This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841033, IEEE Transactions on Industrial Informatics

Jamming and Eavesdropping Defense in Green Cyber-Physical Transportation Systems using Stackelberg Game

Kun Wang, *Senior Member, IEEE,* Li Yuan, Toshiaki Miyazaki, *Senior Member, IEEE,* Yuanfang Chen, *Member, IEEE,* and Yan Zhang, *Senior Member, IEEE,*

***Abstract*—This paper studies the secure transmission rate issue between sensors and the remote controller to defend the jamming and eavesdropping attacks in Green Cyber-Physical Transportation Systems (GCPTS). In this system, the traffic sensor transmits the transportation state information to the remote controller via wireless networks. Due to the broadcast characteristics of wireless communication, the systems are vulnerable to the eavesdropping and jamming attacks. In this paper, we study how to maximize the secure transmission rate between sensors and the controller with the presence of malicious eavesdropper and jammer. Specifically, the malicious jammer is smart and can choose the optimal power strategy to maximize the side effect with the knowledge of sensor's transmission power. For the purpose of achieving the maximum utility, the optimal strategy is determined via adjusting the sensor's transmission power according to the control feedback conditions. We consider the single-antenna model and the multi-antenna model to formulate this problem as an optimization problem based on the Stackelberg game. We then prove the existence of Stackelberg equilibrium via the interaction between the sensor and the jammer. Moreover, we present two algorithms to obtain the optimal transmission strategy, i.e., stochastic algorithm with feedback (SAF) and renewed intelligent simulated annealing (RISA). Finally, extensive simulations and trace experimental results are presented to verify our theoretical analysis.**

***Index Terms*—Eavesdropping, Control feedback, Green Cyber-Physical Transportation System, Stackelberg Game, Smart jammer.**

I. Introduction

CYBER-physical systems (CPS) combine the capabilities of sensing, control, communication and computing together, and are widely employed in various applications such as aviation, national defense, armamentarium, and industrial automation. In CPS, sensors receive the control commands from the remote controller and respond with the sensing information through an open and wireless communication media. Considering the wireless property of CPS, information communication between sensors and the controller is under the threat of eavesdropping and jamming attacks.

Merge with the previous paragraph. For example, the future intelligent transportation [1] denoted as a cyber-physical transportation system is widely used to manage the transportation situation for vehicles, trains and aeroplanes. In this system, the transportation condition information is mainly transmitted in the public network with open network architecture. It is obvious that the transmission process is vulnerable to security risks, such as stealing, falsifying and interfering the transportation state information.

Any malicious attacks on the transmission process may result in wrong judgement and impact on the transportation condition or even the traffic accident. Therefore, the secure information transmission is an important issue in CPTS [2-5].

Eavesdropping is a popular attack in wireless networks. A plenty of encryption-based approaches are proposed [6]. Without the correct keys shared among the sensors and controller, the malicious eavesdropper doesn't know what is transmitted between sensors and controller even if it has obtained the encrypted data packets. However, the employment of encryption needs much computing power, which is seriously limited due to the small size of the sensors' batteries. Moreover, we have to allocate much computing power of sensors to the operations of analyzing the transportation state information. Therefore, the power-consuming encryption-based approach is not a proper countermeasure to the eavesdropping attacks in CPTS. The physical layer security techniques that do not require any computing power have attracted much attention from both academia and industry. In [7-10], the concept of friendly jammer was proposed to prevent the eavesdropping attacks from intentionally injecting noise in CPTS. In recent years, almost all previous literatures assumed that the jammer is friendly, i.e., the users have the full right to control it. However, in reality, the jammer is not always friendly and may act as a malicious role to transmit noise to disturb the normal information transmission. Since the malicious jammer can substitute the friendly jammer and reduce the power consumption of the whole CPTS, this system may achieve green and we call it Green Cyber-Physical Transportation Systems (GCPTS) [11-13].

In this paper, we study the eavesdropping defense with the

K. Wang is with Jiangsu Engineering Research Center of Communication and Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China, and also with the School of Computer Science and Engineering, The University of Aizu, Aizu-Wakamatsu City 965-8580, Japan (e-mail: kwang@njupt.edu.cn).

L. Yuan is with the National Engineering Research Center of Communications and Networking, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: xzsnyli@gmail.com).

T. Miyazaki is with the School of Computer Science and Engineering, The University of Aizu, Aizu-Wakamatsu City 965-8580, Japan (e-mail: miyazaki@u-aizu.ac.jp).

Y. Chen is with the School of Cyberspace, Hangzhou Dianzi University, Hangzhou, 310018, China (e-mails: yuanfang chen@ieee.org).

Y. Zhang is with University of Oslo, Oslo 0315, Norway. He is also with Simula Research Laboratory, Lysker 1325, Norway. (e-mail: yanzhang@ieee.org).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841033, IEEE Transactions on Industrial Informatics

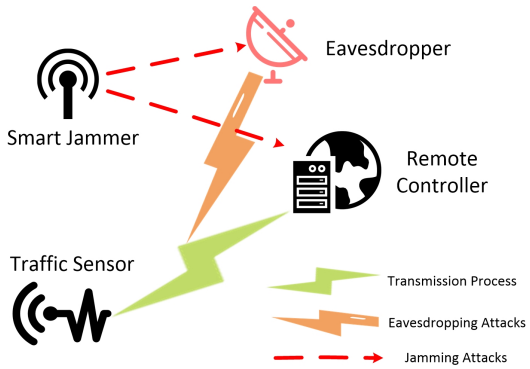


Fig. 1: Eavesdropping defense with smart jammer

jamming attacks shown in Fig. 1. The modeled system consists of four components: traffic sensors, remote controller, malicious jammer and malicious eavesdropper. Since the jammer injects noise in GCPTS via a broadcast manner, it can not only interfere with the transmission between sensors and the controller but also prevent from the eavesdropping attacks to some extent. This paper investigates how to maximize the secure transmission rate with the presence of malicious jammer and how to make the interference of jammer to eavesdropper reach a specific level. With the malicious jammer, source power can be reduced while achieving the same secrecy capacity. In addition, we do not need the power of friendly jammer which exists in previous methods. We have established two types of communication processes: (1) *single-antenna sensor*, where the information is transmitted in one channel; (2) *multi-antenna sensor*, where the information is divided into multiple packets to be transmitted at multiple channels.

We model the power allocation problem as a Stackelberg game [14], in which the sensor is the leader and the jammer is the follower. Both of them intend to maximize their own utilities. We apply this game to a novel CPTS model. This paper takes the eavesdroppers into consideration and studies how to maximize the secure transmission rate between sensors and the controller with the presence of malicious eavesdropper and jammer. In our approach, the jammers are used to defend against the malicious eavesdroppers.

There are three contributions in this paper.

- We consider the transmission security of transportation state information in GCPTS, and the corresponding process is different from traditional wireless transmission with assistance of feedback. By the control feedback, the traffic sensors do not need to allot any computing power to solve the power allocation problem. Moreover, in traditional wireless communications, the sender does not consider the state of the receiver when determining the transmission strategy. It may cause non-optimal strategy choice. On the contrary, the sensors in GCPTS are able to dynamically adjust the communication strategy to achieve the optimization according to the feedback signal from the remote controller. To the best of our knowledge, this is the first piece of work that uses the control feedback to enhance the security of the transmission process in GCPTS.
- Most previous works proposed to use the friendly jammer to improve the security of a transmission process. This is effective but not practical because the jammer is not always friendly and more likely to be a malicious jammer that tries to maximize the side effect to GCPTS. In the GCPTS with both eavesdropping and jamming attacks, the objectives of these two attackers are different. Specifically, the eavesdropping attacker intends to wiretap the transmission content between sensors and the controller, whereas, the jammer intends to corrupt the transmission between sensors and controller. Due to the coexistence of jamming and eavesdropping attackers, the eavesdropping defense with smart jammer (EDSJ) problem is more challenging.
- We explore the relationship between the sensor and the jammer. The sensor is aware of the jammer's intelligence and the corresponding best response of the jammer in GCPTS. Based on this knowledge, the sensor tries to obtain an optimal power allocation strategy in order to achieve the maximum value of its own utility. The power allocation problem can be seen as an optimization problem, and the Stackelberg game is applied to model this problem. In our model, the sensor is a leader while the jammer is a follower. Both of them intend to maximize their utilities and the leader has the priority. For the purpose of achieving the Stackelberg Equilibrium strategies, a stochastic algorithm [15] with feedback (SAF) and a Renewed Intelligent Simulated Annealing (RISA) algorithm are proposed.

The reminder of this paper is organized as follows. In Section II, we propose two feasible communication models of our system. In section III, the EDSJ with the single-antenna sensor is discussed. In Section IV, the EDSJ with the multi-antenna sensor is investigated. Performance evaluation is given in Section V. The related work is briefly described in Section VI and we summarize this paper in Section VII.

II. System Model and Assumptions

In this section, we consider the transmission process of transportation state information with feedback in GCPTS. We are interested in the security of this transmission process in the presence of jamming attack and eavesdropping attack, so we model two communication systems to study this problem.

A. Communication System Model

In the information transmission process of GCPTS, the sensor sends the transportation state information to corresponding remote controller as described in Fig. 2. The system faces threats of eavesdropping attacks and jamming attacks. With the help of control feedback, the sensor can adjusts its condition according to the received feedback from this controller in order to maximize its secrecy capacity. In addition, we utilize the jamming attacks to defend the eavesdropping attacks. Without loss of generality, we assume that the time delay of this feedback can be ignored. We propose the communication model consisting of a transmission channel (i.e., a sensor-controller pair), a jammer, and an

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841033, IEEE Transactions on Industrial Informatics

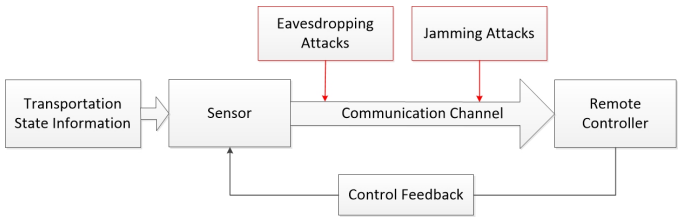


Fig. 2: Information transmission process of GCPTS

eavesdropper. The sensor can set its own transmission power. The channel capacity of senor-controller channel and sensor-eavesdropper channel are shown as follows:

$$C_{SC} = aW\log\left(1+\frac{v_{sc}P}{N+v_{jc}J}\right), \tag{1}$$

$$C_{SE} = aW\log\left(1+\frac{v_{se}P}{N+v_{je}J}\right), \tag{2}$$

where P is the sensor's power and J is the jammer's power. v_{sc}, v_{jc}, v_{se} and v_{je} are the channel gains of sensor-controller channel, jammer-controller channel, sensor-eavesdropper channel, and jammer-eavesdropper channel, respectively. In addition, W and a indicate the bandwidth and the gain coefficient on the channel. N is the channel thermal noise.

From Eqs. (1) and (2), the secrecy capacity of this system is given by:

$$C = (C_{SC} - C_{SE})^{+}, \tag{3}$$

where $(\cdot)+ = \max(\cdot,0)$. According to Eq. (3), the secure transmission rate of transportation state information is related to the power of sensor. Since the sensor can adjust its condition with the received feedback from the controller, we assume the feedback includes the changing flag of security capacity denoted as θ and the power of sensor adjusts its transmission power based on this changing flag. Therefore, we consider a general discrete-time linear power changing process:

$$P^{k+1} = \mathcal{F}(P^k,\theta_k), \tag{4}$$

where k is a positive integer index defined as the system time, P^k is the sensor transmission power vector at time k and θ_k is the feedback information from the controller at time k. Note that the sensor adjusts its transmission power with the received θ_k, P^{k+1} is a function denoted as $\mathcal{F}(\cdot)$ and related to P^k and θ_k. As time goes, the secrecy capacity of this system is becoming larger and larger and eventually achieves the maximum value. This changing process can be modeled as a stochastic algorithm [15] with feedback (SAF). SAF is an iterative optimization approaches and used in real-time estimation and control problems. In such situation of the description above, we consider two communication systems: single-antenna sensor model and multi-antenna sensor model.

Single-antenna model: we use α and β to represent the per unit power of sensor and jammer. As shown in [16] we employ the channel capacity as the profit of transmission nodes. The jammer's utility function is calculated as follows:

$$J_s(P,J) = -C_{SC} - \beta J, \tag{5}$$

and the sensor's utility function is calculated as follows:

$$U_s(P,J) = C_{SC} - C_{SE} - \alpha P, \tag{6}$$

where $P \le P_{max}$ and $J \le J_{max}$ are the system inherent constraints.

In this system, we consider the transmission cost of nodes. Hence, the sensor needs to pay a price to the providers of power. The secrecy capacity is the difference between C and the cost of the source. In addition, the malicious jammer's target is to disturb the transmission of the sensor and the cost of jammer is also considered, so that the utility function of malicious jammer can be expressed as the difference between the negative of the sensor's channel capacity and the cost of jammer.

Multi-antenna model: Assuming the sensor and the jammer have multiple antennas. The sensor divides the transportation state information into multiple packets to be sent at different antennas. v_{sc}^i is the channel gain between the sensor and the controller at antenna i, and v_{se}^i is the channel gain between the sensor and the eavesdropper at antenna i. Similarly, v_{jc}^i is the channel gain between the jammer and the controller at antenna i, and v_{je}^i is the channel gain between the jammer and the eavesdropper at antenna i. Transmission power constraints of the sensor and the jammer are denoted as $P_{max} > 0$ and $J_{max} > 0$, respectively. P_i is the transmission power at antenna i and $\mathbf{P} = (P_1,P_2,...,P_n)$ denotes the transmission power vector of the sensor. Similarly, J_i is the transmission power at antenna i and $\mathbf{J} = (J_1,J_2,...,J_n)$ denotes the power vector of the jammer transmitted. $\mathcal{P} = \{(P_1,P_2,...,P_n) \mid P_i \ge 0, \sum_{i=1}^n P_i \le P_{max}\}$ is a feasible set of $\mathbf{P}$ and $\mathcal{J} = \{(J_1,J_2,...,J_n) \mid J_i \ge 0, \sum_{i=1}^n J_i \le J_{max}\}$ is a feasible set of $\mathbf{J}$. N_i is the variance of thermal noise for channel i. Same as the single-antenna model, α and β denote the cost of per unit transmission power by the sensor and the jammer, respectively. The jammer's utility function is calculated as follows:

$$J_m(\mathbf{P},\mathbf{J}) = -\sum_{i=1}^{n} aW\log\left(1+\frac{v_{sc}^i P_i}{N_i + v_{jc}^i J_i}\right) - \sum_{i=1}^{n}\beta J_i, \tag{7}$$

and the sensor's utility function is calculated as follows:

$$\begin{aligned} U_m(\mathbf{P},\mathbf{J}) =& \sum_{i=1}^{n} aW\log\left(1+\frac{v_{sc}^i P_i}{N_i + v_{jc}^i J_i}\right) \\ &- \sum_{i=1}^{n} aW\log\left(1+\frac{v_{se}^i P_i}{N_i + v_{je}^i J_i}\right) - \sum_{i=1}^{n}\alpha P_i. \end{aligned} \tag{8}$$

Similar to single-antenna model, the sensor needs to pay a price to the providers of power. Considering the sensor and the jammer have multiple antennas, the secrecy capacity of this model is the sum of differences between each antenna's conventional secrecy capacity and the cost of each antenna. The utility function of the malicious jammer is the sum of the differences between negative of each antenna's secrecy capacity and the cost of each antenna.

In this paper, the jammer is smart and can choose the optimal transmission strategy with the knowledge of sensor's transmission power to maximize utility. It is applied to strengthen the system security against the eavesdropper. We study how to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841033, IEEE Transactions on Industrial Informatics

allocate the power of the sensor transmitted for achieving the maximum utility and make the problem called eavesdropping defense problem with smart jammer.

B. Oligopoly Market and Stackelberg Game

This power allocation problem can be modeled as an oligopoly market. Oligopoly market is a definition in economics, consisting of a few sellers (i.e., oligopolists) who can manage the production and sales of a special market which is defined as transmission power P, J and utility function $U(P,J)$ in this paper. In our system, the sensor and the jammer can be seen as sellers who try to sell their power P and J at a certain price. Since the smart jammer chooses the optimal transmission power strategy J on the basis of the sensor' transmission power P, the sensor is active while the jammer is passive. Therefore, Stackelberg game is proposed as an appropriate tool. In Stackelberg game, the leader chooses its strategy P first and the follower chooses an optimal responding strategy J according to the leader's selection. Because the leader and the follower understand the reaction to each other, both of them intend to maximize their profit and the leader has the priority. By analyzing the interaction of the leader and the follower, we can obtain a Stackelberg Equilibrium (SE) denoted as $\left(P^{SE},J^{SE}\right)$ with the optimal strategies of the leader and the follower achieved.

III. Analysis of EDSJ under Single-Antenna Model

In this section, the EDSJ with the single antenna is discussed. First, we analyze the jammer's utility function and obtain the optimal relevant strategy with the given strategy of the sensor. Then, we obtain the optimal strategy of the sensor on the basis of the jammer's optimal responding strategy. In the end, we propose the SAF algorithm to achieve the optimal strategy of the sensor.

A. Analysis of Jammer (Follower)

Definition 1: Given the utility function of the jammer, we can obtain the optimal power of jammer transmitted figuring out the following optimization problem:

$$\max_{J\geq 0} J_s(P,J) = -aW\log\left(1+\frac{v_{sc}P}{N+v_{jc}J}\right) - \beta J, \quad (9)$$

where P denotes the given power strategy of the sensor transmitted and is assumed as a constant in this situation. v_{sc} is the channel gain between the sensor and the controller, and v_{se} is the channel gain between the sensor and the eavesdropper. Similarly, v_{jc} is the channel gain between the jammer and the controller, and v_{je} is the channel gain between the jammer and the eavesdropper.

For the purpose of achieving the maximum value of the jammer's utility, Eq. (9) is differentiated with respect to J as follows:

$$\frac{\partial J_s(P,J)}{\partial J} = -aW\left(\frac{v_{jc}/\ln 2}{N+v_{jc}J+v_{sc}P} - \frac{v_{jc}/\ln 2}{N+v_{jc}J}\right) - \beta. \quad (10)$$

By setting the Eq. (10) as 0, closed-form solution can be achieved as:

$$J(P) = \begin{cases} 0, & P \leq T, \\ \dfrac{-(2N+v_{sc}P)+\sqrt{v_{sc}^2P^2+KP}}{2v_{jc}}, & P > T, \end{cases} \quad (11)$$

where

$$K = \frac{4aWv_{sc}v_{jc}}{\ln 2\beta}, \ T = \frac{4N^2}{K-4Nv_{sc}}. \quad (12)$$

It is obvious that $J(P)$ is a continuous function in P. In next subsection, we substitute $J(P)$ into $U_s(P,J)$.

B. Analysis of Sensor (Leader)

Definition 2: The sensor knows the jammer's optimal responding strategy, and tries to achieve the maximum value of its own utility. We can formulate the corresponding optimization problem as:

$$\begin{aligned}\max_{P\geq 0} U_s(P,J(P)) =& aW\log\left(1+\frac{v_{sc}P}{N+v_{jc}J(P)}\right) \\ &- aW\log\left(1+\frac{v_{se}P}{N+v_{je}J(P)}\right) - \alpha P,\end{aligned} \quad (13)$$

where $J(P)$ is given in Eq. (11).

By substituting Eq. (11) into the utility function of the sensor, we have:

$$\begin{aligned} &U_s(P,J(P)) \\ &= \begin{cases} aW\log\left(1+\frac{v_{sc}P}{N}\right) - aW\log\left(1+\frac{v_{se}P}{N}\right) - \alpha P, & P \leq T, \\ aW\log\left(1+\frac{2}{\sqrt{1+\frac{KP}{(v_{sc})^2P^2}}}\right) - \alpha P & \\ -aW\log\left(\frac{2v_{jc}v_{se}P}{2(v_{jc}-v_{je})N-v_{je}v_{sc}P+v_{je}\sqrt{(v_{sc})^2P^2+KP}}\right), & P > T. \end{cases} \end{aligned} \quad (14)$$

Lemma 1: $U_s(P,J(P))$ is a continuous function of P.

Proof: From Eq. (8), We can achieve that U_s is a continuous function of variables (P,J). By Eq. (11), it is observe that $J(P)$ is monotonic increase by P. Therefore, we can achieve that $U_s(P,J(P))$ shows succession in P. ■

Theorem 1: This is a Stackelberg equilibrium (P^{SE},J^{SE}) in the EDSJ and it is the solution to this optimization problem.

Proof: From **Lemma 1**, we prove the continuity of $U_s(P,J(P))$ in P. As P is continuous, $U_s(P,J(P))$ maximizes its value with a number of point $P^E \in P$. ■

To solve this optimization problem, a stochastic algorithm is applied to achieve the best strategy of the sensor. We model the transmission process of transportation state information as a stochastic algorithm with feedback (SAF). The stochastic algorithm is a type of iterative optimization method. In Algorithm 1, SAF generates random variables and converges to an optimal value. The input parameter M is the stable number of the same optimal values. i is the system time and θ_i is the feedback flag at time i. The algorithm will achieve the maximum value of $U_s(P,J)$ and obtain the Stackelberg equilibrium in the end. With

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841033, IEEE Transactions on Industrial Informatics

Algorithm 1: SAF

Input: M
Output: P_{best}, J_{best}
Randomly initialize $P[1]$, $P_{best}[1] \longleftarrow P[1]$, $i=0$, $j=0$;
while $true$ **do**
  $i=i+1$;
  $\theta_i=0$;
  $P[i+1]=P_{best}[i]+(rand()-0.5)$;
  if $U_s(P[i+1],J(P[i+1]))>U_s(P_{best}[i+1],J(P_{best}[i+1]))$ **then**
    $\theta_i=1$;
  end
  if $\theta_i=1$ **then**
    $P_{best}[i+1]=P[i+1]$;
  end
  else
    $P_{best}[i+1]=P_{best}[i]$;
    $j=j+1$;
  end
  if $j>M$ **then**
    Break;
  end
end
$P_{best}=P_{best}[i]$;
$J_{best}=J(P_{best})$;

Stackelberg equilibrium obtained, we can achieve the optimal power of the sensor and the jammer. Then, we can figure out the optimal profit of the sensor denoted as U_s, which is the maximum difference between secrecy capacity and the cost of the sensor.

SAF generates random variables and converges to an optimal value. With a random initial power given, we make the power change randomly.When the feedback is better than the last value, we set this value as a parameter called P_{best}. When the feedback is worse than the last value, make the power change to an opposite direction. When the feedback is always worse than P_{best}, we obtain the Stackelberg equilibrium in the end.

IV. Analysis of EDSJ under Multi-Antenna Model

A. Analysis of Jammer (Follower)

Definition 3: With the power allocation strategy of the sensor given as $\mathbf{P}\in\mathcal{P}$, we can figure out the following optimization problem to achieve the maximum utility of the jammer:

$$\max_{\mathbf{J}\in\mathcal{J}} J_m(\mathbf{P},\mathbf{J})=-\sum_{i=1}^{n} aW\log\left(1+\frac{v_{sc}^i P_i}{N_i+v_{jc}^i J_i}\right)-\sum_{i=1}^{n}\beta J_i \tag{15}$$

s.t.

$$\sum_{i=1}^{n} J_i\le J_{max}, J_i\ge 0, i\in[1,n],$$

For the purpose of achieving the maximum value of the jammer, we differentiate Eq. (15) with respect to J_i for $i\in[1,n]$ as:

$$\frac{\partial J_m(\mathbf{P},\mathbf{J})}{\partial J_i}=-aW\left(\frac{v_{jc}^i/\ln 2}{N_i+v_{jc}^i J_i+v_{sc}^i P_i}-\frac{v_{jc}^i/\ln 2}{N_i+v_{jc}^i J_i}\right)-\beta. \tag{16}$$

Rearranging Eq. (16) and setting it to 0, we can obtain the solution as:

$$J_i^*(\mathbf{P})=\begin{cases}0, & P_i<\frac{N_i^2}{K_i-N_i v_{sc}^i},\\ \frac{-(2N_i+v_{sc}^i P_i)+\sqrt{(v_{sc}^i P_i)^2+4K_i P_i}}{2v_{jc}^i}, & P_i\ge\frac{N_i^2}{K_i-N_i v_{sc}^i},\end{cases} \tag{17}$$

where

$$K_i=\frac{aW v_{sc}^i v_{jc}^i}{\ln 2\beta}.$$

We can obtain that $J_i^*(\mathbf{P})$ in Eq. (17) is the best strategy of the jammer antenna i with given $\mathbf{P}$. However, we may notice the limited conditions of J_{max} in this situation. In other words, the optimal strategy $J_i(\mathbf{P})$ of the jammer should satisfy the equation that $\sum_{i=1}^{n} J_i^*(\mathbf{P})\le J_{max}$.

Then, we consider the other situation $\sum_{i=1}^{n} J_i^*(\mathbf{P})>J_{max}$ where the value of $\partial J_m(\mathbf{P},\mathbf{J})/\partial J_i$ is not equal to zero and all antennas of the jammer have their own tendencies. Therefore, we should make them have same tendencies π in order to obtain a relatively steady state. With setting the Eq. (16) equal to π, it can be expressed as follows:

$$-aW\left(\frac{v_{jc}^i/\ln 2}{N_i+v_{jc}^i J_i+v_{sc}^i P_i}-\frac{v_{jc}^i/\ln 2}{N_i+v_{jc}^i J_i}\right)-\beta=\pi. \tag{18}$$

By figuring out the equation above, we can obtain

$$J_i^{**}(\mathbf{P})=\frac{-(2N_i+v_{sc}^i P_i)+\sqrt{(v_{sc}^i P_i)^2+4K_i' P_i}}{2v_{jc}^i}, \tag{19}$$

where

$$K_i'=\frac{4aW v_{sc}^i v_{jc}^i}{\ln 2(\beta+\pi)}\ and\ P_i\ge\frac{N_i^2}{K_i-N_i v_{sc}^i}.$$

By substituting Eq. (19) into constraint conditions, we have

$$\sum_{i=1}^{n}\frac{-(2N_i+v_{sc}^i P_i)+\sqrt{(v_{sc}^i P_i)^2+4K_i' P_i}}{2v_{jc}^i}=J_{max}. \tag{20}$$

First, let omit the constraints, so there are $\sum_{i=1}^{n} J_i>J_{max}$. For the purpose of satisfying constraints, each J_i decreases and π increases correspondingly. When the J_i is reduced to $\sum_{i=1}^{n} J_i<J_{max}$, each of J_i will have an incentive to increase with positive π. Therefore, the $sum_{i=1}^{n} J_i$ is always equal to J_{max} in this situation. From above, the coefficient π should meet Eq. (20). The approximate solution process is given **as Algorithm 1**.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841033, IEEE Transactions on Industrial Informatics

Algorithm 2: approximate solution process process of $\mathbf{J}(\mathbf{P})$

Input: $\mathbf{P}$
Output: $\mathbf{J}(\mathbf{P})$
if $P_i < \frac{N_i^2}{K_i - N_i v_{sc}^i}$ **then**
  return *0*;
end
if $\sum_{i=1}^{n} J_i^*(\boldsymbol{P}) < J_{max}$ **then**
  $J_i(\mathbf{P}) = J_i^*(\mathbf{P})$;
  return $\boldsymbol{J(P)}$;
end
else
  $\pi = 0$;
  while $\sum_{i=1}^{n} J_i^{**}(\boldsymbol{P}) > J_{max}$ **do**
    $\pi = \pi + rand() * 0.01$
  end
  $J_i(\mathbf{P}) = J_i^{**}(\mathbf{P})$;
  return $\boldsymbol{J(P)}$;
end

B. Analysis of Sensor (Leader)

Definition 4: The optimal responding strategy of the jammer is obtained in the subsection above and the sensor knows it. Hence, the utility optimization problem of the sensor is shown as:

$$\begin{aligned}\max_{\mathbf{P}\in\mathcal{P}} U_m(\mathbf{P},\mathbf{J}(\mathbf{P})) =& \sum_{i=1}^{n} aW\log\left(1+\frac{v_{sc}^i P_i}{N_i + v_{jc}^i J_i(\mathbf{P})}\right) \\ &-\sum_{i=1}^{n} aW\log\left(1+\frac{v_{se}^i P_i}{N_i + v_{je}^i J_i(\mathbf{P})}\right) - \sum_{i=1}^{n}\alpha P_i,\end{aligned} \tag{21}$$

s.t.

$$\sum_{i=1}^{n} P_i \le P_{max}, P_i \ge 0, i \in [1,n],$$

Lemma 2: When $\{\mathbf{P}[k]\}$ converges to $\mathbf{P^*}$ ($\mathbf{P^*} \in \mathcal{P}$), we denote $\mathbf{J(P^*)}$ as the jammer's optimal strategy.

Proof: The given set $\{\mathbf{P}[k]\}$ converges to the $\mathbf{P^*}$ ($\mathbf{P^*} \in \mathcal{P}$). We assume there is a subset $\mathbf{J}(\mathbf{P}^k)$ converging to a $\mathbf{J'} \neq \mathbf{J}(\mathbf{P^*})$. Therefore, the $\{\mathbf{P}[k],\mathbf{J}(\mathbf{P}[k])\}$ converges to $\{\mathbf{P^*},\mathbf{J'}\}$.

From the analysis of $\mathbf{J(P)}$ in Section V-A, we know that $\mathbf{J}$'s optimal strategy is $\mathbf{J}(\mathbf{P^*})$. Hence, we can obtain

$$U_m(\mathbf{P^*},\mathbf{J}(\mathbf{P^*})) - U_m(\mathbf{P^*},\mathbf{J'})) \ge 0. \tag{22}$$

Then, we define

$$U_m(\mathbf{P^*},\mathbf{J}(\mathbf{P^*})) - U_m(\mathbf{P^*},\mathbf{J'})) \doteq 3\gamma, \tag{23}$$

where γ is any positive number greater than zero. With $\{\mathbf{P[k]}\}$ converging to $\mathbf{P^*}$ and $\mathbf{J(P[k])}$ converging to $\mathbf{J'}$, we have

$$|U_m(\mathbf{P^*},\mathbf{J'}) - U_m(\mathbf{P}[k],\mathbf{J}(\mathbf{P}[k]))| \le \gamma, \; when \; k \ge K, \text{ and} \tag{24}$$

$$|U_m(\mathbf{P^*},\mathbf{J}(\mathbf{P^*})) - U_m(\mathbf{P}[k],\mathbf{J}(\mathbf{P^*}))| \le \gamma, \; when \; k \ge K, \tag{25}$$

where K is an integer that is positive and large enough. Hence, when $k \ge K$, we have

$$\begin{aligned} U_m(\mathbf{P}[k],\mathbf{J}(\mathbf{P^*})) &> U_m(\mathbf{P^*},\mathbf{J}(\mathbf{P^*})) - \gamma && (26)\\ &= U_m(\mathbf{P^*},\mathbf{J'}) + 2\gamma && (27)\\ &> U_m(\mathbf{P}[k],\mathbf{J}(\mathbf{P}[k])) + \gamma. && (28)\end{aligned}$$

Note that Eq. (28) conflicts with the assumption that $\mathbf{J}(\mathbf{P^*})$ is not the optimal strategy of the jammer. Therefore, we prove this lemma. ■

Theorem 2: The optimal strategy of the sensor $\mathbf{P}^{SE}$ exists and the Stackelberg equilibrium as $(\mathbf{P}^{SE},\mathbf{J}(\mathbf{P}^{SE}))$ can be obtained.

Proof: The continuity of $U_m(\mathbf{P},\mathbf{J})$ within the scope of $\mathcal{P} \times \mathcal{J}$. Considering **Lemma 2**, $\mathbf{J}(\mathbf{P})$ has continuity with $\mathbf{P}$. Therefore, the continuity of $U_m(\mathbf{P},\mathbf{J}(\mathbf{P}))$ in $\mathbf{P}$ has proved. Due to the compact set $\mathcal{P}$, there exists a maximum values of $U_m(\mathbf{P},\mathbf{J}(\mathbf{P}))$ at a certain point $\mathbf{P}^E \in \mathcal{P}$. The theorem proves. ■

With the existing of optimal solution , we propose an algorithm called renewed intelligent simulated annealing (RISA) to achieve the optimal strategy of the sensor, shown in **Algorithm 2**. RISA is a modified simulated annealing which has a better convergence performance than traditional simulated annealing.

In RISA, the initial temperature is denoted as $T > 0$, which is high enough. I and J are denoted as the number constraints of P_{best} and P'_{best}, respectively. q and p is the stay number of P'_{best} and P_{best}. i is the system time and θ_i is the feedback flag at time i. $\mathbf{P}_i$ is the feasible power strategy at time i and $neighbour(\mathbf{P}_i)$ is defined as: $P'_i = [P_i + \mu_i]$, where $\mu_i \in [-\mu,\mu]$. If $\sum_{i=1}^{n} P'_i \ge P_{max}$, we have $P'_i = \frac{P_{max} P'_i}{\sum_{i=1}^{n} P'_i}$. AN is denoted as the accepted number of U_{temp} at the same temperature and ξ indicate the temperature drop coefficient. When the accepted number of U_{temp} is low, it means that P_{best} will approaches to the equilibrium quickly. So the ξ is low and the changing rate of T is getting fast. On the contrary, the changing rate of T is getting slow. With the help of AN and ξ, the simulated annealing algorithm can decrease its iterations. When the algorithm is run over, we will achieve the Stackelberg Equilibrium of this optimization problem. In this algorithm, we can achieve the optimal profit of the sensor with the Stackelberg equilibrium P_{best}. Then, we obtain the optimal profit of sensor denoted as U_m with the Stackelberg equilibrium. Specifically, U_m is the maximum secrecy capacity of the sensor in this model.

V. Performance Evaluation

In this section, the performance of our algorithm is validated through the simulations and trace experiments. In the simulation analysis, we compare the equilibrium of proposed EDSJ with different scenarios. In the trace experiment analysis, we collect the traces from deployed experiments in our laboratory and compare the secrecy capacity and the power consumption of our algorithm with that of others via these traces.

A. Simulation Analysis

For the single-antenna model, the noise level N is given as 1, the gain coefficient a is set as 0.2, and the bandwidth W is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841033, IEEE Transactions on Industrial Informatics

Algorithm 3: RISA

Input: I, J, T
Output: $\mathbf{P}_{best}$

Randomly initialize $\mathbf{P}_1 \doteq \{P_i\}_{i=0}^{n}$, $\mathbf{P}_{best} \longleftarrow \mathbf{P}_1$;
while $T > 1$ *or* $p < I$ **do**
  $AN = 0$;
  while $q < J$ **do**
    $\theta_i = 0$;
    $\mathbf{P}_{temp} \longleftarrow$ *neighbour*$(\mathbf{P}_i)$;
    $\mathbf{P}'_{best} \longleftarrow \mathbf{P}_{best}$;
    Randomly select $\varepsilon \in (0,1)$;
    if $U_m(\boldsymbol{P}_{temp}, \boldsymbol{J}(\boldsymbol{P}_{temp})) \geq U_m(\boldsymbol{P}_i, \boldsymbol{J}(\boldsymbol{P}_i))$ *or* $\varepsilon \leq e^{(U_m(\boldsymbol{P}_{temp},\, \boldsymbol{J}(\boldsymbol{P}_{temp})) - U_m(\boldsymbol{P}_i,\, \boldsymbol{J}(\boldsymbol{P}_i)))/T}$ **then**
      $\theta_i = 1$;
      $q = 0$;
      $AN = AN + 1$;
      if $U_m(\boldsymbol{P}_{temp}, \mu(\boldsymbol{P}_{temp})) \geq U_m(\boldsymbol{P}'_{best}, \mu(\boldsymbol{P}'_{best}))$ **then**
        $\mathbf{P}'_{best} \longleftarrow \mathbf{P}_{temp}$;
      end
    end
    else
      $q = q + 1$;
    end
  end
  if $\theta_i = 1$ **then**
    $\mathbf{P}_i = \mathbf{P}_{temp}$;
  end
  else
    $\mathbf{P}_i = \mathbf{P}_{i-1}$;
  end
  if $U_m(\boldsymbol{P}_{best}, \boldsymbol{J}(\boldsymbol{P}_{best})) \geq U_m(\boldsymbol{P}'_{best}, \boldsymbol{J}(\boldsymbol{P}'_{best}))$ **then**
    $p = p + 1$;
  end
  else
    $\mathbf{P}_{best} \longleftarrow \mathbf{P}'_{best}$;
    $p = 0$;
  end
  $\xi = \frac{AN}{AN+J}$;
  $T \longleftarrow e^{-\xi} T$
end

set as 5. The costs of per transmission power of the jammer and sensor are $\alpha = 0.01$ and $\beta = 0.05$, respectively. The channel gains vector $[v_{sc}, v_{jc}, v_{se}, v_{je}]$ is set as [1, 1, 1.2, 1.5].

For the multi-antenna model, the channel gains v^i_{sc}, v^i_{jc}, v^i_{se} and v^i_{je} are randomly distributed in (0,2]. As in the single-antenna model, we set $a = 0.2$, $W = 5$, $N = 1$, $\alpha = 0.01$ and $\beta = 0.05$. In addition, we set $n = 3$ and $J_{max} = 10$. For the algorithm RISA, the parameters are set as $I = 20$, $J = 20$ and $T = 100$.

We present the changes of the sensor profit U_s and the jammer profit J_s versus the sensor transmission power P and the jammer transmission power J. Then, we compare the equilibrium of the proposed EDSJ in different scenarios:

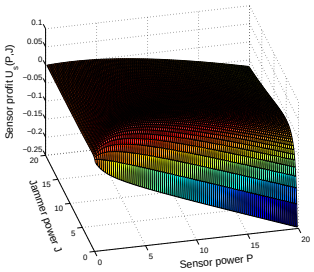


Fig. 3: $U_s(P,J)$ versus the power of sensor and jammer

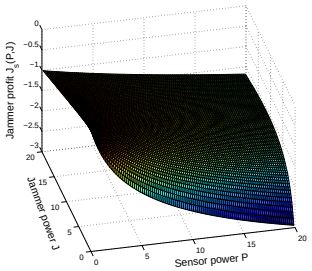


Fig. 4: $J_s(P,J)$ versus the power of sensor and jammer

- Random power allocation (RPA) [17]: The sensor and the jammer both allocate their power randomly. Obviously, the power allocations are feasible.
- Power allocation without regard to smart jammer (PAWSJ) [14]: The sensor achieves the maximum profit regardless of the existence of the jammer while the jammer is smart.
- Power allocation with mistakes (PAM) [18]: The sensor decides its power allocation with smart jammer existing, while the jammer is a traditional jammer which transmits interference signal with even power.

Kim *et al.* proposed a random power control approach in [17]. In order to make comparison with their own approaches, the PAWSJ and PAM approaches were shown in [14] and [18], respectively. We study these papers and employe these approaches to make comparison with the EDSJ approach.

Figs. 3 and 4 illustrate the results of the single-antenna model. The sensor's profit $U_s(P,J)$ and the jammer's profit $J_s(P,J)$ are shown as the transmission power of the sensor and the jammer. It is obvious that with the changes of P and J, there exists a maximum value of the sensor's profit $U_s(P,J)$. With the sensor's power P increase, the jammer's profit $J_s(P,J)$ decreases. Meanwhile, with the jammer's power J increase, the jammer's profit $J_s(P,J)$ increases at the beginning and then decreases. In this situation, with the assistance of control feedback, the sensor and the jammer will adjust their power P and J to achieve the maximum $U_s(P,J)$ as show in Fig. 3.

Figs. 5 and 6 show the impact of power constraint P_{max} on the profits of the sensor and the jammer under multi-antenna model. J_{max} is set as 10. When the P_{max} increases, the sensor's profits $U_m(\mathbf{P},\mathbf{J})$ of these scenarios except the PAWSJ raise and the jammer's profits $J_m(\mathbf{P},\mathbf{J})$ reduce. In our simulation, the RISA achieves the highest sensor's profit. Meanwhile, the jammer's profit of RISA is lower than PAM. PAWSJ is always the worst in both figures.

Figs. 7 and 8 illustrate the channel gains v^i_{se} how to influence the profits of the sensor and the jammer under multi-antenna model. When v^i_{se} increases, the profits of the sensor and the jammer increase and the values of them are close with each other. In each case of v^i_{se}, RISA leads to the highest sensor's profit and lower jammer's profit.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841033, IEEE Transactions on Industrial Informatics

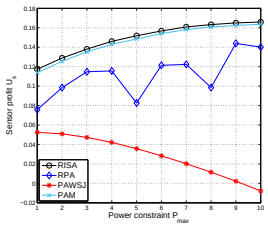


Fig. 5: Impact of P_{max} on sensor's profit

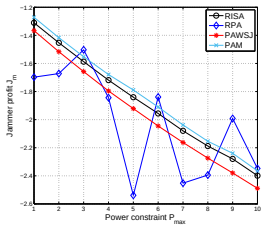


Fig. 6: Impact of P_{max} on jammer's profit

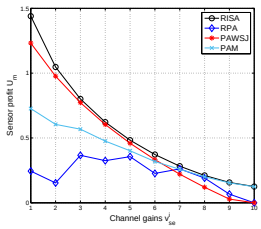


Fig. 7: Impact of v_{se}^i on sensor's profit

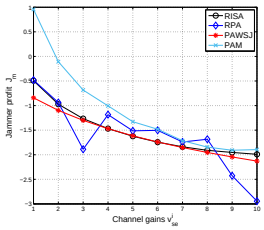


Fig. 8: Impact of v_{se}^i on jammer's profit

B. Trace Experiment Analysis

For the trace experiment, we deploy four equipments in the laboratory. Our experimental site is a meeting room and the size of the room is 15m*10m. One D-Link DIR-600M with a single antenna is used as the traffic sensor which transmit information to the remote controller. One desktop computer with TL-WN725N USB wireless card plays the role of remote controller to receive the information and is modified as in [35]. The other desktop computer with TL-WN725N USB wireless card plays the role of the malicious eavesdropper. Both of the computers run Windows 10 operation system and access the traffic sensor router. The other D-Link DIR-600M plays the role of malicious jammer and transmits jamming signals in the channel, which is the same as the channel of the traffic sensor. We set the jammer and the traffic sensor working in IEEE802.11n AP mode at 2.4GHz with 10MHz bandwidth. Hence, jammer can interference the signal transmission of the traffic sensor. The traffic sensor, remote controller, jammer and eavesdropper are deployed as Fig. 1. More precisely, the distance of the traffic sensor and remote controller, the distance of the traffic sensor and eavesdropper, the distance of the jammer and remote controller, and the distance of the jammer and eavesdropper is 5m, 10m, 15m and 5m, respectively. The jammer will affect eavesdropper more than traffic sensor. We can change the transmission power of the traffic sensor and jammer in the route setting interface. Transmission rate is achieve as the trace data. The difference between the remote controller's transmission rate and the eavesdropper's transmission rate is the secrecy capacity. Each experiment will last for one hour and repeats three times to get the average value. We compare the result in different models:

- Common wiretapping model (CWM) [19]: The eavesdropper intercepts the information between the traffic sensor and the remote controller. No jammer exists.
- Wiretapping model with friendly jammer (WMFJ) [20]: The main channel applies a friendly jammer to resist the eavesdropper.
- Wiretapping model with malicious jammer (WMMJ): The main channel applies a malicious jammer to resist the eavesdropper.

Fig. 9 shows the impact of the traffic sensor's power on the secrecy capacity on different models. The secrecy capacity of CWM is always the lowest and the growth range is also the lowest. The secrecy capacity and its increasing level of WMFJ and WMMJ are of little difference. In addition, Fig. 10 shows the power of friendly sides with the same secrecy capacity. The power of WMFJ is much higher than that of WMMJ due to the existence of friendly jammer's power. Hence, the WMMJ achieves a relatively high secrecy capacity with less power.

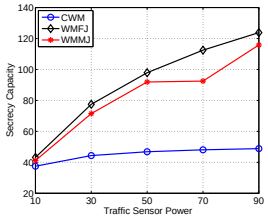


Fig. 9: Secrecy capacity versus the power of traffic sensor

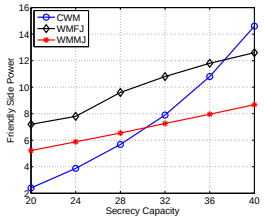


Fig. 10: Power of friendly side with the same secrecy capacity

VI. Related Work

A. Security in CPTS

In recent years, the CPS security has attracted many interests in recent years. Cárdenas *et al.* [21] studied the deception attacks and DoS attacks. The purpose of DoS attacks is to block the information exchange between different parts of the CPS. The purpose of Deception attacks is to cheat the systems and make them judge mistakes. Wu *et al.* [22] proposed a data integrity attack scheme at attacker side. An optimal feedback attack law is presented for maximizing the difference between the output of the attacked system and the secure system.

The security properties of CPTS were studied. Gokhale *et al.* [23] studied the timeliness and credibility of the control information in intelligent transportation systems. A CPS-based solution was proposed to overcome the physical and cyber interferences in order to improve these two characters. Zhou *et al.* [24] considered the privacy protection in CPS when the traffic state are collected. In this paper, they proposed a novel scheme which can gather the traffic flow data with protecting the privacy of each vehicle.

B. Jamming and Eavesdropping in the Physical Layer

With the transmission process security studied, the definition of secrecy capacity was applied to the system security. The secrecy capacity was established by Shannon in [25] and extended to the discrete memoryless channel with wiretap channel.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841033, IEEE Transactions on Industrial Informatics

With the existence of eavesdropper, some approaches [7, 9, 26] were proposed to protect the information security. Zheng $et\ al.$ [7] proposed a wireless network consisting of a single-antenna source, a multi-antenna destination and a multi-antenna eavesdropper. They apply the cooperating full-duplex jammers to improve the secrecy rate in this system. Han $et\ al.$ [26] considered a wireless transmission channel in the presence of a malicious eavesdropper. Multiple friendly jammers are employed to improve the communication security. Considering the interaction between source and jammer, a Stackelberg game was studied and the equilibrium was obtained.

In reality, jammers are not always friendly and maybe act as malicious nodes and this situation was considered in [14, 27, 28]. Yang $et\ al.$ [14] investigated the wireless networks with the existence of a smart jammer which wants to disturb the information transmission process. In addition, the jammer is intelligent to adjust its transmitted power for maximizing the effect of damage with knowing source's power. They studied the power control problem as a optimization problem and modeled the problem as a Stackelberg game. The jamming attacks on mobile CPS were studied in [27]. The attacks may degrade the quality of communication and that for mobile CPS were described. Wang $et\ al.$ [28] applied multiple relays to defend the threat of eavesdropping attacks. In order to maximize the secrecy transmission rate of a channel, three different power control schemes were presented.

C. Analysis with Game Theory

Game theory was applied to study the interactions between intelligent decision makers as an effective approach [29-31]. The game-theoretic frameworks that can improve the security of networks were summarized and classified in [32]. Miao $et\ al.$ [33] selected a system including one controller, one estimator and one detector from the CPS. A hybrid stochastic game model was proposed to model this system and a moving-horizon approach was presented to solve this game. In the end, they achieve a saddle-point equilibrium as a optimal strategy. Niyato $et\ al.$ [34] investigated a wireless powered network where the user can submit an energy demand to the energy source for its transmission power. In this system, they consider a malicious node which steal the energy to jam the information transmitted by the user. Then, they propose a game theoretic model to analyze the relationship between the attacker and the user. They designed an iterative algorithm to obtain the Nash equilibrium of this game.

Different from previous work, we consider the transmission security of GCPTS with the assistance of feedback in the presence of jamming attacks and eavesdropping attacks. When we try to mitigate the impacts of jamming attacks, the signal of the malicious jammer is used to reduce the wiretap quality of eavesdroppers. In this paper, we propose an eavesdropping attacks defense approach with the help of the malicious jammer. Then we study how to choose the power allocation of the sensor and the jammer to maximize the secure transmission rate with the control feedback.

VII. CONCLUSION

In this paper, we have investigated the eavesdropping defense issue in the transmission process of GCPTS with a smart jammer. The relationship between the sensor and the jammer is studied and jammer's transmission power proves as a function of the sensor's transmission. The sensor adjusts the transmitted power of it to obtain the maximum utility by the help of control feedback. Two system models, i.e., single-antenna model and multi-antenna, are used to analyze this problem. For both models, the Stackelberg game is applied to formulate this problem and the existence of equilibrium was proved. SAF and RISA are employed as efficient algorithms to obtain the optimal strategies. We conduct some experiments to validate the performance of our approach. The results match well with the theoretical analysis to demonstrate the correctness.

ACKNOWLEDGEMENT

This work is supported by NSFC (61572262); China Postdoctoral Science Foundation (2017M610252); China Postdoctoral Science Special Foundation (2017T100297); the projects 240079/F20 funded by the Research Council of Norway; the project Security in IoT for Smart Grids, with number 248113/O70 part of the IKTPLUSS program funded by the Norwegian Research Council, and Strategic Information and Communications R&D Promotion Programme (SCOPE No.162302008), MIC, Japan; the Open Research Fund of the Jiangsu Engineering Research Center of Communication and Network Technology, NJUPT; and the National Engineering Research Center of Communications and Networking (Nanjing University of Posts and Telecommunications) (TXKY17014).

REFERENCES

[1] D. P. F. Mller and H. Vakilzadian, "Cyber-physical systems in smart transportation," in *proc. 2016 IEEE Int. Conf. Electro. Inform. Technol.*, pp. 776-781, May. 2016.

[2] S. Xie, W. Zhong, K. Xie, R. Yu and Y. Zhang, "Fair energy scheduling for vehicle-to-grid networks using adaptive dynamic programming," *IEEE Trans. Neural Netw. Learning Syst.,* vol. 27, no. 8, pp. 1697-1707, Aug. 2016 .

[3] W. Zhong, K. Xie, Y. Liu, C. Yang and S. Xie, "Topology-aware vehicle-to-Grid energy trading for active distribution systems," *IEEE Trans. Smart Grid,* vol. PP, no. 99, pp. 1-9, Jan. 2018.

[4] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchain," *IEEE Trans. Indust. Inform.,* vol. 13, no. 6, pp. 3154-3164, May. 2017.

[5] X. Huang, R. Yu, J. Kang, Y. He, and Y. Zhang, "Exploring mobile edge computing for 5G enabled software defined vehicular networks," *IEEE Wirel. Commun.,* vol. 24, no. 6, pp. 55-63, Dec. 2017.

[6] H. Delfs and H. Knebl, *Introduction to Cryptography* vol.2 Berlin etc.: Springer, 2002.

[7] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using Full-Duplex jamming receivers," *IEEE Trans. Signal Process.,* vol. 61, no. 20, pp. 4962-4974, Jun. 2013.

[8] K. Wang, L. Yuan, T. Miyazaki, D. Zeng, S. Guo, and Y. Sun, "Strategic anti-eavesdropping game for physical layer security in wireless cooperative networks," *IEEE Trans. Veh. Technol.,* vol. 66, no. 10, pp. 9448-9457, Oct. 2017.

[9] X. Li and H. Dai, "Friendly-jamming: an anti-eavesdropping scheme in wireless networks," in *proc. Int. Sym. World Wireless (WoWMoM),* pp. 1-3, Jun. 2017.

[10] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," in *proc. 2016 IEE ICC,* pp. 1-6, May. 2016.

[11] X. He, K. Wang, T.Miyazaki, H. Huang, Y. Wang, and S. Guo, "Green resource allocation based on deep reinforcement learning in content-centric IoT," *IEEE Trans. Emerging Topics in Comput.,* vol. PP, no. 99, pp. 1-16, Feb. 2018.

[12] K. Wang, Y. Wang, Y. Sun, S. Guo, and J. Wu, "Green industrial Internet of Things architecture: an energy-efficient perspective," *IEEE Commun. Mag.,* vol. 54, no. 12, pp. 48-54, Dec. 2016.

[13] M. Gao, K. Wang, and L. He, "Probabilistic model checking and scheduling implementation of energy router system in energy internet for green cities," *IEEE Trans. Indust. Inform.,* vol. 14, no. 4, 1501-1510, Apr. 2018.

[14] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a smart jammer in wireless networks: a Stackelberg game approach," *IEEE Trans. Wireless Commun.,* vol. 12, no. 8, pp. 4038-4047, Jul. 2013.

[15] P. Clarke and R. C. Lamare "Joint iterative power allocation and relay selection for cooperative MIMO systems using discrete stochastic algorithms," in *proc. Wirel. Commun. Syst. 2011 Int. Symp.,* pp. 432-436, Nov. 2011.

[16] R. Zhang, L. Song, Z. Han, and B. Jiao, "Improve physical layer security in cooperative wireless network using distributed auction games," in *Porc. INFOCOM WKSHPS,* pp. 18-23, Apr. 2011.

[17] T. Kim and S. Kim, "Random power control in wireless ad hoc networks," *IEEE Commun. Lett.,* vol. 9, no. 12, pp. 1046-1048, Jan. 2006.

[18] B. Duan, Y. Cai, J. Zheng, and W. Yang, "Cooperative jammer power allocation - a Nash bargaining solution method," in *Porc. WCSP,* pp. 15-17, Oct. 2015.

[19] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. Journ.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[20] K. Wang, L. Yuan, T. Mizayaki, Y. Sun, and S. Guo, "Anti-eavesdropping with selfish jamming in wireless networks: a bertrand game approach," *IEEE Trans. Veh. Technol.,* vol. 66, no. 7, pp. 6268-6279, Jul. 2017.

[21] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: towards survivable cyber-physical systems," in *proc. 2008 ICDCS,* pp. 495-500, Jun. 2008.

[22] G. Wu and J. Sun, "Optimal data integrity attack on actuators in cyber-physical systems," in *proc. 2016 Amer. Control Conf.,* pp. 1160-1164, Jul. 2016.

[23] A. Gokhale, M. P. Mcdonald, S. Drager, and W. Mckeever, "A cyber physical systems perspective on the real-time and relibale dissemination of information in intelligent transportation systems," *Macrothink Institute,* vol. 2, no. 3, pp. 116-136, Oct. 2010.

[24] Y. Zhou, Z. Mo, Q. Xian, S. Chen, and Y. Yin, "Privacy-preserving transportation traffic measurement in intelligent cyber-physical road systems," *IEEE Trans. Veh. Technol.,* vol. 65, no. 5, pp. 3749-3759, May. 2016.

[25] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. Journ.*, vol. 8, no. 4, pp. 656-715, Apr. 2014.

[26] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," in *Proc. GameNets,* pp. 287-294, May. 2009.

[27] E. Guirguis, Mina Guirguis, and N. Halkude, "A case for low-level jamming attacks on mobile CPS in target tracking applications ," in *proc. 2012 Int. Symp. Pervasive Syst. Algor. Netw.,* pp. 216-221, Dec. 2012.

[28] H. M. Wang, Q. Yin, and X. G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.,* vol. 60, no. 7, pp. 3532-3545, Jul. 2012.

[29] R. Gibbons, *A primer in game theory* Harvester Wheatsheaf Hemel Hempstead, 1992.

[30] K. Wang, M. Du, D. Yang, C. Zhu, J. Shen, and Y. Zhang, "Game theory-based active defense for intrusion detection in cyber-physical embedded systems," *ACM Trans. Embedded Comput. Syst.,* vol. 16, no. 1, article 18, Oct. 2016.

[31] K. Wang, M. Du, S. Maharjan, and Y. Sun, "Strategic honeypot game model for distributed denial of service attacks in the smart grid," *IEEE Trans. Smart Grid,* vol. 8, no. 5, pp.2474-2482, Sep. 2017.

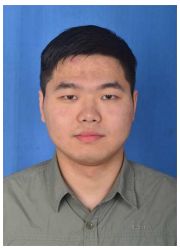
[32] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *proc. Syst. Sci. 2010 Hawaii Int. Conf.,* pp. 1-10, Jan. 2010.

[33] F. Miao and Q. Zhu, "A moving-horizon hybrid stochastic game for secure control of cyber-physical systems," in *proc. IEEE Conf. Decis. Contr.,* pp. 517-522, Dec. 2014.

[34] D. Niyato, P. Wang, D. I. Kim, Z. Han, and L. Xiao, "Game theoretic modeling of jamming attack in wireless powered communication networks," in *proc. IEEE ICC,* pp. 6018-6023, Jun. 2015.

[35] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, "Tool release: Gathering 802.11n traces with channel state information," *ACM SIGCOMM Comput. Commun. Rev.,* vol. 41, no. 1, pp. 53-53, Jan. 2011.

Kun Wang received two PhD degrees from Nanjing University of Posts and Telecommunications,China in 2009 and from the University of Aizu, Japan in 2018, respectively, both in Computer Science. From 2013 to 2015, he was a Postdoc Fellow in Electrical Engineering Department, University of California, Los Angeles (UCLA), CA, USA. He is currently a Research Fellow in the Department of Computing, the Hong Kong Polytechnic University, Hong Kong, China, and also a Full Professor in the School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing, China. He has published over 100 papers in referred international conferences and journals. He has received Best Paper Award at IEEE GLOBECOM16. He serves as Associate Editor of IEEE Access, Editor of HYPERLINK http://www.journals.elsevier.com/ journal-of-network-and-computer-applications/ Journal of Network and Computer Applications, Journal of Communications and Information Networks, EAI Transactions on Industrial Networks and Intelligent Systems and Guest Editors of IEEE Access, Future Generation Computer Systems, Peer-to-Peer Networking and Applications, and Journal of Internet Technology. He was the symposium chair/co-chair of IEEE IECON16, IEEE EEEIC16, IEEE WCSP16, IEEE CNCC17, etc. His current research interests include area of big data, wireless communications and networking, smart grid, energy Internet, and information security technologies. He is a senior member of the IEEE and member of the ACM.



Li Yuan is a postgraduate student in Information Security at Nanjing University of Posts and Telecommunications, China. His current research interests include Wireless Networks, physical layer security.

Toshiaki Miyazaki received the BE and ME degrees in applied electronic engineering from the University of Electro-Communications, Tokyo, Japan in 1981 and 1983, respectively, and the PhD degree in electronic engineering from the Tokyo Institute of Technology in 1994. He is a professor of the University of Aizu, Fukushima, Japan, and the dean of the Undergraduate School of Computer Science and Engineering. His research interests are in reconfigurable hardware systems, adaptive networking technologies, and autonomous systems. Before joining the University of Aizu, he has worked for NTT for 22 years, and engaged in research on VLSI CAD systems, telecommunications-oriented FPGAs and their applications, active networks, peer-to-peer communications, and ubiquitous network environments. He was a visiting professor of the graduate school, Niigata University in 2004, and a part-time lecturer of the Tokyo University of Agriculture and Technology in 2003-2007. He is a senior member of the IEEE, IEICE and IPSJ.

Yuanfang Chen received her Ph.D. and M.S. degrees from Dalian University of Technology, China, and second Ph.D. degree from University Pierre and Marie CURIE, France. She currently works in Hangzhou Dianzi University as a Professor. She was an assistant researcher of Illinois Institute of Technology, USA with Prof. Xiangyang Li. She has been invited as the Session Chair of some conferences, the associate editor of Industrial Networks and Intelligent Systems, and the guest editor of MONET.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2841033, IEEE Transactions on Industrial Informatics

Yan Zhang is Full Professor at the Department of Informatics, University of Oslo, Norway. He received a PhD degree in School of Electrical & Electronics Engineering, Nanyang Technological University, Singapore. He is an Associate Technical Editor of IEEE Communications Magazine, an Editor of IEEE Network Magazine, an Editor of IEEE Transactions on Green Communications and Networking, an Editor of IEEE Communications Surveys & Tutorials, an Editor of IEEE Internet of Things Journal, an Editor of IEEE Vehicular Technology Magazine, and an Associate Editor of IEEE Access. He serves as chair positions in a number of conferences, including IEEE GLOBECOM 2017, IEEE VTC-Spring 2017, IEEE PIMRC 2016, IEEE CloudCom 2016, IEEE ICCC 2016, IEEE CCNC 2016, IEEE SmartGridComm 2015, and IEEE CloudCom 2015. He serves as TPC member for numerous international conference including IEEE INFOCOM, IEEE ICC, IEEE GLOBECOM, and IEEE WCNC. His current research interests include: next-generation wireless networks leading to 5G, green and secure cyber-physical systems (e.g., smart grid, healthcare, and transport). He is IEEE VTS (Vehicular Technology Society) Distinguished Lecturer. He is also a senior member of IEEE, IEEE ComSoc, IEEE CS, IEEE PES, and IEEE VT society.