Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 202 (2022) 15–20

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Identification, Information and Knowledge in the Internet of Things, 2021

A Friendly Jamming Handover Scheme for a Conscious Mobile Eavesdropper in IoT systems

Dequan Shen, Yan Huo, Qinghe Gao*

School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing and 100044, China

Abstract

Physical layer security (PLS) in Internet-of-Things (IoT) has attracted great attention in recent years. As an important and intrinsic property in an IoT system, node mobility is not fully investigated when designing a PLS scheme. Existing PLS works with mobility are designed with typical random mobile models, which cannot represent a real scenario. Considering this challenge, we propose a friendly jamming handover scheme to protect the downlink transmission from a controller to an actuator, with the help of multiple cooperative jammers to fight against a mobile conscious eavesdropper. In particular, we first introduce a conscious eavesdropping model (CEM) to characterize a real mobile wiretapping scenario. Second, we present a handover scheme to enhance security in a mobile scenario and then define handover efficiency to discuss the handover performance. Finally, numerical results are provided to verify the effectiveness of the proposed handover scheme, which demonstrates that our scheme can efficiently fight against a conscious mobile eavesdropper.

Keywords: Friendly jamming handover; conscious eavesdropping model; handover efficiency; physical layer security; Internet of Things.

1. Introduction

Internet of Things (IoT) is expected as a promising technique to achieve ubiquitous connectivity and intelligent information processing for the intelligent future life [1, 2]. Since the IoT is penetrating our daily life, the security and privacy are of the utmost importance [3–5]. Physical layer security (PLS) techniques have been attracted growing interests for the scenarios with resource-constrained IoT sensors and actuators [6–8]. A PLS scheme taking advantage of the unique properties of wireless channels can guarantee the information-theoretic communication security, regardless of the computing capability of eavesdroppers [9]. Various PLS schemes have been investigated to enhance secrecy in

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000.
E-mail address: qhgao@bjtu.edu.cn

1877-0509
10.1016/j.procs.2022.04.003

IoT networks, including multi-antenna beamforming and precoding [10, 11], artificial noise (AN) [12], intermittent cooperative jamming [13], and sociability-enabled PLS [8, 14, 15].

Yet, most existing works only considered PLS for a static IoT system in many scenarios. In these cases, nodes including users and eavesdroppers are stable, which does not satisfy an actual scenario. Recently, there has been a growing interest to investigate PLS with mobility models. The most commonly used mobility models are the random waypoint(RWP) model, random direction (RD) model and border move (BM) model [16, 17], which can be studied through their spatial node distribution functions (SPDF). The work of [16] investigated secrecy outage probability (SOP) and ergodic secrecy capacity for a random mobile receiver with Rayleigh fading , where the receiver follows the RWP and RD modelS. In [17], the authors investigated a secrecy throughput maximization problem for a mobile IoT node with an RWP and RD model. The work in [18] derived exact expressions of SOP in the presence of multiple RWP moving interfering nodes with Nakagami-m fading. For millimeter wave (mmWave) communication, the authors analyzed the average secrecy rate and SOP performances with a single RWP mobile receiver in [19]. It is verified that RWP mobility improves the secrecy rate in mmWave communication scenario. However, neither users or eavesdroppers move in a certain area without explicit intent in a real scenario. Moreover, existing works focus on mobility analysis and secrecy optimization without utilizing the AN technology to degrade the reception of eavesdroppers. When a conscious eavesdropper moves and tries to find a better eavesdropping location, network secrecy of the systems implementing traditional cooperative jamming schemes may be more easily compromised. To cope with these challenges, we introduce a conscious mobile model (CEM) for an eavesdropper, named as conscious eavesdropping model, and propose a jamming handover scheme to fight against mobile wiretapping with the help of cooperative jammers. Our contributions are as follows.

- We introduce the conscious eavesdropping model to represent a real world subhuman eavesdropper and compare it with the traditional RWP model which has been proved as the best mobile model in the existing mobile models. We derive the explicit expression of the connection probability and secrecy outage probability.
- We propose a novel jamming handover scheme to confront a mobile eavesdropper. Then, we introduce a metric called as handover efficiency (HE) to analyze the performance of our scheme.
- We provide numerical results of SOP and HE to prove that our scheme can efficiently confront a conscious mobile eavesdropper.

2. Models

2.1. System Model

In this paper, we consider a downlink IoT network as shown in Fig. 1, where a controller (Alice) located in the center of a specific circular area Ω with radius R intends to transmit a confidential message to a legitimate actuator (Bob) in Ω, while a passive mobile eavesdropper (Eve) is moving in Ω and trying to eavesdrop the confidential data signals. We assume that Alice employs a guard zone with radius R_{Guard} which is shown by the dotted line circle, and Eve can be detected when moves into the guard area.

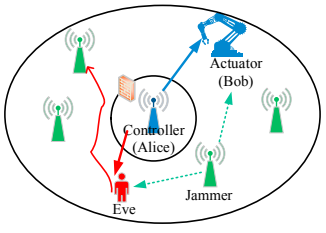

Fig. 1. System model.

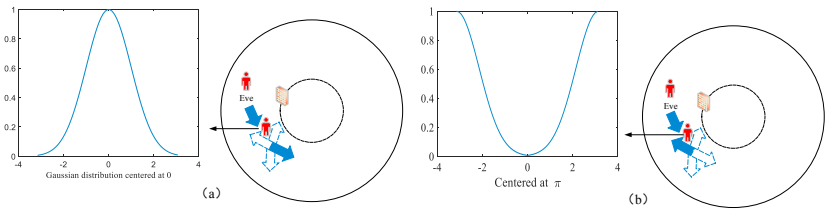

Fig. 2. (a) Eve with CEM in improving phase. (b) Eve with CEM in decreasing phase.

We assume that Alice, Bob and Eve are equipped with single antenna, in the presence of multiple cooperative jammers equipped with N_j antennas. The set of the jammers is defined as $\kappa \triangleq \{1, 2, \ldots, K\}$. When the communication starts, we randomly activate a jammer, radiating jamming signal to confuse the Eve. When Eve moves far away from

the jammer or close to the Alice, we consider that a handover happens to the Eve, with the aid of other jammers. That means when the distance between the jammer and Eve increases to a certain degree, received signal-to-interference-plus-noise ratios (SINRs) at Eve will be larger than a threshold, a closer jammer should take over the jamming task and emit jamming signals to impair the eavesdropper's performance as a result. We assume that all wireless channels are independent and experience a large scale path loss governed by the exponent $a > 2$, and all receivers' perfect CSI are available.

2.2. Mobility Model

The RWP is a classical mobility model. In the model, Eve randomly chooses a point D_0 as a start point in the circular region Ω. Moreover, it randomly selects a coordinate D_1 (D_1 is uniformly distributed in Ω) as its next destination and moves to the destination with a constant speed v_1 (v_1 is uniformly chosen from $[v_{min}, v_{max}]$). After arriving at the destination, Eve can choose to stop for a random pause time $t_{p,1}$ ($t_{p,1}$ that is randomly chosen from $[t_{p,min}, t_{p,max}]$). Then it moves to another destination D_2 with a new speed v_2 following the same rules. Eve continues this process until the end.

Different from the RWP model, we next present the conscious eavesdropping model. We assume that Eve knows Alice's location and the guard zone, but the deployment of the jammers is well protected. The conscious Eve keeps exploring in the moving area refer to the SINR at the previous coordinate. First, Eve randomly chooses a point D_0 as a start point in the area and randomly selects a direction θ from $[-\pi, \pi]$. Considering that Eve moves to converge at a good eavesdropping position, we let Eve move a fixed distance d every time so that Eve can easily get to that position. Due to the three sigma principle of Gaussian distribution, the consciousness of Eve is approximately modeled as a Gaussian function with zero mean and unit variance. As is shown in Fig. 2, the phase of Eve contains two cases. If the current SINR of Eve is greater than the previous, Eve is considered in the improving phase and randomly select an additional angle $\Delta\theta$ from $[-\pi, \pi]$ according to the gaussian distribution. If the current SINR of Eve is less than the previous, Eve is considered in the decreasing phase and randomly select an additional angle $\Delta\theta$ from $[0, 2\pi]$ according to the Gaussian distribution centered at π. Eve adds the additional angle $\Delta\theta$ onto the direction θ as its next direction and moves a fixed distance d. Then Eve chooses the direction according to the changing SINR and continues the process until the end.

3. Problem Formulation

The distance between Alice and Eve is assumed to be d_{AE}, when Bob is with a distance of d_{AB} to Alice ($0 < d_{AE}, d_{AB} < R$). The distance between the kth jammer and Eve is assumed to be d_{Ek}, when Bob is with a distance of d_{Bk} to the kth jammer ($0 < d_{Ek}, d_{Bk} < R$). Due to the mobility of Eve, d_{AE} and d_{Ek} ($k \in \kappa$) is time varying during the communication period. Without loss of generality, we assume that Jammer 1 activates first. The received signal at Bob and Eve can be expressed as follows.

$$y_B = \frac{\sqrt{P_A}}{d_{AB}^{a/2}} h_{AB} s + \frac{\sqrt{P_{J1}}}{d_{B1}^{a/2}} h_{B1} z + n_B, \qquad y_E = \frac{\sqrt{P_A}}{d_{AE}^{a/2}} h_{AE} s + \frac{\sqrt{P_{J1}}}{d_{E1}^{a/2}} h_{E1} z + n_E, \tag{1}$$

where P_A and P_{J1} denote the transmit power of Alice and Jammer 1. h_{AB} and h_{AE} denote the channels from Alice to Bob and Eve, which follows Rayleigh fading with a zero-mean unit-variance circularly symmetric complex Gaussian random variable. $h_{B1} \in C^{N_j}$ and $h_{E1} \in C^{N_j}$ denote channels from Jammer 1 to Bob and Eve. s denotes a data symbol with $E[|s|^2] = 1$, $z \in C^{N_j}$ is the AN vector, and n_B and n_E represent independent complex Gaussian noise with zero-mean unit-variance at Bob and Eve.

Note that z should be properly designed to null out the interference at Bob because the AN may disrupt Eve and Bob simultaneously. Let $[h_{B1}, H]$ be an orthogonal basis, where $H \in C^{N_j \times (N_j - 1)}$. By introducing H, then we can design z as $z = Hx$. Here, $x \in C^{N_j - 1}$ is a Gaussian noise vector with a distribution $C\mathcal{N}(0, 1)$. According to (1), the SINRs at Bob and Eve are given as follows

$$\gamma_B = \frac{P_A |h_{AB}|^2}{d_{AB}^a}, \qquad \gamma_E = \frac{P_A |h_{AE}|^2 d_{AE}^{-a}}{1 + P_{J1} \|h_{E1} H\|^2 d_{E1}^{-a}}. \tag{2}$$

The above equations show that the SINR at Eve is related to d_{AE} and d_{E1}. If d_{AE} reduces or d_{E1} increases, the SINR at Eve will increase. In other words, Eve can move to find a better eavesdropping location. Thus, we should take necessary measures to enhance communication security. In this paper, we consider a handover happens on Eve and the jammer closest to the Eve always takes over the jamming task, when the **SINR constraint:** $\gamma_E > \beta$ holds, where β is the SINR threshold for the jamming handover. We assume that Jammer 2 takes over the jamming task from Jammer 1 after a period of movement. According to (2), the SINR at Eve after handover happens is given by $\overline{\gamma_E} = \frac{P_A|h_{AE}|^2 d_{AE}^{-a}}{1+P_{J2}\|h_{E2}H\|^2 d_{E2}^{-a}}$, where P_{J2} represents the transmit power of Jammer 2.

Utilizing the well-known Wyner's wiretap encoding scheme, we encode the secret messages before transmission to enhance information security. Let R_b denote the overall codeword rate at Alice and R_s the rate of secret message. Then $R_E = R_b - R_S$ denotes the rate of redundant information which can be exploited for counter-eavesdropping. The follow-up security analysis is based on whether the channel has the capacity to support the information rate. According to (2), capacities of the legitimate channel and the eavesdropping channel can be expressed as follows.

$$C_B(d_{AB}, d_{B1}) = \log(1 + \gamma_B(d_{AB}, d_{B1})), \qquad C_E(d_{AE}, d_{E1}) = \log(1 + \gamma_E(d_{AE}, d_{E1})). \tag{3}$$

Naturally, the instant secrecy capacity under Rayleigh fading channel is $C_S = C_B - C_E = \log(1 + \gamma_B(d_{AB}, d_{B1})) - \log(1 + \gamma_E(d_{AE}, d_{E1}))$.

According to the above analysis, we now declare the secrecy metrics studied in this paper.

- *Secrecy Outage Probability (SOP):* If the Alice-Eve link can support the redundant rate R_E, the secrecy performance will be compromised. Thus, the secrecy outage probability is defined as the capacity of the Alice-Eve link lies above the redundant rate, i.e.,$P_{so} \triangleq \mathbb{P}\{C_E > R_E\} = \mathbb{P}\{\gamma_E > \beta_E\}$, where $\beta_E \triangleq 2^{R_E} - 1$ denotes the SINR threshold for Eve. Note that two thresholds β_E and β are different. β_E is used to decide whether the secrecy outage event occurs or not and calculate SOP, while β is used to decide whether the jamming handover happens or not. In this paper, we analyze the secrecy outage probability to figure out the secrecy performance of our system.
- *Handover Efficiency (HE):* Friendly jamming handover is the main research point of this paper. We introduce a metric called as the handover efficiency to represent the handover performance. The handover efficiency is defined as average secrecy improvement per handover time compared with the non-handover system, i.e.,$\Psi \triangleq \frac{\hat{P}_{so} - \hat{P}^*_{so}}{\sigma}$. Here, σ is the handover times after Eve moves for a period of time, $\hat{P}_{so}$ denotes the SOP with handover scheme after integrating over d_{AE} and d_{Ek}, and $\hat{P}^*_{so}$ denotes the SOP with non-handover.

4. Secrecy Analysis and Numerical Results

4.1. Secrecy Analysis

When Eve moves into a certain area, both handover and mobility make it difficult to derive the expression of SOP. We first consider a non-handover scenario that only Jammer 1 is activated to secure the communication link. Eve is with a distance d_{AE} to Alice and with a distance d_{E1} to Jammer 1. According to (2), the explicit expression of SOP in a non-handover static scenario is $P_{so} = (\frac{\lambda_1}{\lambda_1 + \lambda\beta_E})^{\alpha_1} \frac{1}{e^{\lambda\beta_E}}$, where $\lambda = \frac{d_{AE}^a}{P_A}$, $\lambda_1 = \frac{d_{E1}^a}{P_{J1}}$, and $\alpha_1 = N_j - 1$.

Proof: $P_A|h_{AE}|^2 d_{AE}^{-a} \sim Exp(\frac{d_{AE}^a}{P_A})$ holds for $|h_{AE}|^2 \sim Exp(1)$, $\|h_{E1}H\|^2 \sim \Gamma(N_j - 1, 1)$ holds for $|h_{A1}|^2 \sim Exp(1)$, and an orthogonal basis $H \in C^{N_j \times (N_j - 1)}$ is designed for $[h_{B1}, H]$. Using (2), we can conclude that $\gamma_E \sim \frac{\exp(d_{AE}^a/P_A)}{1+\Gamma(N_j-1, d_{Ek}^a/P_{Jk})}$. Similar to [6], the complementary cumulative distribution function(CCDF) of γ_E can be expressed as $F(\tau) = (\frac{d_{E1}^a/P_{J1}}{d_{E1}^a/P_{J1} + \tau d_{AE}^a/P_A})^{N_j - 1} \frac{1}{\exp(\tau d_{AE}^a/P_A)}$. This completes the proof.

In order to transform the mobile state into steady state, we provide a simple method enlightened by the integral average of a definite integral to get the overall SOP performance. Combine with the handover scheme which has illustrated in the above section, we can get the expression of the SOP below.

$$P_{so} = \frac{\iint_{\sum_i l_i} (\frac{\lambda_1}{\lambda_1 + \lambda\beta_E})^{\alpha_1} \frac{1}{e^{\lambda\beta_E}} dd_{AE} dd_{Ek}}{\iint_{\sum_i l_i} dd_{AE} dd_{Ek}} \tag{4}$$

where $k \in \kappa$ and d_{Ek} denotes the distance between the Eve and the Jammer k. l_i denotes i_{st} legally moves in the fixed domain. When the **SINR constraint** is satisfied, Eve is closer enough to Alice or too far to the current Jammer. In this case, the system should switch to the closest Jammer to ensure physical layer security. Thus, $k \in \kappa$ is a variable parameter that makes the integral path change with the system condition.

Proof: We consider the moving path of Eve as the integral path, the changeable d_{AE} and d_{Ek} as the integral variables. With the help of curvilinear integral, we get the sum SOP performance through calculating the integral along the moving path. Different from the SPDF method, the above curvilinear integral is a simple sum of the SOP. Enlightened by the integral average method, we calculate the overall performance by solving the integral average of the double curvilinear integral. We consider the static SOP as the integrand and get the expression of the overall SOP. Due to the complex double curvilinear integral and changeable k correlated to the handover condition, it is difficult to get the closed-form expression.

4.2. Numerical Results

Fig. 3 shows the numerical results of SOP and compares the performance difference of the RWP model and the CEM model. From the figure, it is shown that the SOP decreases with the SINR threshold of Eve increases. That means the secrecy performance improves while the rate of redundant information increases. We find that with the handover threshold decreases, the system obtains better secrecy performance. We also find that the CEM model has advantages over the typical RWP model. The advantages increase while handover times decrease. That explains that our handover scheme can efficiently confront the conscious eavesdropper.

For a CEM Eve, Fig. 4 shows the value of SOP versus the handover threshold β. From the curve we can analyze the eavesdropping condition of a mobile Eve. It can be shown that the SOP performance is degraded as β increases. Because the handover is no longer sensitive with Eve's SINR increases. However, influenced by the distribution of the jammers, decrease the value of β can't always improve the secrecy. The left flat part in the figure shows the β range of secrecy lower bound. Similarly, when β increases to a certain extent where Eve's SINR can't achieve, the value of SOP stops increasing. That means the handover event never happens and the system degrades to a typical model with one cooperative jammer. Besides, the value of SOP increases dramatically in two ranges which have been circled in the figure. According to the definition of β, we infer that Eve's SINRs are mainly distributed in these two ranges.

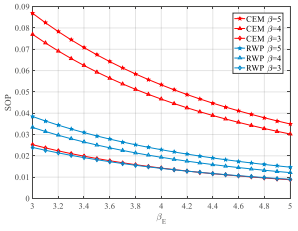

Fig. 3. SOP for RWP and CEM Eve.

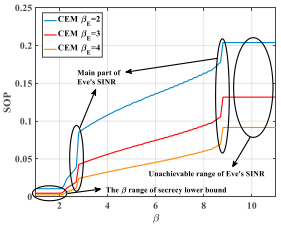

Fig. 4. SOP with different CEM Eves.

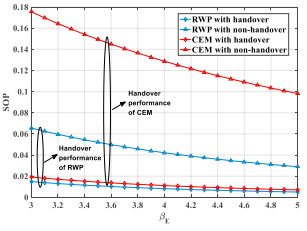

Fig. 5. SOP comparison of handover and non-handover.

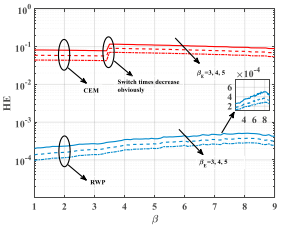

Fig. 6. HE comparison of CEM and RWP Eve.

Fig. 5 studies the handover performance from comparing the value of SOP with handover scheme and typical non-handover scheme. We find the proposed handover scheme improves the secrecy performance of the system that leads to a lower SOP value. A CEM Eve can plan the path of his movement, and that will lead a very large SOP. The figure also shows that the handover performance of a CEM Eve is obviously larger than a RWP Eve, which proves that the scheme can be effectively against the conscious eavesdropper.

Fig. 6 compares the HE of a CEM Eve and a RWP Eve. We find that the proposed handover scheme can more efficiently confront a conscious eavesdropper than a random mobile eavesdropper. With β increases, the HE approximately first increases and then decreases in a proper range. Because, with β decreases, the secrecy performance improves rapidly while the network suffers overreacted problem and switches over frequently. However, if we set a large β, the mobile Eve won't fully switch with the $SINR_E$ increases. Both of those result in a decrease in the value of HE. For a CEM Eve, when β is set in a proper range, the HE increase dramatically, which has been circled in the figure. The main reason is the handover times decrease obviously in that range. Besides, a higher β_E leads to a lower HE, which indicates the design of the redundant rate R_e.

5. Conclusion

This work investigated secure downlink transmmission in an IoT system with a mobile eavesdropper, and proposed a handover scheme to enhance PLS with the help of multiple cooperative jammers. In order to reflect the real situation, the conscious eavesdropping model was proposed to compare with the typical RWP model. Moreover, we introduced a metric called handover efficiency to reflect the handover performance. The numerical results verified that the handover scheme could efficiently improve the secrecy performance and effectively confront the conscious eavesdropper. The proposed scheme is feasible to provide security enhancement in many real mobile eavesdropping scenarios.

Acknowledgements

This work was supported in part by the National Science Foundation of China, under Grant 61871023 and Grant 61931001 and in part by Beijing Natural Science Foundation, under Grant 4202054.

References

[1] Zhipeng Cai and Xu Zheng. A private and efficient mechanism for data uploading in smart cyber-physical systems. *IEEE Transactions on Network Science and Engineering*, 7(2):766–775, 2020.

[2] Zhipeng Cai and Zaobo He. Trading private range counting over big iot data. In *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, pages 144–153, 2019.

[3] Yan Huo, Chun Meng, Ruinian Li, and Tao Jing. An overview of privacy preserving schemes for industrial Internet of Things. *China Communications*, 17(10):1–18, 2020.

[4] Zhipeng Cai, Xu Zheng, and Jiguo Yu. A differential-private framework for urban traffic flows estimation via taxi companies. *IEEE Transactions on Industrial Informatics*, 15(12):6492–6499, 2019.

[5] Zhipeng Cai, Zaobo He, Xin Guan, and Yingshu Li. Collective data-sanitization for preventing sensitive information inference attacks in social networks. *IEEE Transactions on Dependable and Secure Computing*, 15(4):577–590, 2018.

[6] Lin Hu, Hong Wen, Bin Wu, Fei Pan, Run-Fa Liao, Huanhuan Song, Jie Tang, and Xiumin Wang. Cooperative jamming for physical layer security enhancement in Internet of Things. *IEEE Internet of Things Journal*, 5(1):219–228, 2018.

[7] Yan Huo, Yuandong Wu, Ruinian Li, Qinghe Gao, and Xiling Luo. A learning-aided intermittent cooperative jamming scheme for non-slotted wireless transmission in an IoT system. *IEEE Internet of Things Journal*, pages 1–1, 2021.

[8] Yan Huo, Jingjing Fan, Yingkun Wen, and Ruinian Li. A cross-layer cooperative jamming scheme for social Internet of Things. *Tsinghua Science and Technology*, 26(4):523–535, 2021.

[9] Yan Huo, Yuqi Tian, Liran Ma, Xiuzhen Cheng, and Tao Jing. Jamming strategies for physical layer security. *IEEE Wireless Communications*, 25(1):148–153, 2018.

[10] Yan Huo, Xin Fan, Liran Ma, Xiuzhen Cheng, Zhi Tian, and Dechang Chen. Secure communications in tiered 5G wireless networks with cooperative jamming. *IEEE Transactions on Wireless Communications*, 18(6):3265–3280, 2019.

[11] Ran Zi, Jia Liu, Liang Gu, and Xiaohu Ge. Enabling security and high energy efficiency in the internet of things with massive MIMO hybrid precoding. *IEEE Internet of Things Journal*, 6(5):8615–8625, 2019.

[12] Jianwei Hu, Nan Yang, and Yueming Cai. Secure downlink transmission in the internet of things: How many antennas are needed? *IEEE Journal on Selected Areas in Communications*, 36(7):1622–1634, 2018.

[13] Qinghe Gao, Yan Huo, Tao Jing, Liran Ma, Yingkun Wen, and Xiaoshuang Xing. An intermittent cooperative jamming strategy for securing energy-constrained networks. *IEEE Transactions on Communications*, 67(11):7715–7726, 2019.

[14] Zaobo He, Zhipeng Cai, Jiguo Yu, Xiaoming Wang, Yunchuan Sun, and Yingshu Li. Cost-efficient strategies for restraining rumor spreading in mobile social networks. *IEEE Transactions on Vehicular Technology*, 66(3):2789–2800, 2017.

[15] Yingkun Wen, Yan Huo, Liran Ma, Tao Jing, and Qinghe Gao. A scheme for trustworthy friendly jammer selection in cooperative cognitive radio networks. *IEEE Transactions on Vehicular Technology*, 68(4):3500–3512, 2019.

[16] Jie Tang, Monireh Dabaghchian, Kai Zeng, and Hong Wen. Impact of mobility on physical layer security over wireless fading channels. *IEEE Transactions on Wireless Communications*, 17(12):7849–7864, 2018.

[17] Jie Tang, Hong Wen, Huanhuan Song, Tengyue Zhang, and Kaiyu Qin. On the securityreliability and secrecy throughput of random mobile user in Internet of Things. *IEEE Internet of Things Journal*, 7(10):10635–10649, 2020.

[18] Ning Cao, Yunfei Chen, and Zhutian Yang. Secrecy outage probability with randomly moving interferers in Nakagamim fading. *IEEE Communications Letters*, 23(1):76–79, 2019.

[19] Sarankumar Balakrishnan, Pu Wang, Arup Bhuyan, and Zhi Sun. Impact analysis of mobility on physical layer security of mmWave networks. In *2019 Resilience Week (RWS)*, volume 1, pages 163–168, 2019.