be later, we can calculate the secrecy outage probability of the predicted location and decide whether it may steal the information from Alice or not. With the decision, we can take measures to guarantee security beforehand. The criterion of the decision is based on specific secure requirements. Here, we set a target secrecy outage probability γ_{th} to define whether Eve will be harmful to the communication later. The value of γ_{th} is set based on actual requirements of users or administrators in the network. For various network scenarios, this value can be set variously. When $P_{\mathrm{out}}(R_s) < \gamma_{\mathrm{th}}$, we consider that the communication is secure. Conversely, when $P_{\mathrm{out}}(R_s) > \gamma_{\mathrm{th}}$, we consider that the communication is suffering from the risk of being eavesdropped and we need to take some security measures.

4. A Location Prediction-Based Helper Selection Scheme

In this section, we propose a prediction scheme to predict where Eve will be in its later movement, so as to decide whether security measures should be taken against Eve to guarantee security. As we discussed in Section 2, the Markov chain shows effectiveness for mobility prediction in such network scenarios. Hence, we decide to exploit it to achieve our prediction. We first present a detailed illustration of our scheme. Then, we introduce the metrics of our scheme.

4.1. The Prediction Scheme. To give a clear illustration of our scheme, we first introduce some definitions. As we assume that Eve keeps moving in an area all the time, its mobile path is continuous. We predict Eve's location at intervals of one moment, where one moment is set to be one length of time. That is to say, the mobile path that we predict is a discrete one. We consider that the area is composed of an infinite number of points (locations), and Eve moves from one location to another from the current moment to the next moment. This is called one-step movement. For example, we can define $t-1$ as the current moment, t as the next moment, and so on. Because Eve may keep moving randomly in the area all the time, the history information of its movement can be of great usefulness to the prediction. We assume that the history movement information of Eve is known. Note that when there is a newly coming eavesdropper that provides no pattern for mobile path, the prediction scheme is unsuitable. We just treat it as a threat and make the jammer selection as the method shown in Sections 4.2 and 4.3.

In the prediction scheme, we first use the Markov chain to set up a mobile model of Eve, and then try to extract some characteristics from the statistics of history movement information. This is called the transition matrix in the Markov model. Finally, we calculate and compare the probabilities of locations at the next moment to decide which location Eve will move to.

As for setting up a Markov mobile model, it is obvious that every location in the area can be seen as a state. However, it is invalid to carry out the prediction scheme in the case of infinite number of locations as the state space. It inevitably results in high computation complexity, which may cost huge resources. Thus, to improve the efficiency of our prediction scheme, we divide the whole area into an $M \times M$ gridding, as shown in Figure 2. We define each grid as a state. When Eve is moving in the same grid, we consider that it stays at the same state. The length of every grid is set to be 1, and the distance between each pair of adjacent grids is set to be 1. And we assume that the grid is the minimum unit of the area.

To better elaborate the process of modeling, we use a 3×3 gridding as an example. The example gridding is shown

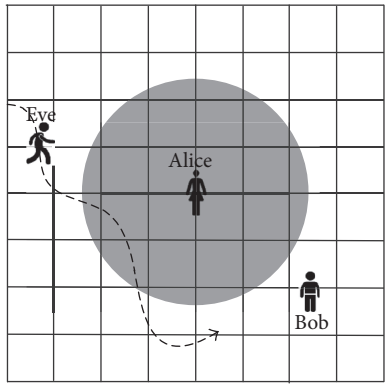

Figure 2: The grid division of the network.

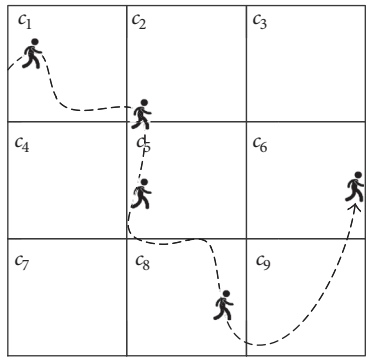

Figure 3: A 3 × 3 example gridding model.

in Figure 3. Here, we number the grids as $c_1, c_2, \ldots, c_9$. The state space of this Markov model is $\mathrm{SP}_{\mathrm{e.g.}} = \{c_1, c_2, \ldots, c_9\}$. And the corresponding transition matrix is a 9 × 9 matrix $P_{\mathrm{e.g.}}$, written as

$$P_{\mathrm{e.g.}} = \begin{bmatrix} p_{11} & p_{12} & 0 & p_{14} & p_{15} & 0 & 0 & 0 & 0 \\ p_{21} & p_{22} & p_{23} & p_{24} & p_{25} & p_{26} & 0 & 0 & 0 \\ 0 & p_{32} & p_{33} & 0 & p_{35} & p_{36} & 0 & 0 & 0 \\ p_{41} & p_{42} & 0 & p_{44} & p_{45} & 0 & p_{47} & p_{48} & 0 \\ p_{51} & p_{52} & p_{53} & p_{54} & p_{55} & p_{56} & p_{57} & p_{58} & p_{59} \\ 0 & p_{62} & p_{63} & 0 & p_{65} & p_{66} & 0 & p_{68} & p_{69} \\ 0 & 0 & 0 & p_{74} & p_{75} & 0 & p_{77} & p_{78} & 0 \\ 0 & 0 & 0 & p_{84} & p_{85} & p_{86} & p_{87} & p_{88} & p_{89} \\ 0 & 0 & 0 & 0 & p_{95} & p_{96} & 0 & p_{98} & p_{99} \end{bmatrix}, \quad (9)$$

where p_{uv} $(1 \le u \le 9, 1 \le v \le 9)$ denotes the transition probability in the ith row and the jth column of the transition matrix $P_{\mathrm{e.g.}}$, which is the probability that Eve is in grid c_i the former moment and chooses to move to grid c_j the latter moment. For the one-step movement, Eve can only move from its current grid to the adjacent grids or stay still (which means it is moving in the same grid). Thus, some of the probabilities in the transition matrix are meant to be 0. For example, if Eve stays in c_1 at the current moment, it can only be in c_1, c_2, c_4, or c_5 at the next moment and cannot be in c_3, c_6, c_7, c_8, or c_9. So, the probabilities $p_{13}, p_{16}, p_{17}, p_{18}$, and p_{19} in the transition matrix $P_{\mathrm{e.g.}}$ are 0.

Now back to the $M \times M$ gridding Markov mobile model, we are going to discuss how to get the transition matrix of it. We use N_{total} to denote the total number of grids, where $N_{\mathrm{total}} = M \times M$. Like the example above, the state space of this $M \times M$ gridding model is $\mathrm{SP} = \{c_1, c_2, \ldots, c_{N_{\mathrm{total}}}\}$. And the corresponding transition matrix is an $N_{\mathrm{total}} \times N_{\mathrm{total}}$ matrix. We use p_{ij} $(1 \le i \le N_{\mathrm{total}}, 1 \le j \le N_{\mathrm{total}})$ to denote the transition probability in the ith row and the jth column of the transition matrix P. Every p_{ij} can be calculated based on the statistics of history movement information. We use N_{ij} $(1 \le i \le N_{\mathrm{total}}, 1 \le j \le N_{\mathrm{total}})$ to denote the total number of times that Eve moves from grid c_i to grid c_j in its movement history; thus, p_{ij} can be expressed as

$$p_{ij} = \frac{N_{ij}}{\sum_{j=1}^{N_{\mathrm{total}}} N_{ij}} \quad \left(1 \le i, j \le N_{\mathrm{total}}\right). \quad (10)$$

After we get the transition matrix P, which is also called the one-step transition matrix, we can further derive the n-step transition matrix $P(n)$. By exploiting $C-K$ equation, we can see that

$$P(n) = P \cdot P(n-1) = P(n-1) \cdot P. \quad (11)$$

Thus,

$$P(n) = P^n. \quad (12)$$

We consider that the location of Eve at the next moment is related to the history movement information, that is, the transition matrix and its states of former k steps of movements. It is obvious that if the moment of the state is nearer to the next moment, this state may have more influence on Eve's next moment movement. And the states of the far past moments can be negligible. There exists an optimal value of k which can lead to the best prediction performance. We can obtain the value by simulation experiences. Based on the foregoing analysis, we decide to use a weighted way to calculate the probabilities of every location at the next moment; that is,

$$X(t) = a_1 S(t-1) P + a_2 S(t-2) P^2 + \cdots + a_k S(t-k) P^k, \quad (13)$$

where $X(t)$ is a $1 \times N_{\mathrm{total}}$ matrix, containing the probabilities of all states. $S(m)$ $(t-k \le m \le t-1)$ is a set containing states' information. It represents the state Eve was at the former mth moment before the next moment. It is also a $1 \times N_{\mathrm{total}}$ matrix. Its value at the first row with the mth column is 1, while other values are 0. $a_1, a_2, \ldots, a_k$ are weighted coefficients, representing different influence degrees that movements at the former 1st, 2nd, …, kth moment before the next moment have on the next moment's movement, respectively. Note that we consider that the influence degree is a relative value. Thus, the summation of $a_1, a_2, \ldots, a_k$ is not 1.

Initialization:
$SP = \{c_1, c_2, \ldots, c_{N_{\text{total}}}\}$;
$S = \{s_1, s_2, \ldots, s_t\}$;
N_{ij} $(1 \le i \le N_{\text{total}}, 1 \le j \le N_{\text{total}})$.
(1) Calculate transition probabilities P_{ij} by N_{ij};
(2) Calculate n step transition matrix $(1 \le n \le k)$, $P, P^2, \ldots, P^k$;
(3) Calculate the predicted probabilities $X(t)$;
(4) Set $X_v \leftarrow 0$
(v are sequence numbers of unreachable states);
(5) Find $(X_max = \max(X(t)))$
(6) Calculate $P_{\text{out}}(R_s)$ with max;
(7) **if** $P_{\text{out}}(R_s) > \gamma_{\text{th}}$ **then**
(8) Take security measures against Eve;
(9) **else**
(10) Break;
(11) **end if**
(12) Modify N_{ij} for the next time prediction.

Algorithm 1: The risk prediction rule.

When obtaining $X(t)$, we can compare these probabilities to decide which state Eve will be at the next moment. As the previous assumption of Eve's movement state (move to the adjacent grids or stay still), we can set the probabilities of those unreachable states to be 0 and only have to compare the probabilities of potential states. The state which the maximum probability is corresponding to is where Eve will be at the next moment. Noting that the result is the location we predict, it may not be the location which Eve actually moves to at the next moment. Every time Eve performs a movement, we need to count N_{ij} again to get the new statistics of the history movement information and to modify the transition matrix, so as to get a more accurate prediction result next time.

Since the location of Eve at the next moment is predicted, we can use this result to decide whether we should take measures against Eve. The way is basically mentioned in Section 3. In particular, we first substitute the predicted location of Eve to the calculation process of the secrecy outage probability $P_{\text{out}}(R_s)$ and then check whether $P_{\text{out}}(R_s)$ is smaller than the threshold probability γ_{th}. If the answer is yes, we consider that the communication is secure; else, we take security measures. The whole decision process is summarized as Algorithm 1.

4.2. Power Allocation for Cooperative Friendly Jamming. According to the above discussion, Alice may be aware of the predicted CSI of Eve. Assuming that the helper has been selected, we would like to design a prediction-based power allocation algorithm to optimize the proportion of P_s and P_J in the total power P_T. The goal of the allocation algorithm is to achieve maximum secrecy rate at Bob; that is,

$$\begin{aligned} \max_{P_s, P_J} \quad & C_s \\ \text{s.t.} \quad & P_s + P_J \leqslant P_T \\ & P_s + P_J > P_T. \end{aligned} \tag{14}$$

In general, jamming signals are deliberately designed in nullspace of the legitimate channel. In this manner, the selected helper may adjust its transmit covariance matrix to jam Eve and simultaneously null out interference at Bob. As a result, the reception SINR at Bob can be described as follows:

$$\text{SINR}_{ab} = \frac{P_s \left\| h_{ab} \right\|^2}{\sigma_n^2}. \tag{15}$$

Accordingly, if we assume that P_s and P_J are much greater than the noise power σ_n^2, we would like to deduce the above optimization as

$$\begin{aligned} \max_{P_s, P_J} \quad & \frac{P_s \left\| h_{ab} \right\|^2}{\sigma_n^2} \times \frac{P_J \omega_J^H h_{eb} h_{eb}^H \omega_J}{P_J \omega_J^H h_{eb} h_{eb}^H \omega_J + P_s \left\| h_{ae} \right\|^2} \\ \text{s.t.} \quad & P_s + P_J \leqslant P_T \\ & P_s + P_J > P_T. \end{aligned} \tag{16}$$

Obviously, (16) is a convex analysis optimization. Here, we employ the method of Lagrange multipliers and the Karush-Kuhn-Tucker (KKT) conditions to provide a closed-form solution of this mathematical optimization. We first introduce an auxiliary function of the optimization objective in (16),

$$\begin{aligned} L\left(P_s, P_J, \lambda\right) = & \frac{P_s \left\| h_{ab} \right\|^2}{\sigma_n^2} \times \frac{P_J \omega_J^H h_{eb} h_{eb}^H \omega_J}{P_J \omega_J^H h_{eb} h_{eb}^H \omega_J + P_s \left\| h_{ae} \right\|^2} \\ & + \lambda \left(P_T - P_s - P_J\right), \end{aligned} \tag{17}$$

where λ is a Lagrange multiplier, and then solve the corresponding gradient expressions

$$\nabla_{P_s, P_J, \lambda} L\left(P_s, P_J, \lambda\right) = 0. \tag{18}$$

Initialization:
The predicted Eve's CSI;
$S_{\text{helper}} = \{J_1, J_2, \ldots, J_N\}$; C_{s_i} $(1 \le i \le N)$.
(1) Determine whether there exist a risk of secure communication between Alice and Bob based on Algorithm 1;
(2) Calculate secrecy rates $\{C_{s_i}\}$ for all helpers based on the predicted Eve's CSI;
(3) Find a helper J^* as a jammer by comparing every C_{s_i};
(4) Calculate information signal power P_s and jamming signal power P_J by (19) and (20) for the J^* helper,
(5) The J^* helper broadcasts artificial noises to jam Eve.

Algorithm 2: The fast helper selection scheme.

Note that (18) amounts to solving three equations in three unknowns. As a result, we can find the following optimal solutions:

$$P_s = \frac{P_T \sqrt{\omega_J^H h_{je} h_{je}^H \omega_J}}{\sqrt{\omega_J^H h_{je} h_{je}^H \omega_J} + \left\| h_{ae} \right\|}, \tag{19}$$

$$P_J = \frac{P_T \left\| h_{ae} \right\|}{\sqrt{\omega_J^H h_{je} h_{je}^H \omega_J} + \left\| h_{ae} \right\|}, \tag{20}$$

$$\lambda = \frac{\sqrt{\omega_J^H h_{je} h_{je}^H \omega_J} \left\| h_{ae} \right\|^2}{\sigma_n^2 \left(\sqrt{\omega_J^H h_{je} h_{je}^H \omega_J} + \left\| h_{ae} \right\| \right)}. \tag{21}$$

Finally, we can calculate the maximum achievable secrecy rate, C_s, by the following equation:

$$C_s = \left[\log_2 \left(\frac{P_T}{\sigma_n^2} \frac{\sqrt{\omega_J^H h_{je} h_{je}^H \omega_J} \left\| h_{ae} \right\|^2}{\left(\sqrt{\omega_J^H h_{je} h_{je}^H \omega_J} + \left\| h_{ae} \right\| \right)} \right) \right]^+. \tag{22}$$

4.3. A Fast Suboptimal Helper Selection Scheme. In order to ensure secure communication from Alice to Bob, a suitable helper may be selected to broadcast jamming signals. We assume there are several helpers in the network, and one of them can satisfy the security requirements if it broadcasts jamming signals. Obviously, this helper should not be selected randomly due to the requirement of secrecy rate. On the contrary, the selected helper should have enough jamming power to prevent Eve from getting information illegally. Here, we would like to design a fast suboptimal helper selection scheme for the mobile Eve.

In the above subsection, the maximum achievable secrecy rate has been calculated via (22). For every helper, we are able to obtain different C_s according to different Eve locations. Intuitively, Alice may select the helper as a jammer that can help Alice obtain the maximum achievable secrecy rate when Eve is in a certain location. Thus, the helper selection scheme can be described as a mathematical expression; that is,

$$J^* = \underset{J^* \in S_{\text{helper}}}{\arg \max} C_s, \tag{23}$$

where J^* represents the selected helper and S_{helper} is the set of all candidate helpers in the network. Accordingly, the secrecy rate at Bob can be computed as follows:

$$C_s^* = \log_2 \left(\frac{\sigma_n^2 + P_s^* \left\| h_{ab} \right\|^2}{\sigma_n^2} \times \frac{\sigma_n^2 + P_J^* \omega_{J^*}^H h_{j^*e} h_{j^*e}^H \omega_{J^*}}{\sigma_n^2 + P_J^* \omega_{J^*}^H h_{j^*e} h_{j^*e}^H \omega_{J^*} + P_s^* \left\| h_{ae} \right\|^2} \right), \tag{24}$$

where h_{j^*e} and ω_{J^*} denote the channel state vector and the beamforming vector between the selected helper J^* and Eve, respectively. P_s^* and P_J^* are the information signal power and the jamming signal power that are calculated by the optimal power allocation algorithm.

Obviously, we can exploit the exhaustive search method to find the optimal helper J^*. This method is suitable for the scenario of static eavesdropping. Nevertheless, Eve is a mobile passive eavesdropper in our system model. The process of searching for and selecting the optimal jammer needs to be repeated, which may undoubtedly result in high computational complexity. To deal with the challenge, we intend to design a suboptimal helper selection scheme.

According to (24), we are aware that C_s is mainly affected by h_{je}. Also, the channel state vector h_{je} is inversely proportional to the distance from the jammer to Eve. As a result, we can select the nearest helper from Eve as the jammer without hesitation; that is,

$$J^* = \underset{J^* \in S_{\text{helper}}}{\arg \max} d_{je}. \tag{25}$$

The whole process of helper selection can be summarized as Algorithm 2.

Remark 1. There is still an extreme case where there are a huge number of helpers in the network. To reduce the computational complexity, Alice may stop searching once it finds a helper that satisfies the security requirement. In other words, $P_{\text{out}}(R_s)$ that a helper provides is lower than γ_{th}. The feasible solution is as follows:

$$J^* = \underset{J^* \in S_{\text{helper}}}{\arg} C_s \left(P_{\text{out}} \left(R_s \right) \le \gamma_{\text{th}} \right). \tag{26}$$

5. Numerical Simulation

5.1. Production Evaluation Metrics. As for a prediction scheme, obviously, an important issue is the accuracy. When it comes to our system model, what we care about most is the accuracy of the risk prediction, not simply the accuracy of the position prediction. We want to know how possible it is when the prediction tells us there are or there are not any risks in the communication process. Actually, we can employ a sum of two different errors to describe the accuracy of prediction. The first error is caused by misdetection. In that case, Eve is actually in the secrecy outage region although the prediction result says the communication is secure, which will lead to information leakage. Second, a false alarm also introduces prediction errors. This may let the system take unnecessary security measures and waste system power. According to the above description, we define an index P_e to represent the error level of our prediction scheme; that is,

$$P_e = \frac{\sum S(D_0 \mid H_1) + \sum S(D_1 \mid H_0)}{N_{\text{count}}}, \tag{27}$$

where 1 means true (there exist risks in the communication process) and 0 means false. D_1 denotes that the decision result is true, and D_0 denotes that the decision result is false. H_1 denotes that the actual result is true, and H_0 denotes that the actual result is false. $S(a \mid b)$ denotes the amount of the states with the actual state a and the predicted state b. N_{count} denotes the total time of the prediction. And the simulation results in Section 5 show the error level of our scheme.

5.2. Prediction Performance Analysis. In this subsection, simulation results are shown to verify the effectiveness of our prediction scheme (here, we first employ the transition probability of Eve's location to simulate its movement in a predefined secrecy outage region; this probability can be computed by the historical data collected by Alice, which will be presented in our future work; also, in the future work, we will provide real-life datasets based on typical social applications, e.g., WeChat or Facebook, to conduct further experiments and analyses). We observe the error probability P_e in scenarios with different settings of parameter values, which are the number of grids of the area N_{total}, the number of the considered former steps of movements before the next moment k, and the number of history movements N. Those parameters may cause varying degrees of influences on the error probability of the prediction scheme. Therefore, we intend to divide the area into a $10 \times 10, 20 \times 20$, and 30×30 gridding, respectively. In other words, the area, respectively, consists of 100, 400, 900 grids. Besides, we set k to be 3, 5, 10 and N to be 2000, 4000, 8000 and set the target secrecy outage probability γ_{th} to be 0.8, whose value can be adjusted based on actual requirements.

Figure 4 provides a description of P_e with different values of N_{total} and different values of k. As for the relationship between P_e and N_{total}, it is shown that P_e is monotonously decreasing with N_{total}, indicating that as the division unit of the area goes smaller, the accuracy degree of the prediction scheme goes higher. There exist two reasons to illustrate the result. One is that when the division unit of the area is large, this grid division will lead to a take-security-measure decision if Eve moves around the edge of the target secrecy outage region. Both the neighboring area in the target secrecy outage region and the neighboring area out of the target secrecy outage region can be in the same grid, which impacts the decision. Another reason is that when the division unit of the area is smaller, the number of paths in the same grid goes smaller. As a result, the history movements can provide more information for setting up the corresponding Markov mobile model, so as to perform a more accurate prediction.

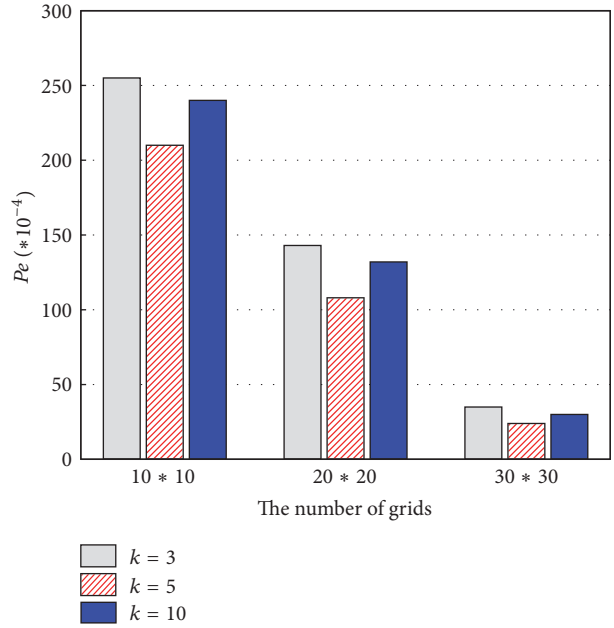

Figure 4: P_e versus N_{total} and k. Parameters setting: $N = 2000$, $N_{\text{total}} = 10 \times 10, 20 \times 20, 30 \times 30$, and $k = 3, 5, 10$.

Besides, as for the relationship between P_e and k, the result in Figure 4 also demonstrates that as the value of k increases, the value of P_e goes down at first and then goes up. Obviously, the value of P_e is at the minimum if $k = 5$. The result indicates that in the prediction process it may give rise to a better accuracy performance without employing more previous steps of movements. When too much former steps of movements are considered, which are not that related to the movement of Eve at the next moment, this consideration will impact the prediction result reversely.

In Figure 5, we present a description of P_e with different values of N_{total} and different values of N. It is shown that P_e is monotonously decreasing with N, indicating that the error probability of the prediction scheme decreases along with the increase in the number of history movements. This is reasonable because the history movements are crucial to the generation of the transition matrix of the Markov chain. More history movements can provide more information about the mobile characteristics of Eve. Thus, more historical movement information data should make the transition matrix more specific to represent those mobile characteristics. In one word, the prediction result with more history movement information can be more accurate.

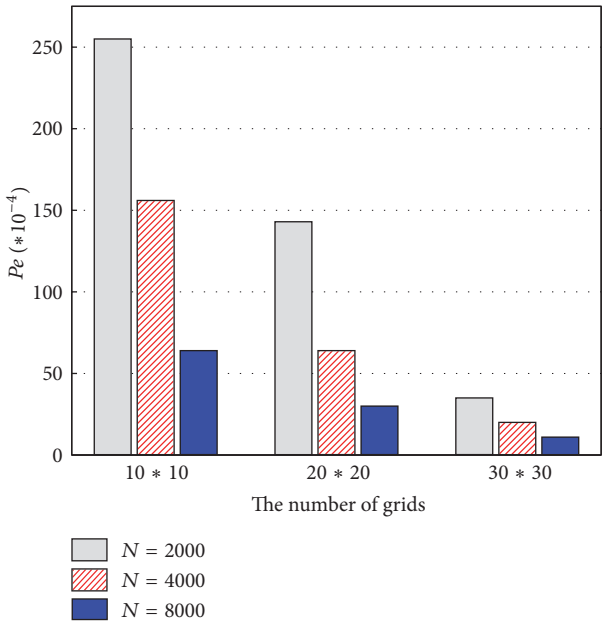

FIGURE 5: P_e versus N_{total} and N. Parameters setting: $k = 3$, $N_{\text{total}} = 10 \times 10, 20 \times 20, 30 \times 30$, and $N = 2000, 4000, 8000$.

From these simulation results, we can see that the value of the error probability in our proposed risk prediction scheme is in a relatively acceptable range; that is to say, the secrecy performance of this risk prediction scheme can be guaranteed. If we want to achieve a better secrecy performance, we need to divide the area into more grids and to gather and utilize more history movement information, thus to lower the value of the error probability.

5.3. Secrecy Performance Analyses. In this section, we conduct several simulations to verify the secrecy performance of the proposed power allocation scheme as well as the corresponding helper selection method. Without loss of generality, we assume that channels among all nodes in the network are modeled as Rayleigh fading channels. Also, there exists the additive white Gaussian noise (AWGN) with mean 0 and variance σ_n^2. The CSI of legitimate nodes is known to each other, while that of Eve has been estimated by the location prediction scheme.

We first study the secrecy performance of the optimal helper selection scheme and the suboptimal scheme. Supposing Eve is at a position in the secrecy outage region, we conduct 30 simulations to compare the difference between two schemes in the case of various distributions of helpers.

It can be seen from Figure 6 that the difference of secrecy rate between two selection schemes is not significant. And they even have the same secrecy rate sometimes (i.e., the two schemes choose the same helper as a jammer). Yet, compared with the optimal helper selection scheme, the suboptimal one can drastically reduce the computational complexity of the selection procedure in the case of similar security rate.

Next, we investigate the effect of total system power on the secrecy rate when the number of helpers is 10. Here, we

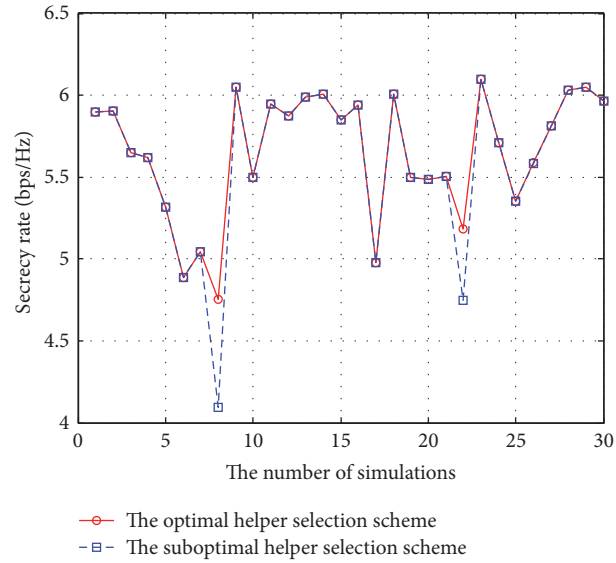

FIGURE 6: The instantaneous secrecy rate between two selection schemes, with $N_{\text{helper}} = 10$ and $P_T = 30$ dB.

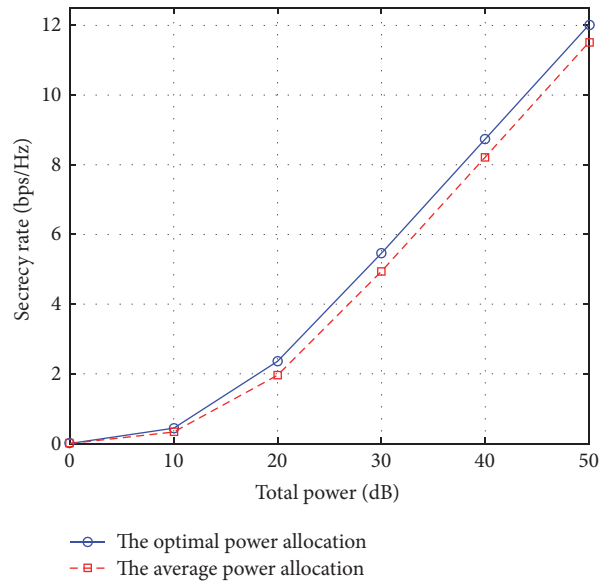

FIGURE 7: Secrecy rate versus P_T, with $N_{\text{helper}} = 10$.

assume the total power $P_T = 10, 20, 30, 40, 50$ dB. In Figure 7, we are aware that the secrecy rate increases as the total power grows for two schemes. This is because the stronger jamming power may further deteriorate the receiving signal quality of Eve. Besides, it is obvious that the proposed optimal power allocation scheme has better secrecy performance than the average method.

As a benchmark, we also derive the effect of the number of helpers on the secrecy rate by running the experiment with $N_{\text{helper}} = 5, 10, 20, 30, 40, 50$ to compare the performance of our power allocation scheme and the average scheme. In Figure 8, along with the increase in the number of nodes in

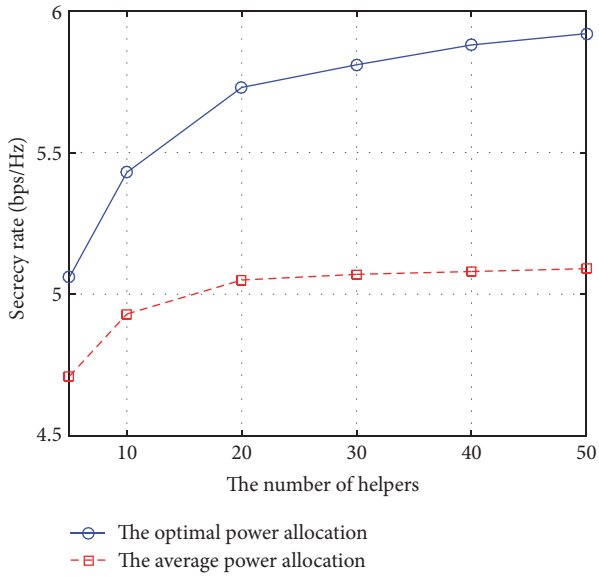

FIGURE 8: Secrecy rate versus N_{helper}, with $P_T = 30$ dB.

the network, we can see that the secrecy rates of both schemes are growing fast at first and then flatten. The reason is that there may be some adjacent helpers as the number of helpers in the network increases. These adjacent helpers may have a similar impact on Eve.

According to these simulation results, we can find that the proposed schemes are effective in achieving the requirement of secrecy rate at the legitimate receiver. Also, the proposed suboptimal helper selection scheme can save the system resources while ensuring the secure communication of legitimate channel.

6. Conclusion

This paper proposes a location prediction-based helper selection scheme to address physical layer security in the communication scene with a suspicious mobile eavesdropper, the case where the eavesdropper's CSI is unknown to the legitimate users. In this scheme, we exploit the secrecy outage probability as the security metric, set a target secrecy outage probability for the risk decision, and perform the prediction by using the Markov chain. With a Markov mobile model of the eavesdropper set up, the history movement information of the eavesdropper is employed to form the transition matrix. Besides, the position of the eavesdropper at the next moment we want to predict is related to both the history movement information and its own former states. Based on this, a weighted method is used to do the prediction. Next, a power allocation scheme and a fast suboptimal helper selection method are developed to interfere with a mobile eavesdropper. In order to demonstrate the effectiveness and the secrecy performance of our scheme, a set of simulations are conducted. These simulation results illustrate that the prediction scheme is with low error probability. Also, secrecy performance analyses demonstrate that the optimal power allocation with suboptimal helper selection scheme can achieve the requirement of secrecy rate.

Note that, in this paper, we only discuss the mobile eavesdropper in a basic single-antenna network model. As for future work, we are going to reinvestigate such problem in a MIMO (multiple-input-multiple-output) system and come up with a specific physical layer security strategy.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Fundamental Research Funds for the Central Universities (Grants nos. 2017JBM004 and 2016JBZ003), the National Natural Science Foundation of China (Grants nos. 61471028, 61572070, 61371069, and 61702062), and the Open Project of Science and Technology on Communication Networks Laboratory (no. KX162600033).

References

[1] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, 2016.

[4] Z. He, Z. Cai, J. Yu, X. Wang, Y. Sun, and Y. Li, "Cost-efficient strategies for restraining rumor spreading in mobile social networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2789–2800, 2017.

[5] L. Zhang, Z. Cai, and X. Wang, "FakeMask: A Novel Privacy Preserving Approach for Smartphones," *IEEE Transactions on Network and Service Management*, vol. 13, no. 2, pp. 335–348, 2016.

[6] X. Zheng, Z. Cai, J. Li, and H. Gao, "Location-privacy-aware review publication mechanism for local business service systems," in *Proceedings of the IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, pp. 1–9, Atlanta, GA, USA, May 2017.

[7] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and Efficient Data Communication Protocol for Wireless Body Area Networks," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 2, pp. 94–107, 2016.

[8] S. A. A Mukherjee, J. Fakoorian, and A. L. Huang, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[9] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Communications Magazine*, vol. 18, no. 2, pp. 66–74, 2011.

[10] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[11] Z. Li, T. Jing, X. Cheng, Y. Huo, W. Zhou, and D. Chen, "Cooperative jamming for secure communications in MIMO Cooperative Cognitive Radio Networks," in *Proceedings of the IEEE International Conference on Communications, ICC 2015*, pp. 7609–7614, UK, June 2015.

[12] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1728–1740, 2013.

[13] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.

[14] H.-M. Wang and F. Liu, "Secrecy signal and artificial noise designs in cellular network," in *Proceedings of the IEEE China Summit and International Conference on Signal and Information Processing, ChinaSIP 2015*, pp. 273–277, China, July 2015.

[15] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-Aided Secure Communication in Massive MIMO Rician Channels," *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6854–6868, 2015.

[16] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1568–1571, 2013.

[17] Y. Tian, Y. Huo, C. Hu, Q. Gao, and T. Jing, "A Location Prediction-based Physical Layer Security Scheme for Suspicious Eavesdroppers," in *Wireless Algorithms, Systems, and Applications*, vol. 10251 of *Lecture Notes in Computer Science*, pp. 854–859, Springer International Publishing, Cham, 2017.

[18] S. Kim, "Cognitive radio anti-jamming scheme for security provisioning IoT communications," *KSII Transactions on Internet and Information Systems*, vol. 9, no. 10, Article ID A4177, pp. 4177–4190, 2015.

[19] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proceedings of the 62nd Vehicular Technology Conference, VTC 2005*, pp. 1906–1910, USA, September 2005.

[20] C.-L. Wang, T.-N. Cho, and F. Liu, "Power allocation and jammer selection of a cooperative jamming strategy for physical-layer security," in *Proceedings of the 2014 79th IEEE Vehicular Technology Conference, VTC 2014-Spring*, Republic of Korea, May 2014.

[21] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, "Cooperative networking towards secure communications for CRNs," in *Proceedings of the 2013 IEEE Wireless Communications and Networking Conference, WCNC 2013*, pp. 1691–1696, China, April 2013.

[22] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, 2013.

[23] K. Jiang, T. Jing, F. Zhang, Y. Huo, and Z. Li, "ZF-SIC Based Individual Secrecy in SIMO Multiple Access Wiretap Channel," *IEEE Access*, vol. 5, pp. 7244–7253, 2017.

[24] Z. Li, T. Jing, L. Ma, Y. Huo, and J. Qian, "Worst-case cooperative jamming for secure communications in CIoT networks," *Sensors*, vol. 16, no. 3, article no. 339, 2016.

[25] J. Yang, Q. Li, Y. Cai, Y. Zou, L. Hanzo, and B. Champagne, "Joint Secure AF Relaying and Artificial Noise Optimization: A Penalized Difference-of-Convex Programming Framework," *IEEE Access*, vol. 4, pp. 10076–10095, 2016.

[26] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K.-K. Wong, "Secrecy performance analysis for tas-mrc system with imperfect feedback," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1617–1629, 2015.

[27] Z. Zhu, Z. Chu, Z. Wang, and I. Lee, "Outage Constrained Robust Beamforming for Secure Broadcasting Systems with Energy Harvesting," *IEEE Transactions on Wireless Communications*, vol. PP, no. 99, 2016.

[28] P. Fazio and S. Marano, "Mobility prediction and resource reservation in cellular networks with distributed Markov chains," in *Proceedings of the 8th IEEE International Wireless Communications and Mobile Computing Conference, IWCMC 2012*, pp. 878–882, Cyprus, August 2012.

[29] S. Bitam and A. Mellouk, "Markov-history based modeling for realistic mobility of vehicles in VANETs," in *Proceedings of the 2013 IEEE 77th Vehicular Technology Conference, VTC Spring 2013*, Germany, June 2013.

[30] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, 2011.

[31] H. Li, X. Wang, and W. Hou, "Security enhancement in cooperative Jamming using compromised secrecy region minimization," in *Proceedings of the 2013 13th Canadian Workshop on Information Theory, CWIT 2013*, pp. 214–218, Canada, June 2013.