TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 12/15 pp523–535
DOI: 10.26599/TST.2020.9010020
Volume 26, Number 4, August 2021

A Cross-Layer Cooperative Jamming Scheme for Social Internet of Things

Yan Huo*, Jingjing Fan, Yingkun Wen, and Ruinian Li

Abstract: In this paper, we design a friendly jammer selection scheme for the social Internet of Things (IoT). A typical social IoT is composed of a cellular network with underlaying Device-to-Device (D2D) communications. In our scheme, we consider signal characteristics over a physical layer and social attribute information of an application layer simultaneously. Using signal characteristics, one of the D2D gadgets is selected as a friendly jammer to improve the secrecy performance of a cellular device. In return, the selected D2D gadget is allowed to reuse spectrum resources of the cellular device. Using social relationship, we analyze and quantify the social intimacy degree among the nodes in IoT to design an adaptive communication time threshold. Applying an artificial intelligence forecasting model, we further forecast and update the intimacy degree, and then screen and filter potential devices to effectively reduce the detection and calculation costs. Finally, we propose an optimal scheme to integrate the virtual social relationship with actual communication systems. To select the optimal D2D gadget as a friendly jammer, we apply Kuhn-Munkres (KM) algorithm to solve the maximization problem of social intimacy and cooperative jamming. Comprehensive numerical results are presented to validate the performance of our scheme.

Key words: Internet of Things (IoT); artificial intelligence; Device-to-Device (D2D) communications; social network; cooperative jamming

1 Introduction

As one of the core researches of 5G wireless communications, enhanced mobile broadband provides convenience for numerous applications[1]. People are increasingly using multimedia services, such as virtual reality, augmented reality, real-time broadcasting, telemedicine, and distance education to publish various data[2–4]. These diverse services promote the development of a heterogeneous Internet of Things (IoT) ecosystem and induce the explosive growth of billions of wireless devices[5,6]. A typical heterogeneous IoT system is composed of a cellular network with underlaying Device-to-Device (D2D) communication[7,8]. In this system, secure interconnection of massive wireless devices with higher-level requirements has been put forward for heterogeneous network resources and hardware capabilities.

Traditional methods for achieving a secure communication with high spectrum utilization include spectrum sensing and reusing technologies for the physical layer[9,10] and cryptography-based security mechanisms for the network layer[11–13]. However, both methods are difficult to implement in massive low-capability IoT devices. Spectrum sharing for numerous devices may cause collisions and interference, which lead to failure in reuse. Meanwhile, low-capability devices may lack hardware resources and computing capability to achieve encrypted communication.

• Yan Huo, Jingjing Fan, and Yingkun Wen are with the School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China. E-mail: {yhuo, 18120050, wenyingkun}@bjtu.edu.cn.
• Ruinian Li is with the Department of Computer Science, Bowling Green State University, Bowling Green, OH 43403, USA. E-mail: lir@bgsu.edu.
∗To whom correspondence should be addressed.
Manuscript received: 2020-04-22; revised: 2020-06-11; accepted: 2020-06-12

Thus, cooperative jamming communication is one of the promising technologies to achieve secure interconnection of massive wireless devices in an IoT system.

Cooperative jamming-based physical layer security exploits Artificial Noise (AN) to block eavesdroppers without degrading the receiving performance of legitimate nodes[14]. In review studies of cooperative jamming, all existing methods focus on the design of physical layer characteristics, including Channel State Information (CSI), signal power and phase, and antenna transmit parameters. These studies always select a friendly jammer to send AN to achieve the maximal secrecy capacity or minimal secrecy outage probability. However, they ignore a basic problem, i.e., the relationship between a candidate friendly jammer and the target legitimate node[15]. If an excellent social relationship exists between a candidate and the target legitimate node, the candidate is willing to transmit beneficial AN; otherwise, it may not provide cooperative jamming. Thus, how to reasonably select a candidate jammer is a bottleneck to achieve secure communications.

In this paper, we present a cross-layer-based cooperative jamming scheme for a heterogeneous IoT system. In the scheme, we intend to exploit social relationships to select a feasible D2D gadget to help cellular users achieve secure communication. In particular, we utilize a novel approach to quantify the intimacy degree based on social relationship (contact history records among devices) of the application layer. Specifically, we introduce the number of successful communications to describe social intimacy. Here, the premise of successful communication is that two devices have enough contact duration to avoid communication interruption and device reselection. This duration must be longer than the minimum contact duration threshold, and the threshold should be an adaptive set to adapt to changeable scenarios.

After analyzing the large amount of social relationships over the application layer, we further exploit Artificial Intelligence (AI) to predict social intimacy[16–18]. Here, AI is a kind of development software and machine which can imitate human-like intelligence to capture abstraction of social relationships in the application layer. We use an AI forecasting model, called the Prophet forecasting model, to mine the subsequent social intimacy[19–21]. In the Prophet model, different prediction technologies, such as auto-regressive integrated moving average and exponential smoothing, are considered. Compared with the general prediction models, the Prophet model can create reasonable and accurate forecasts in a simpler and more direct manner. This model is also robust against lost and abnormal data and can identify outliers and deal with complex features in a time series. Based on the calculated intimacy between devices, potential devices are screened and filtered to effectively reduce the detection and calculation costs.

In accordance with the social relationship analysis, we design an optimal scheme to closely integrate virtual social relationships with actual communication systems. In the scheme, we intend to find an optimal solution for the normalization indexes of intimacy, security rate of cellular nodes, and D2D throughput. This co-optimization problem for cellular nodes and D2D gadgets can be regarded as the maximum matching problem of the weighted bipartite graph. To find the optimal match, we apply Kuhn-Munkres (KM) algorithm to solve the maximization problem. The main contributions of this paper are summarized as follows.

- We propose a cross-layer-based friendly jammer selection scheme, where both physical layer security and social interactions in the application layer are considered, in a social IoT system. In the physical layer, the selected friendly jammer sends out jamming signals to improve the secrecy performance of the network. In the application layer, we use contact history records among devices to quantify the degree of social intimacy.
- We design an adaptive communication time threshold. The adaptive threshold can be adjusted based on changeable scenarios. We also exploit the Prophet model, which is robust against lost and abnormal data, to create a reasonable and accurate social intimacy forecast.
- We formulate an optimization problem to find the optimal match between D2D and cellular devices in social IoT systems, and then use the KM algorithm to solve the optimization problem.

The rest of the paper is organized as follows. The related work is reviewed in Section 2. In Section 3, we provide a cross-layer heterogeneous IoT system with cellular and D2D communications on the physical layer and abstract the corresponding social relationship on the application layer. Next, we analyze social relationship among nodes in the IoT system and present a cross-layer-based friendly jammer selection scheme in Section 4. We report our numerical simulation results to discuss the performance of our scheme in Section 5. Finally, we

draw a conclusion in Section 6.

2 Related Work

Cooperative jamming-based communication, which was proposed by Tekin and Yener[22], is an effective technology to achieve secure transmission. They designed an optimal policy to preserve secrecy via stopping nodes from transmission. Following this work, existing studies on cooperative jamming focused on secure communication in various scenarios, including relay networks[23], full-duplex networks[24], multiple antenna systems[25], energy-constrained systems[26], D2D communications[27], and heterogeneous networks[28]. Most of these works formulated different optimization problems based on various network frameworks, designed beamforming vectors and precoding matrices, optimized jamming transmission power, and finally achieved secure communication. Essentially, these methods are implemented based on the signal processing technology over the physical layer.

We consider the secure transmission in D2D communications as an example. D2D communication[29] is a direct communication between two nodes without a base station. This type of communication has attracted major attention due to its potential capability to improve spectrum efficiency. Zhang et al.[30] derived an optimal power control scheme, designed a secrecy-based access control scheme, and used a max-coalition order to present a merge-and-split-based coalition formation algorithm to achieve efficient cooperation for cellular links and D2D devices. Other authors formulated a trading scheme with two situations in which base stations or D2D transmitters play the leader role and achieve the Stackelberg equilibrium via closed form solutions[27]. One study provided an adaptive jamming receiver to adapt to different receiving modes in a D2D link[31]. This work optimized transmitted powers, secrecy rate, and mode switch criteria in the case of secrecy outage probability constraint. Given a nonorthogonal multiple access-based cooperative D2D network, in another work, jamming signals were injected to a full-duplex receiver to actively prevent eavesdropping without interfering with legitimate receivers[32].

The above studies on secure D2D communication only focused on physical signal processing and transmitted power optimization. However, a physical network not only has inherent physical characteristics, but also the corresponding inter-entities relationships that cannot be ignored. With the emergence of social network, several scholars noticed its serious effect and studied various schemes while considering social characteristics[33]. Social relationships motivated the strong desire for cooperation among cellular and D2D devices. Several researchers introduced node attributes to the cooperative jamming design and analyzed the impact of attributes on security performance of D2D communication. Wang et al.[34] evaluated the trust degree of potential jammers and designed an algorithm to select a jammer and allocate transmission power to achieve secrecy-oriented D2D cooperation. Similarly, Wen et al.[35] investigated the influence of node reputation on the secrecy performance and proposed a scheme for trustworthy-friendly jammer selection in perfect and statistical CSI scenarios. Wang et al.[36] formulated a double-gamma-ratio approach to describe social trust degree and obtained closed forms of connection outage probability and secrecy outage probability. Zhao et al.[37] introduced either altruistic or selfish feature into a distributed resource allocation scheme with low computation complexity and achieved Nash equilibrium for the proposed social group utility maximization game. One study proposed a data dissemination scheme based on social tie strength and utilized different mechanisms in accordance with the application environment[38]. Another research presented a social-community-aware D2D resource allocation framework underlying cellular networks and solved a two-step coalition game by adopting merge-and-split iterations[39].

A notable challenge in above works is the lack of a specific description of social relationship measurement. Most of these research used node properties, such as trust degree or reputation, to enhance system performance[40–42]. These properties are inherent social features of an individual node, whereas social relationship is the basic characteristic of the application layer. In Ref. [43], the authors defined social relationship with content popularity and user impacts, and designed a joint power, channel and link allocation, and welfare maximization scheme based on social influence to improve system efficiency. Wu et al.[44] exploited social ties relying on common friends and transmission bytes with a two-sided provider-demander matching algorithm with respect to power control and pairing scheduling. In addition, Sun et al.[45] modeled social relationship used the Bayesian nonparametric model to integrate historical observation sets from the social network and presented a coalitional graph game to realize efficient data spreading.

However, social relationships between devices are constantly updated over time due to the time-varying characteristics of interactive records in D2D communication. To the best of our knowledge, no research reported the use of changeable social relationship to implement power control and resource allocation. We apply the time series model prediction method to calculate social relationships between devices, and then exploit the predicted relationship to achieve secure communication and improve the system transmission rate.

3 System Model and Preliminary

3.1 Network model

We consider a heterogeneous IoT system with cellular and D2D communications (Fig. 1). In the view of physical layer, the system is composed of a Macro Base Station (MBS), N_c cellular devices, and N_d D2D gadgets. The MBS with a single antenna located in a macro cellular can provide data transmission for cellular (legitimate) nodes randomly located within the communication range. These nodes do not interfere with each other due to the orthogonality of spectrum resource allocation. The D2D gadgets with a single antenna are scattered in the macro cellular. They share spectrum with the cellular nodes in an underlaying paradigm. Given direct communications, the distance between both sides of the underlaying D2D communication is restricted to less than $D_{\max}$.

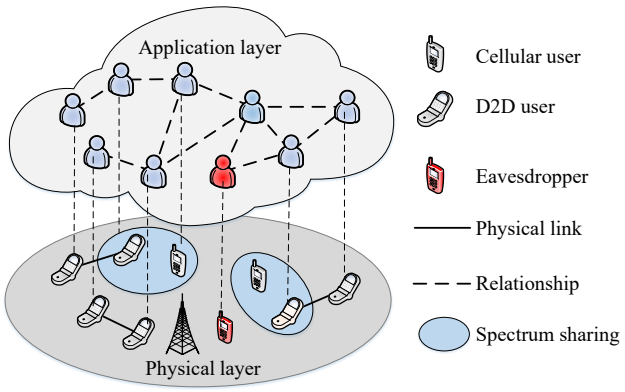

Fig. 1 Heterogeneous IoT system supporting D2D communication.

A single-antenna malicious node, called as an eavesdropper, exists in the IoT system. The eavesdropper constantly desires to eavesdrop messages transmitted from cellular devices to the MBS. To protect the transmitted messages from being eavesdropped, cellular users may select a D2D gadget as a friendly jammer to interfere with the eavesdropper. In return, the D2D gadget may be allowed to use the cellular spectrum to communicate with the D2D receiver.

In the view of application layer, the above physical entities can be mapped into nodes with various social relationships. The relationships include ordinary, affiliated, familiar, stable, and close. In our work, we exploit contact history records to compute intimacy, so as to measure these various relationships. Intuitively, high intimacy of two nodes indicates their high frequency contact and closeness. When selecting one node as a jammer, the user should be willing to assist their close friend to achieve cooperative jamming-based secure communication. On the contrary, poor intimacy implies rare communication with each other, i.e., an ordinary relationship. One node may not use its own energy to transmit AN for an ordinary friend. As a result, we can discuss the influence of social relationships on jammer selection and exploit the intimacy to modulate the implementation of cooperative jamming.

In order to better describe the signal transmission model in the following subsection, we list the notations and their descriptions in Table 1.

3.2 Signal transmission model

Within the physical layer, the i-th cellular device (C_i) transmits its signals s_c^i to the MBS, whereas the j-th

Table 1 Notation and the corresponding description.

Notation	Description
C_i, D_j	The i-th cellular device and the j-th D2D transmitter, respectively
h_{cb}^i, h_{ce}^i, h_{cd}^{ij}, h_{db}^j, h_{de}^j, h_{dd}^j	Channel fading from C_i and D_j to the MBS, the eavesdropper, and the D2D receiver
α	Path loss factor
σ^2	Variance of additive white Gaussian noise
α^{ij}, Ω	Binary matching indicator and its set of cooperative jamming
p_c^i, p_d^j	Transmission power of C_i and D_j, respectively
γ_{cb}^i, γ_{ce}^i, γ_{dd}^j	Received Signal to Interference plus Noise Ratio (SINR) at the MBS, the eavesdropper, and the D2D receiver
R_c^i,R_d^j	Achievable data rate of C_i and D_j, respectively
$\omega_{\mathrm{Ph}}^{ij}$, $\omega_{\mathrm{So}}^{ij}$, u_{cd}^{ij}	Utility of physical, social, and physical-social layers, respectively

D2D transmitter (D_j) sends s_d^j to its corresponding receiver. Then, received signals at the MBS, the eavesdropper, and the j-th D2D receiver can be expressed as follows:

$$y_{\mathrm{cb}}^i = h_{\mathrm{cb}}^i s_c^i + \sum_{j=1}^{N_d} \alpha^{ij} h_{\mathrm{db}}^j s_d^j + n_c \tag{1}$$

$$y_{\mathrm{ce}}^i = h_{\mathrm{ce}}^i s_c^i + \sum_{j=1}^{N_d} \alpha^{ij} h_{\mathrm{de}}^j s_d^j + n_e \tag{2}$$

$$y_{\mathrm{dd}}^j = h_{\mathrm{cd}}^{ij} s_c^i + \sum_{j=1}^{N_d} \alpha^{ij} h_{\mathrm{dd}}^j s_d^j + n_d \tag{3}$$

where n_c, n_e, and n_d are the Additive White Gaussian Noise (AWGN) over each transmission link, which have complex normal distributions $\mathcal{CN}(0, \sigma^2)$ over each transmission link. We define a set of binary matching indicator variables as $\Omega = \{\alpha^{ij}\}$. The variables denote whether C_i and the j-th D2D pair cooperate to achieve cooperative jamming and spectrum multiplexing. If C_i selects the j-th D2D pair, α^{ij} is set as 1, otherwise α^{ij} is set as 0. For the simplicity of calculation, the quasi-static channel fading of our wireless transmission model is modeled as $h_{uv}^w = g_{uv}^w (d_{uv}^w)^{-\frac{\alpha}{2}}$, $u, v \in \{c, b, e, d\}$, $w \in \{i, j\}$. The small-scale Rayleigh fading g_{uv}^w is distributed as $\mathcal{CN}(0, 1)$. Meanwhile, $(d_{uv}^w)^{-\frac{\alpha}{2}}$ is the standard path loss for the large-scale fading, where d_{uv}^w is the distance from transmitter u to receiver v and α is the path loss factor.

Based on the above signal transmission model, the correspondingly received SINR at the MBS, the eavesdropper, and the D2D receiver can be expressed as follows:

$$\gamma_{\mathrm{cb}}^i = \frac{p_c^i |h_{\mathrm{cb}}^i|^2}{\sum_{j=1}^{N_d} \alpha^{ij} p_d^j |h_{\mathrm{db}}^j|^2 + \sigma^2} \tag{4}$$

$$\gamma_{\mathrm{ce}}^i = \frac{p_c^i |h_{\mathrm{ce}}^i|^2}{\sum_{j=1}^{N_d} \alpha^{ij} p_d^j |h_{\mathrm{de}}^j|^2 + \sigma^2} \tag{5}$$

$$\gamma_{\mathrm{dd}}^j = \frac{\sum_{j=1}^{N_d} \alpha^{ij} p_d^j |h_{\mathrm{de}}^j|^2}{p_c^i |h_{\mathrm{cd}}^{ij}|^2 + \sigma^2} \tag{6}$$

where $p_c^i = |s_c^i|^2$ and $p_d^j = |s_d^j|^2$ refer to the transmission power of C_i and D_j, respectively.

Given the SINR expressions from Eqs. (4)–(6), the achievable secrecy data rate of the i-th cellular device C_i can be given by the following equation:

$$R_c^i = [\log_2(1 + \gamma_{\mathrm{cb}}^i) - \log_2(1 + \gamma_{\mathrm{ce}}^i)]^+ \tag{7}$$

where $[\cdot]^+ \triangleq \max(\cdot, 0)$. In addition, if the j-th D2D pair reuses the spectrum resources via the cellular network, its transmission data rate is given by

$$R_d^j = \log_2(1 + \gamma_{\mathrm{dd}}^j) \tag{8}$$

Using the above expressions of secrecy rate (Eq. (7)) and transmission rate (Eq. (8)), we further introduce social relationship to formulate an optimization problem to maximize the total utility of the heterogeneous IoT system supporting D2D communication.

4 Cross-Layer Cooperative Jamming Scheme Based on Social Relationship

In this section, we propose a cross-layer cooperative jamming scheme (Fig. 2). In the scheme, we first analyze social relationship in the heterogeneous IoT system with cellular and D2D communications. We define the intimacy degree based on the contact history records between devices and predict the social intimacy by using the Prophet forecasting model. Next, we formulate an achievable rate maximization problem and propose the cross-layer cooperative jamming scheme.

In an actual scenario, device locations and social relationships are constantly updated over time. We present a framework to update the optimal scheme as shown in Fig. 3. We assume that the time period is T_1, $T_2, \ldots, T_{n+m}$. Here n and m denote the label of the time periods. We take the first m time periods as historical records of the social relationship. The physical utility is updated with the locations update for D2D and cellular

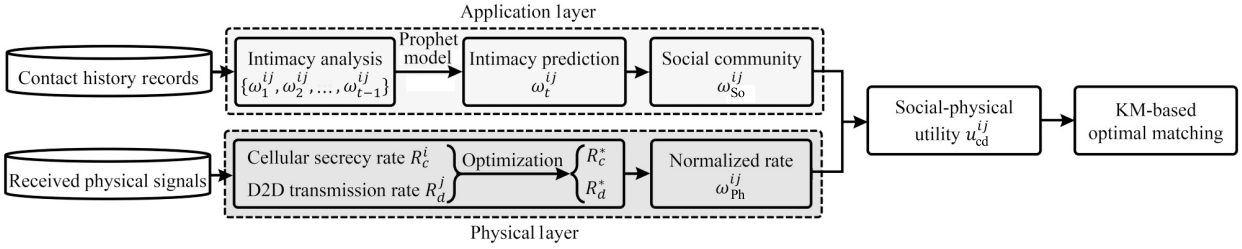

Fig. 2 Framework of proposed scheme.

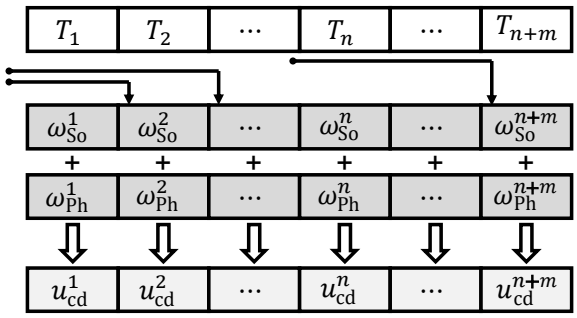

Fig. 3 Framework to update the optimal scheme.

devices. In the social layer, the previous maximum of m time periods is used as contact history records. Based on the physical utility and the social intimacy, we update the optimization scheme accordingly.

4.1 Analysis of social relationship

We introduce a social layer model to identify the suitability and reciprocity of cellular nodes and D2D gadgets. In real scenarios, a device always cooperates with its familiar and close friends. Taking full advantage of social relationship can effectively motivate cooperation and stop selfishness. Then, we can extract and utilize interactive information to analyze social relationship during the cooperation process. In Fig. 1, devices (including cellular users and D2D gadgets) naturally construct a community with inherent social ties. We define intimacy as a reflection and characterization of the degree of devices' tight social relationship with one another. In particular, we use a weighted graph $G = \{V, E, \omega\}$ to model a social domain, where V is the set of vertices corresponding to the cellular devices and D2D gadgets, E refers to the set of available edges in terms of whether social ties exist between devices, and $\omega_{\mathrm{So}}^{ij}$ denotes the social graph weight, ω, assigned to C_i and D_j, which is the quantitatively measured strength of social intimacy.

4.1.1 Intimacy degree

In general, social intimacy is related to the contact history between devices in the heterogeneous IoT system. In the existing references, the distribution of devices' contact duration is modeled as a Gamma distribution $\Gamma(k,\theta)$[46,47], where k and θ are two parameters that determine the shape of the distribution function. The values of k and θ are related with the mean and variance of the contact duration. We assume that each contact process between different devices is independent of one another, and use CD_{ij}^n and CN_{ij} to represent the record of contact duration and the number of contacts for C_i and D_j. The statistically expected contact duration E_{ij} of the contact process and the variance Var_{ij} to reflect the dispersion degree can be computed as follows:

$$E_{ij} = \frac{\sum\limits_{n} \mathrm{CD}_{ij}^n}{\mathrm{CN}_{ij}},\ \mathrm{Var}_{ij} = \frac{\sum\limits_{n} (\mathrm{CD}_{ij}^n - E_{ij})^2}{\mathrm{CN}_{ij}}.$$

Based on the mean and variance of the contact process, the contact duration distribution is as follows:

$$\mathrm{CD}_{ij}^n \sim \Gamma(k,\theta) = \Gamma(E_{ij}^2/\mathrm{Var}_{ij}, \mathrm{Var}_{ij}/E_{ij}).$$

Then, we can obtain the probability density function of the contact duration,

$$f(x_{ij};k,\theta) = \frac{1}{\theta^k}\frac{1}{\Gamma(k)} x_{ij}^{k-1} \mathrm{e}^{-\frac{x_{ij}}{\theta}},$$

where $\Gamma(\cdot)$ is the Gamma function. An important prerequisite for successful communication is that the contact duration cannot be less than the minimum threshold $\mathrm{CD}_{ij}^{\min}$.

In addition, we exploit CP_{ij} to denote the probability of qualified contact duration, i.e.,

$$\mathrm{CP}_{ij} = \int_{\mathrm{CD}_{ij}^{\min}}^{\infty} f(x_{ij};\, k,\theta)\mathrm{d}x_{ij} = 1 - \frac{\gamma(k, \frac{\mathrm{CD}_{ij}^{\min}}{\theta})}{\Gamma(k)} \quad (9)$$

where $\gamma(\cdot)$ is the lower incomplete Gamma function. In this case, how to determine $\mathrm{CD}_{ij}^{\min}$ plays a core role in the calculation of CP_{ij}. If $\mathrm{CD}_{ij}^{\min}$ is set at extremely high value, the probability CP_{ij} will be notably low. This condition will result in a limited number of devices that will be eligible to cooperate with each other, and vice versa. The threshold expresses the degree of feasibility and acceptance of device communication. The determination of the threshold must be consciously objective, which also forms the evident characteristics of the method for determining the threshold.

Assuming the mean, minimum, and maximum of E_{ij} as $\overline{E}$, $E^{\min}$, $E^{\max}$, respectively, we define two average values as $\overline{E^1} = (E^{\min} + \overline{E})/2$ and $\overline{E^2} = (E^{\max} + \overline{E})/2$. The threshold $\mathrm{CD}_{ij}^{\min}$ is selected based on E_{ij} to adapt to the devices' contact network, which can be represented as follows:

$$\mathrm{CD}_{ij}^{\min} = \begin{cases} E^{\min}, & \text{if } E_{ij} < \overline{E^1}; \\ \overline{E^1}, & \text{if } \overline{E^1} \leqslant E_{ij} < \overline{E}; \\ \overline{E}, & \text{if } \overline{E} \leqslant E_{ij} < \overline{E^2}; \\ \overline{E^2}, & \text{else.} \end{cases}$$

Considering the success probability CP_{ij} and the number of contacts CN_{ij} comprehensively, we obtain the number of successful communications $\mathrm{SN}_{ij} = \mathrm{CP}_{ij}\mathrm{CN}_{ij}$. The

strength of social intimacy can be normalized as follows:

$$\omega_{\mathrm{So}}^{ij} = \frac{\mathrm{SN}_{ij}}{\sqrt{\mathrm{SN}_i \mathrm{SN}_j}} \tag{10}$$

where $\mathrm{SN}_i = \sum_{j=1}^{N_d} \mathrm{SN}_{ij}$ and $\mathrm{SN}_j = \sum_{i=1}^{N_c} \mathrm{SN}_{ij}$ denote the total interaction in the application layer of C_i and D_j, respectively.

4.1.2 Prediction of social intimacy

Social relationship between devices is related to human behavior. This relationship can be regular and predictable in the interaction process. According to the theoretical analysis above, the value of social intimacy can be calculated and can be mapped into a time series $\{\omega_{t-1}^{ij}, \omega_{t-2}^{ij}, \ldots\}$. The prediction of social intimacy at time t, denoted by ω_t^{ij}, is carried out by the Prophet forecasting model. The range of social intimacy is $\omega_t^{ij} \in [0, 1]$. Here, 0 means that the two nodes have never intersected. Furthermore, high value of ω_t^{ij} implies the close relationship between two nodes.

The Prophet model allows us to intuitively adjust interpretable parameters for the time series prediction. The output of the Prophet model is given by the following:

$$\omega(t) = g(t) + s(t) + h(t) + \epsilon_t \tag{11}$$

where $g(t)$ represents the trend to fit nonperiodic changes in a time series, $s(t)$ is the seasonality reflecting periodic changes, $h(t)$ denotes the effect caused by holidays, festivals, and other special occasions, and ϵ_t is the error term reflecting the random and unpredictable fluctuations. Here, ϵ_t follows a normal distribution $\mathcal{CN}(0, \sigma_e^2)$ and its parameter σ_e^2 is estimated from data.

In the Prophet model, we model the trend term $g(t)$ of Eq. (11) as a piecewise linear function, which can be expressed as follows:

$$g(t) = (b + \boldsymbol{a}(t)^{\mathrm{T}}\boldsymbol{\eta})t + (d + \boldsymbol{a}(t)^{\mathrm{T}}\boldsymbol{\zeta}) \tag{12}$$

where $b + \boldsymbol{a}(t)^{\mathrm{T}}\boldsymbol{\eta}$ is the growth rate of the trend, b is the growth rate, $\boldsymbol{\eta}$ is the adjustment of b based on the change points. η_j represents the amount of change in the growth rate on the timestamp t_j. $\boldsymbol{a}(t) \triangleq [a_j(t)] \in \{0, 1\}$ is defined as a binary indicator function,

$$a_j(t) = \begin{cases} 1, & \text{if } t \geqslant t_j; \\ 0, & \text{else.} \end{cases}$$

In addition, d is the offset parameter. $\zeta_j = -t_j \eta_j$ must be adjusted to guarantee that the function is continuous.

For the periodic function, we use the Fourier series to simulate the seasonality component of time series, and can be expressed as follows:

$$s(t) = \sum_{l=-L}^{L} \left(c_l \mathrm{e}^{\mathrm{j}\frac{2\pi l t}{T}} \right) \tag{13}$$

where T represents the regular period and L is the order of the Fourier series, L can be set to a high value and used to improve prediction accuracy. c_l is a coefficient of the Fourier Series that follows a normal distribution with mean 0.

In Eq. (11), the effects of different holidays are independent of each other. The holiday term is defined as follows:

$$h(t) = D(t)\vartheta \tag{14}$$

where $D(t) = [\mathbf{1}, \mathbf{1}, \ldots, \mathbf{1}]$, $t \in D_1, D_2, \ldots, D_z$, represents the list of holidays and ϑ is a prior parameter reflecting the corresponding influence, following the normal distribution.

4.2 A cross-layer cooperative jamming scheme

Considering all cooperative devices in the heterogeneous IoT system with cellular and D2D communications, we embody a transmission rate influence factor. The factor is the weight of physical layer, i.e., $w_{\mathrm{Ph}}^{ij} = R_c^{i*}/R_c^* + R_d^{j*}/R_d^*$, by a normalization process. In this case, we maximize the achievable rate of C_i and D_j while satisfying several constraints. Specifically, for C_i or D_j, we have a similar objective function in the optimization problem, which is expressed as follows:

$$R_c^* = \max_{\Omega, p_d^j} R_c^i, \; R_d^* = \max_{\Omega, p_d^j} R_d^j \tag{15}$$

The optimization problem comes with five constraints:

$$\mathrm{C1}: \quad p_d^j \leqslant p_{\max} \tag{16}$$

$$\mathrm{C2}: \quad \sum_{i=1}^{N_c} \alpha^{ij} \leqslant 1 \tag{17}$$

$$\mathrm{C3}: \quad \sum_{j=1}^{N_d} \alpha^{ij} \leqslant 1 \tag{18}$$

$$\mathrm{C4}: \quad R_c^i \geqslant R_{\mathrm{cth}} \tag{19}$$

$$\mathrm{C5}: \quad R_d^j \geqslant R_{\mathrm{dth}} \tag{20}$$

where C1 specifies the transmission power constraint. C2 and C3 indicate that each cellular device can be only selected at most one D2D pair and each D2D pair can reuse the spectrum resource from at most one cellular device. C4 and C5 guarantee the performance requirements of cellular links and D2D links, respectively. Note that R_{cth} denotes the minimum secrecy rate threshold for cellular devices and R_{dth} denotes the minimum data rate threshold of D2D

communications. Then, we introduce two lemmas to compute the optimal value of R_c^i and R_d^j.

Lemma 1 For the achievable secrecy rate in Eq. (7), we define the following equations:

$$A = |h_{\mathrm{ce}}^i|^2|h_{\mathrm{db}}^j|^2 - |h_{\mathrm{cb}}^i|^2|h_{\mathrm{de}}^j|^2,$$
$$B = (|h_{\mathrm{ce}}^i|^2 - |h_{\mathrm{cb}}^i|^2)\sigma^2,$$
$$C = \sigma^2\left(\frac{|h_{\mathrm{ce}}^i|^2(p_c^i|h_{\mathrm{cb}}^i|^2+\sigma^2)}{|h_{\mathrm{db}}^j|^2} - \frac{|h_{\mathrm{cb}}^i|^2(p_c^i|h_{\mathrm{ce}}^i|^2+\sigma^2)}{|h_{\mathrm{de}}^j|^2}\right),$$

where the related discriminant is $\Delta = 4(B^2 - AC)$. The optimal solution of transmission power for Eq. (7), p_d^{j*}, in different cases is as follows:

- When $A < 0$ and $\Delta > 0$,

$$p_d^{j*} = \begin{cases} p_{\min}, & \text{when } 0 < p_1 \leqslant p_{\min}; \\ p_1, & \text{when } p_{\min} < p_1 \leqslant p_{\max}; \\ p_{\max}, & \text{when } p_1 > p_{\max}, \end{cases}$$

where

$$p_{\min} = \frac{(2^{R_{\mathrm{dth}}}-1)(p_c^i|h_{\mathrm{cd}}|^2+\sigma^2)}{|h_{\mathrm{dd}}|^2},\ p_1 = \frac{-2B-\sqrt{\Delta}}{2A}.$$

- When $A = 0$ and $B \geqslant 0$, or $A > 0$ and $\Delta \leqslant 0$, $p_d^{j*} = 0$.
- In other cases, $p_d^{j*} = p_{\min}$.

Then, we can obtain the maximum achievable rate $R_c^* = \max_j R_c^{i*}$.

Proof See Appendix A. ■

Lemma 2 In the constraint of C4, the equation $R_c^i = R_{\mathrm{cth}}$ has 0, 1 (p_a), or 2 ($p_a > p_b$) positive solutions. If zero solutions exist or $p_b > p_{\max}$, $p_d^{j*} = 0$. In other cases, $p_d^{j*} = \min(p_{\max}, p_a)$. Thus, we can obtain $R_d^* = \max_i R_d^{j*}$.

Proof See Appendix B. ■

According to Lemmas 1 and 2, we construct an evaluation framework with coupling of social relationships and physical entities, and take $\omega_{\mathrm{Ph}}^{ij}$ and $\omega_{\mathrm{So}}^{ij}$ as two performance indices. In general, we should select D2D gadgets with close social relationships with cellular devices and excellent cooperative jamming capabilities as possible. Consequently, our objective is to maximize the social-physical utility with respect to the binary matching variables Ω, while guaranteeing the requirements of cellular devices and D2D gadgets. The whole optimization problem can be formulated as follows:

$$\max_{\Omega} \quad \sum_{i=1}^{N_c}\sum_{j=1}^{N_d}\alpha^{ij}(\omega_{\mathrm{Ph}}^{ij}+\omega_{\mathrm{So}}^{ij}),$$
$$\text{s.t.} \quad \text{C1—C5} \tag{21}$$

Next, we propose a social property-based cooperative jamming algorithm to solve Eq. (21). Based on the social relationships sorted in descending order, we develop a social group $\mathcal{U}$ to further satisfy requirements of the physical layer. $\mathcal{U}$ is composed of N' D2D gadgets with the highest intimacy degree. In this way, we do not need to traverse all devices to calculate the social-physical utility. Then, we can temporarily match each cellular device C_i with each D2D pair D_j, i.e., $\alpha^{ij} = 1$, to obtain the corresponding social-physical utility. The utility is the weight for all possible matching between cellular devices and D2D gadgets $u_{\mathrm{cd}}^{ij} = \omega_{\mathrm{Ph}}^{ij} + \omega_{\mathrm{So}}^{ij}$. The implementation detail of the proposed algorithm is described in Algorithm 1.

The entire problem involves the spectrum resource allocation belonging to the domain in application of matching theory, and can be modeled as the optimal two-dimensional matching problem of the weighted bipartite graph. Cellular devices and D2D gadgets are disjoint sets of vertices and the set of weights is defined as $\mathcal{W} = \{u_{\mathrm{cd}}^{ij}\}$. We aim to find a matching result to optimize the sum of $\mathcal{W}$ based on graph theory. An equality subgraph is defined as a graph where the sum of labeling is equal to the weight u_{cd}^{ij}. The neighbor of a vertex is defined as a set of all vertices adjacent to the vertex. An augmenting path starts and ends at unmatched points and alternately

Algorithm 1 Social properties-based cooperative jamming

Input: N_d, N_c, $|h_{uv}^w|^2$, p_c^i, $p_{\max}$, R_{cth}, R_{dth}, σ^2
Output: Ω, p_d^j

```
Calculate the value of social intimacy in Subsection 4.1
Sort social intimacy ω_So^ij in descending order
Choose N̄ D2D gadgets with the highest social intimacy to join in the social group U
Calculate the number of devices N' in U
for i ∈ 1 to N_c do
    for j ∈ 1 to N' do
        Initialize the matching indicator as α^ij = 1
        Calculate the weight u_cd^ij of C_i and D_j with the optimization of transmission power p_d^j according to Lemmas 1 and 2
    end for
end for
Utilize Algorithm 2 to obtain the optimal matching Ω
```

passes through unmatched and matched edges. Here, we utilize KM algorithm to obtain the optimal management and control scheme and calculate the total utility. The detail of the KM algorithm is described in Algorithm 2.

5 Performance Analysis and Discussion

In this section, we evaluate and analyze the performance of the proposed cross-layer cooperative jamming scheme for social IoT via numerical simulation. The simulation parameters are summarized in Table 2.

In the simulation, we compare the performance of our scheme with other four schemes. The first one is the socially-blind selection scheme. This scheme considers the weight of physical layer w_{Ph}^{ij}. Second, we exploit the random selection scheme to select a D2D gadget to achieve cooperative jamming, where the D2D gadget randomly reuses cellular spectrum resources. And the last two are the nearest selection and furthest selection schemes. In these two schemes, cellular devices and D2D gadgets with the minimum and maximum distances share the resources.

Algorithm 2 KM algorithm for the optimal scheme

Input: Weight matrix $\mathcal{W}$, N_c, N'
Output: Matching set Ω

Add $|N' - N_c|$ vertices
Set weights of added vertices and original vertices as zero
Initialize Ω as a zero matrix
for $i \in 1$ to N' **do**
  Set the labeling $\xi_c(i) = \max_j(u_{\text{cd}}^{ij})$
end for
for $j \in 1$ to N' **do**
  Set the labeling $\xi_d(j) = 0$
end for
Initialize the equality subgraph ψ
while Ω does not cover all vertices of v_c^i **do**
  Choose a free vertex i in Ω
  Set $S = \{v_c^i\}$, $T = \phi$
  Set the neighbor $N_\xi(S)$ of all vertices in S
  if $N_\xi(S) == T$ **then**
    $d_\xi = \min_{i \in S, j \notin T}\{\xi_c(i) + \xi_d(j) - u_{\text{cd}}^{ij}\}$
    while $v_c^i \in S$ **do**
      $\xi_c(i) = \xi_c(i) - d_\xi$
    end while
    while $v_d^j \in T$ **do**
      $\xi_d(j) = \xi_d(j) + d_\xi$
    end while
  end if
  Choose a vertex $v_d^j \in N_\xi(S) - T$
  if v_d^j is matched by another vertex k **then**
    Set $S = S \cup \{k\}$ and $T = T \cup \{v_d^j\}$
    Go to Line 12
  else
    Find an augmenting path P from v_c^i to v_d^j
    Set $\Omega = \Omega \cup P - \Omega \cap P$
  end if
end while

Table 2 Simulation parameter.

Parameter	Description	Value
R	Maximum cell coverage	100 m
$D_{\max}$	Maximum D2D distance	5 m
α	Path loss factor	4
σ^2	Noise power	10^{-10} W
N_d	Number of D2D gadgets	15
$p_{\max}$	Maximum D2D power	30 dBm
R_{cth}	Threshold for cellular devices	1 bps/Hz
R_{dth}	Threshold for D2D gadgets	1 bps/Hz
N	Number of repeated experiments	100

We first analyze the sum of social-physical utility for different schemes, we set the variable number of cellular devices from 1 to 10, as shown in Fig. 4, the sum utility increases with the increasing number of cellular devices, which indicates that our proposed cross-layer scheme outperforms others. The reason is that our scheme is designed based on the couplings of social relationship in the application layer and physical characteristics of the physical layer. Among the five schemes, the nearest selection scheme has the worst performance. The reason is that D2D gadgets cause the largest interference to cellular devices.

In Fig. 5, we discuss the impact of the number of cellular devices on the sum rate of all cooperative cellular devices and D2D gadgets. The sum rate increases as the number of cellular devices increases. The reason is that one spectrum resource can support additional D2D

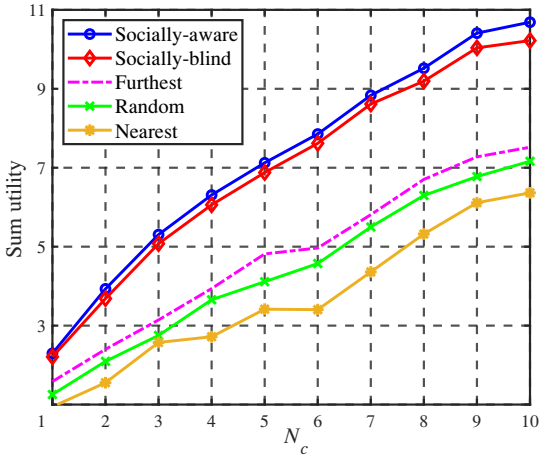

Fig. 4 Influence of the number of cellular users N_c on the sum utility.

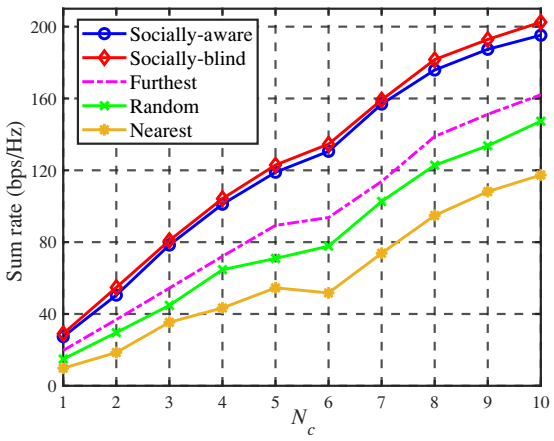

Fig. 5 Effect of the number of cellular users N_c on the sum rate.

and cellular devices to achieve communications. The performance of our scheme is similar to the socially-blind selection scheme in the aspect of the sum rate. This finding illustrates that our scheme can also achieve good performance considering social relationships.

We set the numbers of cellular devices and D2D gadgets to be 5 and 20. The maximum transmission power of D2D gadgets is set as 20 dBm. Figure 6 illustrates that the sum of social-physical utility first increases and then decreases with the increasing transmission power of cellular devices. This finding is attributed to the selection of D2D gadgets with good channel conditions and high transmission power by cellular devices to satisfy the performance requirements. Given the limitations of the maximum transmission power, the role of D2D gadgets to achieve cooperative jamming is limited when the transmission power of cellular devices increases to a definite value. In addition, our proposed scheme achieves better performance than other schemes because spectrum resources are assigned to D2D gadgets optimally.

In Fig. 7, we show the sum rate of the overall network including cooperative cellular devices and D2D gadgets. Increasing the transmission power of cellular devices first increases sum rate and decreases it after exceeding to a certain value. The influence of D2D gadgets also increases initially before decreasing. Moreover, our proposed scheme and the socially-blind scheme achieve similar performances.

6 Conclusion

In this paper, we studied the secure transmission rate in a heterogeneous IoT system with underlaying D2D communications. A cross-layer cooperative jamming scheme was developed by using social relationship mapping from the physical entities to the application layer. In the scheme, we first analyzed the intimacy degree based on the contact history between devices and presented a Prophet model-based prediction method to study probable social relationships in future. Second, we exploited the intimacy to screen and filter potential cooperative devices. Finally, we formulated a maximization problem for the social-physical utility and designed a KM algorithm to find the optimal D2D gadget as a cooperative jammer. In the future, we will investigate how to achieve a feasible secure communication range when considering social relationship in the application layer for the scenario of known statistical CSI in the physical layer.

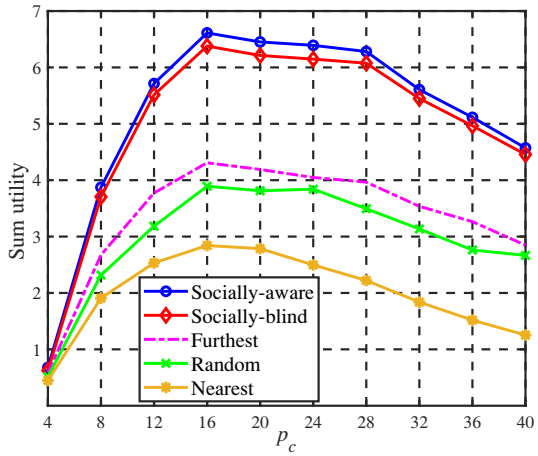

Fig. 6 Effect of the power of cellular users p_c on the sum utility.

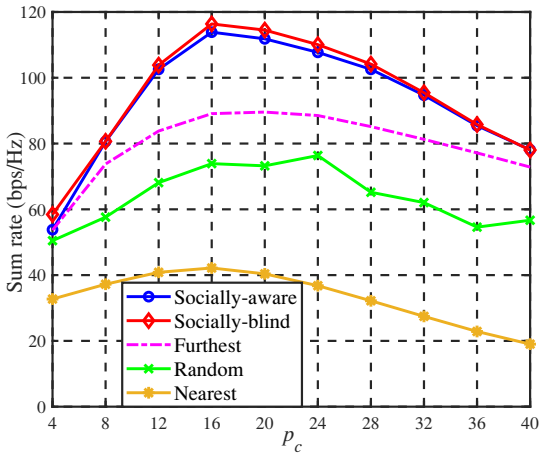

Fig. 7 Effect of the power of cellular users p_c on the sum rate.

Appendix

A Proof of Lemma 1

Under the matching result of C_i and D_j, the derivation of Eq. (7) is given by the following:

$$\frac{\partial R_c^i}{\partial p_d^j} = \frac{A p_d^{j2} + 2Bp_d^j + C}{p_c^i |h_{\mathrm{db}}^j|^2 |h_{\mathrm{de}}^j|^2 I_1 I_2 I_3 I_4} \tag{22}$$

where $I_1 = p_d^j |h_{\mathrm{db}}^j|^2 + p_c^i |h_{\mathrm{cb}}^i|^2 + \sigma^2$, $I_2 = p_d^j |h_{\mathrm{db}}^j|^2 + \sigma^2$, $I_3 = p_d^j |h_{\mathrm{de}}^j|^2 + p_c^i |h_{\mathrm{ce}}^i|^2 + \sigma^2$, and $I_4 = p_d^j |h_{\mathrm{de}}^j|^2 + \sigma^2$. To find the extreme point of Eq. (22), let $\frac{\partial R_c^i}{\partial p_d^j} = 0$, i.e., $A p_d^{j2} + 2Bp_d^j + C = 0$. When $A \neq 0$, the related discriminant is $\Delta = 4(B^2 - AC)$ and the solutions are as follows:

$$p_1 = \frac{-B - \sqrt{B^2 - AC}}{A},\ p_2 = \frac{-B + \sqrt{B^2 - AC}}{A}.$$

Given the constraints of C1 and C5, the value of p_d^j is limited to $[p_{\min}, p_{\max}]$. Here, $p_{\min} = (2^{R_{\mathrm{dth}}} - 1)(p_c^i |h_{\mathrm{cd}}|^2 + \sigma^2)/|h_{\mathrm{dd}}|^2$ is the minimum transmission power to guarantee the rate requirement of D2D links. According to the above analysis, we will discuss different cases as follows:

- Case 1: $A = 0$ and $B \geqslant 0$, or $A > 0$ and $\Delta \leqslant 0$, the cooperation of C_i and D_j will result in a negative secrecy rate $R_c^i < 0$. Therefore, $\alpha^{ij} = 0$ and $p_d^{j*} = 0$.
- Case 2: $A < 0$ and $\Delta > 0$, R_c^i is a unimodal function with a maximum value. Considering the feasible range of p_d^j, we obtain the following:

$$p_d^{j*} = \begin{cases} p_{\min}, & \text{when } 0 < p_1 \leqslant p_{\min}; \\ p_1, & \text{when } p_{\min} < p_1 \leqslant p_{\max}; \\ p_{\max}, & \text{when } p_1 > p_{\max}. \end{cases}$$

- Other cases: we can obtain $p_d^{j*} = p_{\min}$ combined with function trends. Thus, the optimal value is $R_c^* = \max_j R_c^{i*}$.

This completes the proof of Lemma 1.

B Proof of Lemma 2

Intuitively, Eq. (8) monotonically increases with regard to p_d^j. Without loss of generality, we discuss by the following different cases.

- No solution is available in Case 1. The constraint C4 cannot be satisfied. Thus, $p_d^{j*} = 0$.
- One solution (p_a) exists in Case 2. The derivation of Eq. (22) is less than zero. It requires $p_d^j < p_{\max}$. Thus $p_d^{j*} = \min(p_{\max}, p_a)$.
- Two solutions ($p_a > p_b$) exist in Case 3. This condition corresponds to the situation in which R_c^i is a unimodal function. When $p_a \leqslant p_{\max}$, both solutions are less than $p_{\max}$. We consider the large-value $p_d^{j*} = p_a$. When $p_a \geqslant p_{\max}$, it does not meet the restrictive conditions, and thus $p_d^{j*} = 0$. When $p_b < p_{\max} < p_a$, $p_d^{j*} = p_{\max}$. Accordingly, the optimal value is $R_d^* = \max_i R_d^{j*}$.

This completes the proof of Lemma 2.

Acknowledgment

The authors are very grateful to all reviewers who have helped improve the quality of this paper. This work was supported by the National Natural Science Foundation of China (Nos. 61871023 and 61931001) and Beijing Natural Science Foundation (No. 4202054).

References

[1] B. Khalfi, B. Hamdaoui, and M. Guizani, Extracting and exploiting inherent sparsity for efficient IoT support in 5G: Challenges and potential solutions, *IEEE Wireless Communications*, vol. 24, no. 5, pp. 68–73, 2017.

[2] Y. Zhang, B. Wu, Y. Liu, and J. Lv, Local community detection based on network motifs, *Tsinghua Science and Technology*, vol. 24, no. 6, pp. 716–727, 2019.

[3] Z. Cai and X. Zheng, A private and efficient mechanism for data uploading in smart cyber-physical systems, *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.

[4] J. Mao, Y. Zhang, P. Li, T. Li, Q. Wu, and J. Liu, A position-aware merkle tree for dynamic cloud data integrity verification, *Soft Computing*, vol. 21, no. 8, pp. 2151–2164, 2017.

[5] M. Waqas, Y. Niu, Y. Li, M. Ahmed, D. Jin, S. Chen, and Z. Han, Mobility-aware device-to-device communications: Principles, practice and challenges, *IEEE Communications Surveys & Tutorials*, doi：10.1109/COMST.2019.2923708.

[6] X. Zheng and Z. Cai, Privacy-preserved data sharing towards multiple parties in industrial IoTs, *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.

[7] F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, and M. A. Javed, A survey of device-to-device communications: Research issues and challenges, *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2133–2168, 2018.

[8] R. Ansari, C. Chrysostomou, S. A. Hassan, M. Guizani, S. Mumtaz, J. Rodriguez, and J. Rodrigues, 5G D2D networks: Techniques, challenges, and future prospects, *IEEE Systems Journal*, vol. 12, no. 4, pp. 3970–3984, 2018.

[9] X. Xing, T. Jing, W. Cheng, Y. Huo, and X. Cheng, Spectrum prediction in cognitive radio networks, *IEEE Wireless Communications*, vol. 20, no. 2, pp. 90–96, 2013.

[10] J. A. Stine and C. E. C. Bastidas, Enabling spectrum sharing via spectrum consumption models, *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 4, pp. 725–735, 2015.

[11] X. Zheng, Z. Cai, and Y. Li, Data linkage in smart internet of things systems: A consideration from a privacy perspective, *IEEE Communications Magazine*, vol. 56, no. 9, pp. 55–61, 2018.

[12] Z. Cai and Z. He, Trading private range counting over big IoT data, in *Proc. of IEEE 39th International Conference on Distributed Computing Systems*, Dallas, TX, USA, 2019, pp. 144–153.

[13] Y. Jia, Y. Chen, X. Dong, P. Saxena, J. Mao, and Z. Liang, Man-in-the-browser-cache: Persisting https attacks via browser cache poisoning, *Computers & Security*, vol. 55, pp. 62–80, 2015.

[14] Y. Huo, Y. Tian, L. Ma, X. Cheng, and T. Jing, Jamming strategies for physical layer security, *IEEE Wireless Communications*, vol. 25, no. 1, pp. 148–153, 2018.

[15] T. Qiu, B. Chen, A. K. Sangaiah, J. Ma, and R. Huang, A survey of mobile social networks: Applications, social characteristics, and challenges, *IEEE Systems Journal*, vol. 12, no. 4, pp. 3932–3947, 2018.

[16] C. Kong, G. Luo, L. Tian, and X. Cao, Disseminating authorized content via data analysis in opportunistic social networks, *Big Data Mining and Analytics*, vol. 2, no. 1, pp. 12–24, 2019.

[17] J. Mao, W. Tian, Y. Yang, and J. Liu, An efficient social attribute inference scheme based on social links and attribute relevance, *IEEE Access*, vol. 7, pp. 153074–153085, 2019.

[18] 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*, vol. 15, no. 4, pp. 577–590, 2018.

[19] S. J. Taylor and B. Letham, Forecasting at scale, *The American Statistician*, vol. 72, no. 1, pp. 37–45, 2018.

[20] J. S. He, M. Han, S. Ji, T. Du, and Z. Li, Spreading social influence with both positive and negative opinions in online networks, *Big Data Mining and Analytics*, vol. 2, no. 2, pp. 100–117, 2019.

[21] X. Meng, G. Xu, T. Guo, Y. Yang, W. Shen, and K. Zhao, A novel routing method for social delay-tolerant networks, *Tsinghua Science and Technology,* vol. 24, no. 1, pp. 44–51, 2019.

[22] E. Tekin and A. Yener, The general gaussian multipleaccess and two-way wiretap channels: Achievable rates and cooperative jamming, *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[23] Y. Choi and J. H. Lee, A new cooperative jamming technique for a two-hop amplify-and-forward relay network with an eavesdropper, *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12447–12451, 2018.

[24] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, Physical layer network security in the full-duplex relay system, *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 574–583, 2015.

[25] M. Nafea and A. Yener, Secure degrees of freedom for the MIMO wiretap channel with a multi-antenna cooperative jammer, *IEEE Transactions on Information Theory*, vol. 63, no. 11, pp. 7420–7441, 2017.

[26] Q. Gao, Y. Huo, T. Jing, L. Ma, Y. Wen, and X. Xing, An intermittent cooperative jamming strategy for securing energy-constrained networks, *IEEE Transactions on Communications*, vol. 67, no. 11, pp. 7715–7726, 2019.

[27] Z. Chu, H. X. Nguyen, T. A. Le, M. Karamanoglu, E. Ever, and A. Yazici, Secure wireless powered and cooperative jamming D2D communications, *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 1, pp. 1–13, 2018.

[28] Y. Huo, X. Fan, L. Ma, X. Cheng, Z. Tian, and D. Chen, Secure communications in tiered 5G wireless networks with cooperative jamming, *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, pp. 3265–3280, 2019.

[29] T. Shi, Z. Cai, J. Li, and H. Gao, CROSS: A crowdsourcing based sub-servers selection framework in D2D enhanced MEC architecture, in *Proc. of IEEE 40th International Conference on Distributed Computing Systems*, Singapore, 2020, pp. 1–11.

[30] R. Zhang, X. Cheng, and L. Yang, Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks, *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5651–5663, 2016.

[31] H. Wang, B. Zhao, and T. Zheng, Adaptive full-duplex jamming receiver for secure D2D links in random networks, *IEEE Transactions on Communications*, vol. 67, no. 2, pp. 1254–1267, 2019.

[32] Q. Li, P. Ren, Q. Du, D. Xu, and Y. Xie, Safeguarding NOMA enhanced cooperative D2D communications via friendly jamming, in *Proc. of IEEE 90th Vehicular Technology Conference*, Honolulu, HI, USA, 2019, pp. 1–5.

[33] S. Zhu, W. Li, H. Li, L. Tian, G. Luo, and Z. Cai, Coin hopping attack in blockchain-based IoT, *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4614–4626, 2019.

[34] L. Wang, H. Wu, L. Liu, M. Song, and Y. Cheng, Secrecy-oriented partner selection based on social trust in device-to-device communications, in *Proc. of IEEE International Conference on Communications*, London, UK, 2015, pp. 7275–7279.

[35] Y. Wen, Y. Huo, L. Ma, T. Jing, and Q. Gao, A scheme for trustworthy friendly jammer selection in cooperative cognitive radio networks, *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3500–3512, 2019.

[36] H. Wang, Y. Xu, K. Huang, Z. Han, and T. A. Tsiftsis, Cooperative secure transmission by exploiting social ties in random networks, *IEEE Transactions on Communications*, vol. 66, no. 8, pp. 3610–3622, 2018.

[37] Y. Zhao, Y. Li, Y. Cao, T. Jiang, and N. Ge, Social-aware resource allocation for device-to-device communications underlaying cellular networks, *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6621–6634, 2015.

[38] Y. Zhao and W. Song, Energy-aware incentivized data dissemination via wireless D2D communications with weighted social communities, *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 4, pp. 945–957, 2018.

[39] F. Wang, Y. Li, Z. Wang, and Z. Yang, Social-community-aware resource allocation for D2D communications underlaying cellular networks, *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 3628–3640, 2016.

[40] Z. He, Z. Cai, and J. Yu, Latent-data privacy preserving with customized data utility for social network data, *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 665–673, 2018.

[41] X. Zheng, Z. Cai, J. Yu, C. Wang, and Y. Li, Follow but no track: Privacy preserved profile publishing in cyber-physical social systems, *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1868–1878, 2017.

[42] J. Wang, Z. Cai, and J. Yu, Achieving personalized k-anonymity-based content privacy for autonomous vehicles in CPS, *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4242–4251, 2020.

[43] C. Yi, S. Huang, and J. Cai, An incentive mechanism integrating joint power, channel and link management for social-aware D2D content sharing and proactive caching, *IEEE Transactions on Mobile Computing*, vol. 17, no. 4, pp. 789–802, 2018.

[44] D. Wu, L. Zhou, Y. Cai, H. Chao, and Y. Qian, Physical-social-aware D2D content sharing networks: A provider-demander matching game, *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7538–7549, 2018.

[45] Y. Sun, T. Wang, L. Song, and Z. Han, Efficient resource allocation for mobile social networks in D2D communication underlaying cellular networks, in *Proc. of IEEE International Conference on Communications*, Sydney, Australia, 2014, pp. 2466–2471.

[46] M. Alwakeel and V. A. Aalo, A teletraffic performance study of mobile LEO-satellite cellular networks with Gamma distributed call duration, *IEEE Transactions on Vehicular Technology*, vol. 55, no. 2, pp. 583–596, 2006.

[47] H. Zhang, Z. Wang, and Q. Du, Social-aware D2D relay networks for stability enhancement: An optimal stopping approach, *IEEE Transactions on Vehicular Technology*, vol. 67, no. 9, pp. 8860–8874, 2018.

Yan Huo received the BEng and PhD degrees in communication and information system from Beijing Jiaotong University, Beijing, China in 2004 and 2009, respectively. He has been a faculty member at the School of Electronics and Information Engineering, Beijing Jiaotong University since 2011, where he is currently a professor. His current research interests include wireless communication theory, security and privacy, cognitive radio, and signal processing. He is a senior member of IEEE.

Ruinian Li received the PhD degree in computer science from the George Washington University in 2018. He is currently an assistant professor at the Department of Computer Science, Bowling Green State University (BGSU), USA. His research interests include security and privacy-preserving computations, applied cryptography, and blockchain technology. He has been working in a wide area of social networks, auction systems, and IoT, and his work has been published in top-tier journals, such as *IEEE Transactions on Services Computing*, and *IEEE Transactions on Network Science and Engineering*.

Jingjing Fan received the BEng degree from Beijing Jiaotong University, Beijing, China in 2018. She is currently a master student in Beijing Jiaotong University. Her research interests include wireless networks, social networks, and physical layer security.

Yingkun Wen received the BS degree from North China Electric Power University, Baoding, China in 2015. He is currently pursuing the PhD degree in the School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China. His current research interests include cognitive radio networks, physical layer security, and cooperative communication.