**QUEEN'S
UNIVERSITY
BELFAST**

Security Enhanced Content Sharing in Social IoT: A Directed Hypergraph-based Learning Scheme

Wang, B., Sun, Y., Duong, T. Q., Nguyen, L. D., & Zhao, N. (2020). Security Enhanced Content Sharing in Social IoT: A Directed Hypergraph-based Learning Scheme. *IEEE Transactions on Vehicular Technology*, 4412 - 4425. <https://doi.org/10.1109/TVT.2020.2975884>

Published in:
IEEE Transactions on Vehicular Technology

Document Version:
Peer reviewed version

Queen's University Belfast - Research Portal:
[Link to publication record in Queen's University Belfast Research Portal](#)

Publisher rights
© 2020 IEEE.

This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

General rights

Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Security Enhanced Content Sharing in Social IoT: A Directed Hypergraph-based Learning Scheme

Bowen Wang, Yanjing Sun, *Member, IEEE*, Trung Q. Duong, *Senior Member, IEEE*, Long D. Nguyen, Nan Zhao, *Senior Member, IEEE*

Abstract—Security is a critical element to the existing Internet of Things (IoT) deployment, where any user may actively or passively attack the content sharing of others reusing the same channel. As most smart devices are carried by human, we may leverage their owners’ social trust to avoid being intercepted by untrusted users, which conforms to the Social Internet of Things (SIoT) paradigm. In this paper, we propose a secure content sharing (SCS) scheme to strike the trade-off between security and quality of experience (QoE) by exploring the social trust. Firstly, to dynamically extract the social trust, the random walk strategy is employed for prediction based on the proposed “User-Content-Social Group” graph which models users’ preference over time. Given the social trust value, we propose a hierarchical game model to decouple the optimization problem into two sub-problems: user pairing and channel selection. More specifically, the user pairing sub-problem is formulated as a matching sub-game with peer effect, and the embedded rotation-swap matching algorithm can accommodate the dynamics caused by mutual interference. The second sub-problem can be formulated as a secure channel selection sub-game with the directed hypergraph being game space, which is proved to be an exact potential game. Then, we design an uncoupled-user concurrent learning algorithm (UUCL) to search for the optimal pure Nash equilibrium, and thereby the global optimum of this sub-game is achieved. Finally, simulation results generated on realistic social dataset verify that our proposed scheme can notably enhance the security without sacrificing users’ QoE.

Index Terms—Social Internet of Things, directed hypergraph, game theory, machine learning.

I. INTRODUCTION

WITH the densification of 5G network architecture, Internet of Things (IoT) can potentially revolutionize human life by leveraging the heterogeneity and pervasiveness of smart devices. However, it is challenging to design efficient schemes to meet the application demands given such an enormous quantity of data generated on information exchange.

Copyright (c) 2015 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org. This work was supported in part by Key Research & Development Project for Science and Technology of Xuzhou, China (KC18105), the National Natural Science Foundation of China (51734009, 61771417, 51804304, 61871065).

Bowen Wang and Yanjing Sun are with the School of Information and Control Engineering, China University of Mining and Technology, Xuzhou, 221116, China (e-mails: {bowenwang, yjsun}@cumt.edu.cn).

Bowen Wang and Trung Q. Duong are with the School of Electronics, Electrical Engineering and Computer Science, Queen’s University, Belfast, BT7 1NN, UK (e-mail: trung.q.duong@qub.ac.uk).

Nan Zhao is with the School of Information and Communication Engineering, Dalian University of Technology, Dalian, 116024, China (e-mail: zhaonan@dlut.edu.cn).

Long D. Nguyen is with the Duy Tan University, Vietnam (e-mail: dinh-longhcmut@gmail.com).

For the purpose of getting more attention, mobile users (MUs) are more likely to share their first-hand information in social platforms such as Facebook, Sina weibo, etc. Based on this phenomenon, we may investigate the feasibility of exploring the owners’ behaviour in social platforms to improve the performance of content sharing, since most smart devices in IoT are being carried by humans most of the day. Therefore, many researchers have investigated how to incorporate social attributes such as interest, trustworthiness, interaction history into IoT [1], [2]. In [1], the so-called Social Internet of Things (SIoT) is defined as a “Social Collaborative Internet of Things”, in which smart objects can establish social ties and share information socially with their surrounding devices. The authors in [2] demonstrated that the SIoT has advantages in many aspects, such as scalable network management, efficient information exchange, and stable network architecture.

As one of the promising technologies in the future 5G cellular networks, device-to-device (D2D) communication is naturally applicable to the content sharing in SIoT, where the content requester (CR) can directly download their favorite content from content helper (CH) in the close proximity instead of from the base station (BS). Caching on device level can avoid an enormous amount of retransmission, and thus mitigating the overload of BS [3]. In general, D2D users can share licensed spectrum resource in two modes: overlay mode and underlay mode. The overlay mode allows D2D users to transmit data via dedicated spectrum resources without co-channel interferences, and thus improving the throughput. D2D users can also reuse the cellular spectrum in underlay mode, which improves the efficiency of spectrum sharing [4]. Considering the intrinsic broadcast nature in spectrum sharing, the D2D links are highly vulnerable to various security attacks. Any user sharing the same spectrum may act as a potential eavesdropper or jammer, passively or actively attacking others’ content sharing. Since user privacy is of paramount importance, establishing secure communication links among legitimate devices has a higher priority than improving the spectrum efficiency. In this regard, D2D communication along may not be the best choice despite the aforementioned benefits [5].

To combat with various security attacks, such as jamming, eavesdropping, and data falsification attack, some effective physical layer security methods such as artificial-noise-aided security, and secret-key generation have drawn enormous attention [6], [7]. As a valid method, the information-theoretic physical layer security can maximize the reliable communication rate between two legitimate devices while ensuring that

unauthorized users may learn as little information as possible [8]. However, this method ensures secure transmission in the physical layer at the cost of decreasing effective transmission rate, since all users are assumed to be not trustworthy [9], [10]. Therefore, it is challenging to strike the trade-off between security and spectrum efficiency.

Motivated by the aforementioned problems, we aim at leveraging social trust extracted in the social domain to enhance the security of content sharing without sacrificing the spectrum efficiency in the physical domain. Assumed that non-trusted users belong to the eavesdropper category, if users only share contents and spectrum with their trusted users, the number of potential eavesdroppers and jammers will be certainly reduced, which enhances the security of content sharing [11]. In order to understand the impact of social trust on the security of transmissions, the authors in [10] provided theoretical and numerical analysis of the system ergodic rate of social trust aided communications via stochastic geometry, and they showed a 63% increase in system ergodic rate by considering social trust relation. In [11], the authors stated that users at home or office can generally find friendly users in their close proximity, and thus they can share resources with their socially trusted users for communication with confidence. In some large public places such as stadiums, super markets, and airports etc., where the socially trusted users are rare, users can still share spectrum with non-trusted users. The non-trusted users are also considered to belong to the eavesdropper category [10], [11]. Both of the two studies verified the feasibility of exploiting social relationships to improve transmission security. Hence, the authors in [10], [11] utilized socially-aware paradigm to identify trusted and non-trusted users based on the social relationship/ties strength. In [12], the authors analysed the secure capacity for large-scale networks considering social relationships. In [13], the social reciprocity and social trust was adopted to improve the security by jamming the transmission of eavesdroppers. However, all of these works assumed that the social trust value was a binary variable to determine whether or not the trust exists, and thus the dynamics and strength of social relationships were ignored.

Inspired by the above mentioned works, we propose a security enhanced content sharing scheme to achieve a trade-off between security and quality of experience (QoE). There are two key challenges requiring investigation in order that we can explore social trust to improve the security of content sharing, namely, accurately extracting the social trust and utilizing the extracted social trust to improve the security of content sharing with the guarantee of QoE. The first one is to accurately extract the dynamic social attributes over time, because the inaccurate information will affect users' decision-making, and thus the established link will be unreliable. The second one is to efficiently employ social trust to design secure content sharing scheme in SIoT, because the social trust can help to identify trusted and non-trusted nodes, and further provide information confidentiality to all the system entities [11]. For the first problem, we aim to propose an efficient scheme to predict users' preference and behavior based on the user interaction history from the realistic dataset. For the second problem, we model the asymmetric and cumulative

interference effects with the framework of directed hypergraph. Based on this model, we propose a directed-hypergraph learning scheme to achieve the secure content sharing with rapid speed of convergence.

Our contributions are summarized as follows:

- *Modeling*: We design a novel framework by exploring the inter-human social trust to enhance the security of content sharing in the physical domain. Specifically, the proposed scheme comprehensively solves the proactive caching, user pairing, and dynamic spectrum sharing problems with the security guarantee. To the best of our knowledge, this is the first work to apply the social attributes extracted from realistic dataset to enhance the security of content sharing.
- *Social Trust*: We design a novel scheme to predict the potential probability of successfully requesting contents as sharing willingness based on the "User-Content-Social Group" tripartite graph which models users' varying preferences over time. And we further model the social trust as a probability by considering extracted interaction probability, reciprocal probability, and sharing willingness.
- *Secure Content Sharing (SCS) Algorithm*: We investigate the secure channel selection and user pairing sub-problems in SCS, aiming at trading off both the security and QoE. Considering the interaction caused by dynamics, we propose a hierarchical game model. Based on this model, the user pairing sub-problem is formulated as a one-to-one matching sub-game with peer effect, and the embedded rotation-swap matching algorithm can smoothen out the instability caused by competition behaviors. In addition, we depict the security enhanced channel selection sub-problem with the framework of directed hypergraph, and thus formulate it as a secure channel selection sub-game. Then, an uncoupled-user concurrent learning (UUCL) scheme is adopted to achieve the global optimum of the formulated game.
- *Validations*: We comprehensively prove the optimality, stability, convergence, and complexity properties of our proposed scheme. Under various scenarios, simulation results tested on realistic social dataset demonstrate the superiority of our proposed scheme compared with existing methods.

The rest of this paper is outlined as follows. The related work is given in Section II. The architecture for security enhanced SIoT scenario is presented and then the optimization problem is elaborated in Section III. The directed hypergraph-based learning scheme is described in Section IV. Simulation results tested on realistic dataset are provided in Section V, followed by conclusion in Section VI. Some key notations are listed in Table I.

II. RELATED WORKS

Establishing secure D2D link between two legitimate devices on D2D underlay mode, has gained extensive attention from academia and industry [14]. Physical layer security methods can guarantee both the reliability and efficiency of

TABLE I: LIST OF KEY NOTATIONS

CH, CR, CU	The set of CHs, CRs and CUs
F, L_f, Q	The set of all the content items and file size
$R_{i,j}, R_m$	The achievable data rate from CH to CR and CU to BS
$I_{i,j}, r_{b_{i,j}}, P_{i,j}^*, \varpi_{ij}$	The social contact intensity, reciprocal interval, share willingness, and social trust probability
$x_{i,j}, y_{i,j}, b_{i,j}$	The binary variable in incidence matrix, interference state, and user pairing
Ω	The user pairing matching function
$A_i, q_i^{a_i}$	The channel selection profile and channel selection probability
$U_i(a_i, -a_i), C_i(a_i, -a_i), \Phi(a_i, -a_i)$	The utility function, normalized secure content sharing capacity, and potential function

transmission between two legitimate users [8]. However, the assumption that there is no trustworthiness between two users is not practical. Inevitably, users belonging to different social communities must have varying levels of social trust with each other, which intuitively has impact on security. Some studies have leveraged social relationship to solve the physical layer security problems. The so-called social ties are considered to reflect the willingness to share information or resources. Recently, some studies have applied social ties into securing content sharing or information transmission [10], [11], [15], [16]. The authors in [15] designed a coding scheme that not only satisfied the user demands but also the secure D2D communication. In [16], assuming that the relay user with lower social trust degree will act as a potential eavesdropper, the authors proposed a cooperative transmission method with social trust-aided relay selection. In [10], the authors analyzed the theoretical bound of the social trust-aware D2D communication framework using stochastic geometry, and solved the corresponding resource allocation problem using matching theory. In [11], the authors utilized socially-aware paradigm to identify trusted and non-trusted users, and proposed an approach based on coalitional game to ensure secrecy. These studies partly address this issue, but the randomly generated social tie with binary value, where 1 and 0 represent trust and non-trust relationship respectively, cannot reflect the dynamics of social trust. Besides, when the physical or social condition varies over time, the preference will change frequently, which degrades the presented effectiveness in [10], [11]. To better capture social trust, we need to model the social trust as a probability.

As mentioned before, the performance of content sharing is influenced not only by objective factor i.e., physical condition, but also by subjective factor, i.e., user preference [17]. Considering that the storage capacity is limited on device level, it is challenging to pre-cache the needed contents on a certain CH. Meanwhile, willingness to share is also critical. If a CH is not interested in the requested contents or has no social trust with this CR, he is not willing to cache and share it at the cost of storage capacity and energy [18]. In this case, BS still needs to retransmit the content if the content request fails. The authors in [19] proposed a social-aware caching strategy to optimize the hit ratio, where the important users can adaptively change the caching strategy based on neighbors' feedback. However, the social attributes such as their interest similarity were assumed to be unchanged. Considering the varying preferences caused by different external events, accurately capturing preferences on different contents over time is a great practical challenge in content sharing [20]. The authors in

[21] proposed a session-based graph model to predict users' long-term and short-term preference for different items. In practice, current users will also be influenced by their friends in a social network, and the social relationship also changes with interest varying over time. In [22], the authors adopted an unbiased random walk strategy to recommend unknown items by exploiting friendship. However, more comprehensive social attributes should be considered to evaluate the social relationship, for the purpose of improving the hit ratio of recommendation.

Many mathematical tools such as game theory, graph theory, and matching theory have been regarded as efficient resource allocation methods [23]–[25]. Most of the previous works applied traditional binary graph to model the pair-wise strong interference [26]. However, the complex interference relationship cannot be accurately modeled when considering the heterogeneity and densification of user devices. To get around this limitation, the authors in [27] adopted hypergraph model to abstract the complicated interference relationship for D2D underlay communications as hyperedge, and proposed an channel allocation algorithm based on coloring. Upon this model, the authors in [28] formulated the channel allocation problem as a local altruistic game, which belongs to the exact potential game. Furthermore, the same authors utilized advanced directed hypergraph to model the asymmetric interference relationships in [29]. However, the security is ignored when constructing the hypergraph interference model and formulating the corresponding game model. In addition, the user pairing is also omitted for simplicity. Many classical matching game models can be used to formulate the distributed resource allocation or user pairing problems. Our previous work in [30] proposed a rotation-swap matching algorithm, which can handle the dynamically changing co-channel interference in resource allocation problem. However, the effectiveness and convergence will be degraded when considering the dynamics of social attributes.

Based on the discussion above, the existing literature mainly suffers from the following problems. Firstly, the social trust value is dynamically changing instead of remaining unchanged over time, which was not considered in [10], [11], [15], [16]. Secondly, the social relationship prediction models in [21], [22] only considered the single attribute to evaluate the social relationships, which limits accuracy of prediction. Finally, the existing hypergraph based resource allocation methods in [27]–[30] did not consider the impact of social tie on users' content sharing behavior in user pairing problem or the effectiveness and convergence will be degraded when considering the dynamics of social attributes.

Fig. 1: Architecture for the security-enhanced content sharing in SIoT

In this paper, we formulate the user pairing problem as a one-to-one matching sub-game with peer effect, and the rotation-swap matching algorithm can be adopted for further secure transmissions. Besides, we propose a directed hypergraph-based learning algorithm to solve the secure channel selection sub-problem. The differences and new contributions in this work are: 1) For the trust model, our previous work [30] only considered the static social relationships including social similarity, social centrality, and the social contact intensity, which belongs to the category of cooperative behavior. Different from [30], we consider a more comprehensive and accurate social trust model including both cooperative behavior and reciprocal behavior. Besides, we consider that the social trust dynamically changes over time and all the social attributes are extracted from the realistic social dataset for practical purpose. 2) For the user pairing problem, different from [30], we solve the formulated one-to-one matching with externality rather than the many-to-one matching. Since this problem is not our main focus in this paper, we slightly modify the proposed method in [30] to adapt to the matching rule in our model. 3) For the directed hypergraph based learning scheme, the former works [27], [29] considered the mutual interference in physical domain for the hyperedge construction, but our work consider both the mutual interference in physical domain and information in social domain. Overall, we intend to make a simple combination of game theory and learning, with the directed hypergraph as game space. Following this idea, we propose a hierarchical game model to harness the interplay between the channel selection sub-problem and user pairing sub-problem, which is not considered in the former works.

III. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig.1, we consider a cross-layered SIoT architecture consisting of a BS, and a number of MUs containing N D2D users and M cellular users (CUs). Each D2D pair consists of a CH and a CR. Let us denote by $CU = \{c_1, \dots, c_m, \dots, c_M\}$ the set of CUs, by $CH = \{h_1, \dots, h_i, \dots, h_N\}$ the set of CHs, and by $CR = \{r_1, \dots, r_j, \dots, r_N\}$ the set of CRs. In such a D2D underlay scenario, one CH may share their cached popular contents with one CR who has high level of social trust with them, and meanwhile share cellular spectrum with other CHs, for traffic offload. We assume that the CRs prefer requesting contents from adjacent CHs via D2D communications rather than from the BS, unless the failure. In practice, most users may not consume their limited storage capacity to pre-cache some contents for other users, unless they are also interested in the requested contents. Therefore, the CRs can request desired contents based on potential sharing willingness. In addition, the secure content sharing is also important since users are increasingly concerned about privacy issues. For example, in Fig.1, the D2D pair *BoB-Julia*, *Alice-Tom* and the CU *Bowen* have no social tie with each other, all of them will worry about the other's eavesdropping and jamming when sharing the same channel. To solve it, a directed hypergraph-based learning scheme is proposed to let users share contents in a self-organizing manner. We first provide some preliminaries and assumptions in both physical and social domains.

A. Transmission Model

As mentioned before, we consider the D2D underlaying cellular networks, where a set of M channels allocated to M CUs are available to all D2D users. Let F denote the complete file library, $F = \{f_1, \dots, f_l, \dots, f_L\}$. In this paper, we mainly focus on the video content sharing. We assume that each video has the unequal size denoted by L_f . Different from previous work in [30], the popularity distribution is assumed to be dynamically changing with the users' preference in a certain period, which will be elaborated in the next subsection. We further assume that each user has different storage capacity, which is an important metric to select CHs.

As assumed in [10], the channel gain following Rayleigh distribution is given by $h_{ij} = d_{ij}^{-\alpha} \cdot h_0$, where d_{ij} represents the distance between the CH h_i and CR r_j , α and h_0 represent the path-loss exponent and Gaussian channel coefficient, respectively. Based on this assumption, the transmission rate between h_i and r_j is given by

$$R_{i,j} = B \log_2 \left(1 + \frac{P_i h_{i,j}}{\sum_{i' \in D_m} P_{i'} h_{i',j} + P_m h_{m,j} + N_0} \right), \quad (1)$$

where D_m represents the D2D pairs sharing the c_m 's spectrum, B denotes the transmission bandwidth block, P_i and P_m denote the transmit power for h_i and c_m , and N_0 represents the power spectral density of additive white Gaussian noise. Similarly, the uplink transmission rate of c_m can be given by

$$R_m = B \log_2 \left(1 + \frac{P_m h_{m,b}}{\sum_{i \in D_m} P_i h_{i,b} + N_0} \right). \quad (2)$$

In general, the QoE evaluation for multimedia applications is determined by end users' perception. Inspired by the QoE evaluation method in [31], we adopt the Mean Opinion Score (MOS) method to evaluate the quality of content sharing, which incorporates the sender bitrate, packet loss probability, and frame rate. Adopted from [31], the modified MOS is defined as

$$MOS_{i,j} = \begin{cases} \frac{c_1 + c_2 FR + c_2 \ln(R_{i,j})}{1 + c_4 DP + c_5 DP^2}, & \text{if } h_i \text{ shares content to } r_j; \\ 0, & \text{otherwise,} \end{cases} \quad (3)$$

where FR and $R_{i,j}$ is the frame rate and sender bit rate, respectively, and DP is the packet loss probability.

B. Trust Model

In this subsection, we assume that the social trust value is determined by both cooperative behavior and reciprocal behavior. The cooperative behavior consists of social contact and sharing willingness. Since the sharing willingness is influenced by the other two metrics, we introduce these three metrics step by step.

1) Social Contact

The frequent communication between two users may generate a lot of contact history information, implying a close social relationship. The contact intensity can be measured by multiple metrics such as the contact frequency and duration, i.e., how many interactions happen among them and how long each interaction lasts during a certain period. Similar to [32], we adopt the frequency/duration of interacts which occur in content sharing to measure the recent closeness degree. Here, the user set containing CU, CH, and CR is denoted by $U = \{u_1, u_2, \dots, u_V\}$, where $|V| = |M| + |2N|$. Given a time span T , the average interaction duration between two users can be normalized as

$$\bar{\delta}_{i,j} = \frac{\sum_{x=1}^{N_{i,j}^c} t_x^d}{N_{i,j}^c}, \quad (4)$$

where $N_{i,j}^c$ denotes the sum contact times between user i and user j , and t_x^d is the contact duration. For practical purpose, we normalize the intensity degree of all contacts based on the realistic social dataset.

By following the Gaussian similarity function in [32], the normalized interaction strength can be given by

$$I_{i,j} = e^{-\bar{\delta}_{i,j}^2 / 2\sigma^2}, \quad (5)$$

where σ denotes the width of the Gaussian kernel. The $I_{i,j}$ also denotes the probability of interaction.

2) Reciprocal Behavior

Reciprocal behavior represents the mutual aid behaviors among users, which can be categorized into direct reciprocity and indirect reciprocity. The former one can be easy to understand as the concept of "you help me while I help you". The latter one reflects the circular behavior, which can be defined as "I help you, you help him, and finally he helps me". In this paper, we can analyse the reciprocal behavior based on the content sharing history. If user i shares contents

Fig. 2: "User-Content-Social Group" tripartite graph

with user j , we depict an arrow line from i to j and thus we can obtain a directed graph. The reciprocity behaviour can be formulated as finding the directed circle in this graph [13]. The contribution of i to user i can be measured through the interaction duration in reciprocity behaviour. Similar to [32], the reciprocal probability can be normalized as

$$rb_{i,j} = \frac{\int_0^T rc_{ij}(t)dt}{\int_0^T rc_{ij}(t)dt + \int_0^T rc_{ji}(t)dt}, \quad (6)$$

where $rc_{ij}(t)$ determines whether or not user i and user j are in the same reciprocity circle at time t , and $\int_0^T rc_{ij}(t)dt$ represents the sum contribution of i to user i . $rc_{ij}(t) = 1$ means that user i directly or indirectly helps user j at time t . Note that the authors in [32] only considered the direct reciprocity, while we consider both direct reciprocity and the indirect reciprocity.

3) Share Willingness

Now, we will solve the aforementioned challenging problem: how to predict the users' preference and sharing willingness based on the social history contact. The potential cache list for u_v is defined as a triple of $\langle f_l, p_l^v, rh_l^v \rangle$, where f_l represents a content, p_l^v indicates the potential probability that u_v caches or requests the f_l in the future, and rh_l^v represents whether f_l was received by u_v in the receive history. To get the potential value, we first construct a user-content-social group tripartite graph $G_t = (U, F, SG, E)$ as shown in Fig.2, where U , F , and SG represent the user set, content set, and social group set, respectively. E denotes the edge set and an edge represents that a user belongs to a group or a user has cached a content.

In this figure, we can see that user u_1 cached f_1 , u_2 cached f_1 and f_2 , and u_v cached f_2 and f_L . Although there is no direct connection between u_1 and f_2 , they could be connected by the path $u_1 \rightarrow f_1 \rightarrow u_2 \rightarrow f_2$. That implies u_1 might have the interest in requesting f_2 in the future. Different from the the user-content bipartite graph in [18], we further consider the recommendation of social group. Intuitively, most users' preference will be influenced by their friends or colleagues. u_1 will be interested in f_2 if his friends recommend it in the path $u_1 \rightarrow SG(u_1) \rightarrow f_2$. The higher strength of relationship may provide the more reliable recommendation. In [33], the authors selected the users with higher degree of collaboration than the average degree of collaboration as the recommending users. Inspired by this work, we select the users whose both interaction interval and the reciprocal interval are greater than

the average degree of interval between user i and other users. The social group of u_i is given by

$$SG(u_i) = \{u_j \in U | rb_{i,j} \geq \bar{r}b_i \text{ \& } I_{i,j} \geq \bar{I}_i\}. \quad (7)$$

Obviously, the social group members for one user will change over time. The likelihood of caching/requesting these videos will be represented by the potential probability. In this paper, we adopt the random walk strategy to predict the potential probability. In short, the random walk process can be deemed to a finite and discrete Markov chain. Randomly choosing a start point in a graph model, it can move to arbitrary neighbor nodes. Similar in [22], we set users as source nodes since the content recommendation is a user-centered strategy. The edge weights for different walk are as follows:

$$\omega(v, v') = \begin{cases} P_{v,v'}, & v \in U \cup SG, v' \in U \cup C \cup SG; \\ \beta \cdot P_{v,v'}, & v \in C, v' \in U; \\ (1 - \beta) \cdot P_{v,v'}, & v \in C, v' \in SG, \end{cases} \quad (8)$$

where β denotes the probability of jumping to user node in the next step, while $1 - \beta$ denotes the probability of selecting social group node.

The random walk probability $P_{v,v'}$ is given by

$$P_{v,v'} = \begin{cases} \frac{1}{out(v)} \min\{1, \frac{out(v')}{out(v)}\}, & \text{if } v' \text{ is } v\text{'s neighbor;} \\ 1 - \sum_{v'' \neq v} P_{v,v''}, & \text{if } v' = v, \end{cases} \quad (9)$$

where $out(v)$ is the out degree of vertex v . Similar to [21], we define four types of shortest paths starting from source node v_0 to unknown content node v_n within three steps to reduce the complexity. From the intuitive point of view of graph structure, the distance from user/social group nodes to unknown content nodes should be odd numbers equal to or larger than 3. For a user and an unknown content, there will be many paths with distance equaling to at least 3 between these two nodes in the graph. But we only consider the shortest paths to measure the users' preferences on the content for two reasons: 1) short paths contribute more weights than long paths to the final content nodes and may even bring in noise; 2) the shortest paths can be obtained effectively by random walk algorithm [21], [22].

- User-Content-User-Content (P1): The source user node first randomly walks to one of his cached contents, and finally explores the unknown content through other users who has cached the content.
- User-Content-Social Group-Content (P2): The source user node first randomly walks to one of his cached contents, and finally explores the unknown content through recommendation from other users in the same social group, who are also interested the same content.
- User-Social Group-User-Content (P3): The source user node finds the unknown content through recommendation from other users in the same social group, which is similar to P2.
- User-Social Group-Content (P4): This type of path is similar to P2 and P3.

Given a path $P = \{v_0, \dots, v_n\}$, we assume $\Upsilon(P)$ as the probability of a single random walk way from source node v_0 to unknown content node v_n , which is given by

$$\Upsilon(P) = \prod_{v_k \in P, 1 \leq k < n} \omega(v, v+1). \quad (10)$$

Assume the $P(i, l)$ denotes all the paths between user i and content l , the probability of u_i requesting or caching f_l is given by:

$$p_{il} = \sum_{P \in P(i, l)} \Upsilon(P). \quad (11)$$

Now, we propose the User Preference Prediction (UPP) algorithm in Algorithm 1.

Algorithm 1 User Preference Prediction Algorithm (UPP)

- 1: Construct the "User-Content-Social Group" tripartite graph based on realistic social dataset;
 - 2: **for** $\forall u_i \in U, f_l \in F$ **do**
 - 3: **for** $\forall P \in P(i, l)$ **do**
 - 4: Calculate the random walk probability based on equation (8);
 - 5: Random walk within the 3-step;
 - 6: $\Upsilon(P) = \prod_{v_k \in P, 1 \leq k < n} \omega(v, v+1)$;
 - 7: **end for**
 - 8: $p_{il} = \sum_{P \in P(i, l)} \Upsilon(P)$;
 - 9: **end for**
 - 10: Obtain the potential cache/request list.
-

For each CH or CR, the potential cache/request list can be represented as: $P_i^{cache} = \{p_{i1}, \dots, p_{il}, \dots, p_{iL}\}$ or $P_j^{request} = \{p_{j1}, \dots, p_{jl}, \dots, p_{jL}\}$. Note that if the CR r_j has received the f_l , the corresponding p_{jl} is set to be 0. Because one user may not request the same content received before. For r_j , if the most interested content of r_j is f_l (p_{jl} is the maximum in $P_j^{request}$), he will request to those CHs who also have high probability of caching f_l . The share willingness P_{ij}^{l*} can be defined as the potential probability of h_i caching f_{l*} :

$$P_{ij}^{l*} = \frac{p_{il*}}{\sum_{l=1}^L p_{il}}. \quad (12)$$

Therefore, the social trust value ϖ_{ij} can be defined as weight sum of social interaction probability, reciprocal probability and potential probability of content sharing. The normalized social trust probability between h_i and r_j can be given by

$$\varpi_{ij} = \lambda_1 I_{ij} + \lambda_2 rb_{ij} + \lambda_3 P_{ij}^{l*}, \quad (13)$$

where $\lambda_1 + \lambda_2 + \lambda_3 = 1$. In this paper, we set $\lambda_1 = \lambda_2 = \lambda_3$ to give equal importance. Note that we model the social trust as a probability, which represents the probability of content sharing or spectrum sharing with confidence. Given the social trust, we can construct a social trust graph, in which the edge between two users exists when the social trust exceeds a threshold. Then the betweenness centrality can be obtained using the equation (6) in [30]. The BS can employ some MUs as CHs considering both the betweenness centrality and storage capacity.

C. Directed Hypergraph Model

Now, we will construct directed hypergraph for the cumulative and asymmetric interference with context information and social trust. We first give the definitions of conventional hypergraph's variation: directed hypergraph.

Definition 1 ([27], [34]): A hypergraph $G_H = (V, E)$ on a finite vertex set $V = \{v_1, \dots, v_n\}$ is a family $E = \{e_1, \dots, e_m\}$ of subsets of V , satisfying: 1) $e_i \neq \emptyset, \forall e_j \in E$, and 2) $\bigcup_{e_j \in E} e_j = V$, and each element e_j of E is termed as hyperedge.

Hypergraph is a generalized graph where each hyperedge contains any subset of vertex set. Note that the above definition normally describes the undirected hypergraph. Given V and E , the undirected hypergraph can be expressed by a $n \times m$ incidence matrix. According to [34], the incidence matrix $X = [x_{ij}]_{n \times m}$ specified from an undirected hypergraph $G_H = \{V, E\}$ is a Boolean matrix, where $x_{ij} = 1$ or 0 can determine whether or not v_i belongs to e_j .

The undirected hypergraph has been widely used to model the cumulative interference effect caused by multiple weak interferers, so that users can avoid sharing spectrum with other users in the same hyperedge. Considering that the traditional bipartite graph can only capture the pair-wise interference while the hypergraph can capture more complex interference relationship among more than two users. However, the undirected hypergraph cannot accurately reflect the asymmetric relationship, since the interfered users and non-interfered users are not clearly classified. In this case, we adopt the directed hypergraph to model the asymmetric interference relationships.

Definition 2 ([35]): Given a finite vertex set V , a directed hypergraph or hyperarc is an ordered pair $E = (T, H)$ of disjoint subsets of V , where T is the tail set and H is the head set. A directed hypergraph G_{DH} can be denoted as a pair $\{V, E\}$.

For a directed graph G_{DH} , the advanced incidence matrix $X = [x_{ij}]_{n \times m}$ can be redefined as

$$x(i, j) = \begin{cases} 1, & \text{if } v_i \in H(e_j); \\ -1, & \text{if } v_i \in T(e_j); \\ 0, & \text{otherwise,} \end{cases} \quad (14)$$

where $H(e_j)$ and $T(e_j)$ represent the head and tail of directed hyperedge e_j , respectively. It is worth mentioning the head node represents the interfered user and the tail node represents non-interfered user.

For the construction of directed hypergraph, the authors in [27] considered that the hyperedge is constructed only if the wanted signal ratio to the interference is below a threshold. In [10], the author stated that it will be interesting to investigate how to model the social trust as a probability, how to decide the threshold to trust, and how to design the suitable resource allocation scheme based on the probability in the future work. Inspired by [10], [27], we consider not only the physical interference, but also the social trust probability of the interference source. For a D2D pair i , we assume that social trust value ϖ_i denotes the probability of establishing a social-trusted link of D2D pair i , since ϖ_i can represent the social trust probability [32]. Meanwhile, D2D pair i will

Fig. 3: An example of directed hypergraph and its incidence matrix

actively or passively attack the content sharing of D2D pair j . Considering that their social trust probability is ϖ_{ij} , the social untrust probability can be represented by $(1 - \varpi_{ij})$. For the D2D pair set $D = \{d_1, \dots, d_i, \dots, d_N\}$, if the wanted signal with the social trust probability ϖ_{ij} , i.e., $\varpi_i P_i h_i$, to the cumulative social untrusted interference ratio falls below a threshold η_d , the d_i as well as all the interferers form a directed hyperedge, i.e.,

$$\frac{\varpi_i P_i h_i}{\sum_{i' \in D_m} (1 - \varpi_{i', i}) P_{i'} h_{i', i} + (1 - \varpi_{m, i}) P_m h_{m, i}} < \eta_d. \quad (15)$$

Similarly, for a CU c_m , if the wanted signal to the cumulative social untrusted interference ratio falls below a threshold η_c , the c_m and all the interferers and together form a directed hyperedge, i.e.,

$$\frac{P_m h_m}{\sum_{i' \in D_m} (1 - \varpi_{i', m}) P_{i'} h_{i', m}} < \eta_c. \quad (16)$$

Note that the difference between the above two conditions is that the D2D pair should also consider the social trust between the D2D transmitter (CH) and receiver (CR). For these two conditions, it is rational to consider both the wanted signal to the cumulative interference ratio as well as the social trust. Because one user may not only consider the signal and interference intensity, but also the social trust with the interferers. For example, when the social trust between each member is high, we can tolerate a certain degree of rate decrease in spectrum-sharing since we do not worry about the privacy. Based on this idea, we give a simple example of a directed hypergraph and its incidence matrix as shown in Fig.3.

Note that we have to do a slight adjustment for some special directed hyperedges. For example, all the user nodes belonging to $E2$ are interfered. Similar to [29], we set a virtual node VN as the head for special hyperedges, avoiding the lack of head. Similar to [27], we set the maximum cardinality of hyperedge equals to 3 to reduce the complexity. Next, we will utilize the different interference states to formulate the optimization problem.

D. Problem Formulation

Based on above descriptions and assumptions, we first introduce a binary variable y_{ij} to represent user i 's interference

state in hyperedge e_j , which is defined as follows:

$$y_{ij} = \begin{cases} 1, & \text{if } x_{i,j} = -1; \\ 0, & \text{otherwise.} \end{cases} \quad (17)$$

Definition 3 (Social interference): Let $SI_i(a_i)$ represent user i 's received cumulate social interference when selecting channel a_i , which is given by

$$SI_i(a_i, a_{-i}) = \sum_{e_j \in E} \phi_i(e_j) y_{ij}, \quad (18)$$

where $a_i \in A_i$ and a_{-i} denote the current channel selection profile for user i and all users except i . $A_i = 0, 1, \dots, M$ is user i 's available channel set. The strategy '0' indicates that the user does not select any channel. The indicator function $\phi_i(e_j)$ is defined as follows:

$$\phi_i(e_j) = \begin{cases} 1, & \text{if } a_i \neq 0, a_i = a_{i'}; \forall v'_i \in e_j; \\ 0, & \text{otherwise.} \end{cases} \quad (19)$$

Let C_i denote the normalized secure content sharing capacity of user i , which is given by

$$C_i(a_i, a_{-i}) = \begin{cases} 1, & \text{if } a_i \neq 0, SI_i(a_i, a_{-i}) = 0; \\ 0, & \text{otherwise,} \end{cases} \quad (20)$$

where $C_i(a_i, a_{-i}) = 0$ implies that user i cannot share contents securely. Given the above assumption, the optimization problem is formulated as

$$\max_{a_i \in A_i} \sum_{i=1}^N C_i(a_i, a_{-i}), \quad (21)$$

$$s.t. \quad C_m(a_m, a_{-m}) = 1, \forall c_m \in CU, \quad (22)$$

where C1 ensures the secure transmission for each CU, which can be achieved by portraying hyperedge connecting each two CUs. The problem (21) is a NP-hard combinatorial optimization problem. Meanwhile, the implied D2D pairing problem should also be solved. We will propose a directed hypergraph-based learning scheme to jointly solve the channel selection and user pairing problems in an iterative way.

IV. SECURITY ENHANCED CONTENT SHARING SCHEME

In this section, we propose a hierarchical game model to decouple the aforementioned optimization problem into a user pairing sub-problem and a resource allocation sub-problems. Based on this model, we formulate the first sub-problem as a rotation-swap matching sub-game and the second one as a secure channel selection sub-game, respectively. Then, the corresponding rotation-swap matching algorithm and learning algorithm are proposed to solve these two sub-problem in an iterative way. Finally, some crucial properties such as convergence, optimality, stability, and complexity will be analyzed in detail.

A. User Pairing Problem

In each content sharing process, one CR will request desired contents from one CH, which belongs to the category of one-to-one matching game. However, different from the conventional one-to-one matching problem such as classic stable marriage problem, the preference will dynamically change in the matching process, due to the co-channel interference from other CHs sharing the same spectrum. This interaction is known as *peer effect* or *externality* in matching theory. Generally, the set of $CH = \{h_i\}_{i=1}^{|N|}$ and $CR = \{r_j\}_{j=1}^{|N|}$ are assumed to be two disjoint sets of rational and selfish players for their own benefits. The optimization problem of user pairing can be further formulated as

$$\max_{b_{ij}} \sum_{i=1}^N \sum_{j=1}^N b_{ij} C_i(a_i, a_{-i}), \quad (23)$$

$$s.t. \quad C1: \sum_{i=1}^N b_{ij} = 1, \sum_{j=1}^N b_{ij} = 1, \quad (24)$$

where b_{ij} is a binary variable to determine whether or not h_i accepts the request from r_j . C1 makes sure that one CR can request content from one CH while one CH can only serve one CR per time. The utility function U_i^h for h_i is measured by the social trust over each CR. And the utility function U_j^r for r_j is measured by both the wanted signal to the cumulative social interference ratio as well as the social trust with the requested CH, as same as the equation (15). This setting can guarantee that the optimization problem in user pairing keeps the same as in problem (21).

Definition 4: The one-to-one matching Ω is a function mapping from $CR \cup CH \cup \emptyset$ into $CR \cup CH \cup \emptyset$ such that for $r_j \in CR$ and $h_i \in CH$: 1) $|\Omega(r_j)| = 1, \forall r_j \in CR$ and $\Omega(r_j) = \emptyset$, if $\Omega(r_j) \notin CH$; 2) $|\Omega(h_i)| = 1, \forall h_j \in CH$, and $\Omega(h_i) = \emptyset$, if $\Omega(h_i) \notin CR$; and 3) $\Omega(r_j) = h_i$, only if $h_i \in \Omega(r_j)$.

We write $(h_i, \Omega) \succ_{r_j} (h_{i'}, \Omega')$ to mean r_j prefers h_i in Ω to $h_{i'}$ in Ω' , when $U_r^j(h_i, \Omega) > U_r^j(h_{i'}, \Omega')$. It is obvious that the utility function is influenced not only by its matching partner, but also other users reusing the same spectrum.

Definition 5 ([30]): As a subset of CR , the rotation-swap blocking family $\mathcal{K} = \{r_1, \dots, r_j, \dots, r_k\}$, $1 \leq k \leq N$ satisfies the following condition: for each r_j , $1 \leq j \leq k$ ($j-1 = k$ when $j=1$), $\Omega(r_{j-1}) \succeq_{r_j} \Omega(r_j)$.

The rotation-swap blocking family reorganizes the swap intention of users in a circular manner. In this way, not only the direct blocking relation but also the undirected relation can be satisfied. In short, the direct blocking relation is "You prefer my partner while I prefer your partner". The undirected blocking relation is "I prefer your partner, you prefer his partner, and finally he prefers my partner". In addition, the swap-operation should ensure that the utilities of users within rotation-swap blocking family increase while the utilities of the outside users are at least not worse. Therefore, the rotation-swap matching is given by

$$\Omega_{RS} = \Omega(\{(r_1, \Omega(r_1)), (r_2, \Omega(r_2)), \dots, (r_k, \Omega(r_k))\} \cup \{(r_1, \Omega(r_k)), (r_2, \Omega(r_1)), \dots, (r_k, \Omega(r_{k-1}))\}) \quad (25)$$

Equation (25) reflects that the swap intention of users in rotation-swap blocking family is satisfied while keeping the state of other users unchanged. Finally, the definition of rotation-swap stability is given by

Definition 6: A matching Ω containing no rotation-swap blocking family is rotation-exchange stable.

Based on the above definition, we adopt the rotation-swap matching algorithm in [30] to self-organize the D2D user pairing. Note that we can satisfy each rotation-swap blocking family rather than run this algorithm again after the first iteration. The obtained D2D pair set is denoted as $D = \{d_i\}_{i=1}^{|N|}$.

B. Secure Channel Selection Problem

To further enhance the security of content sharing, we should optimize the channel selection strategy for each D2D user and cellular user. For simplicity, we use the common mobile user set $MU = \{u_1, \dots, u_i, \dots, u_V\}$ to represent all D2D users and CUs, where $|V| = |N| + |M|$. We first formulate a secure channel selection game $\mathcal{G} = \{\mathcal{V}, \mathcal{M}, \{A_i\}_{i=1}^{|V|}, \{U_i\}_{i=1}^{|V|}\}$, where $\mathcal{V} = \{1, \dots, V\}$ represents the users, $\{A_i\}_{i=1}^{|V|}$ denotes user i 's available channel selection set, and $\{U_i\}_{i=1}^{|V|}$ denotes the utility. Hence, player i 's utility function can be represented as

$$U_i(a_i, a_{-i}) = C_i(a_i, a_{N_i}) + \sum_{k \in N_i} C_k(a_k, a_{N_k}) \varphi_{i,k}, \quad (26)$$

where N_i represents user i 's neighbor nodes in directed hypergraph (in the same hyperedge), a_{N_i} denotes the channel selection profiles of i 's neighbor nodes, and $\varphi_{i,k}$ is a binary variable to determine whether or not user k is interfered by user i . This setting can make sure the secure content sharing for both user i and its neighbor users. Given this setting, the secure channel selection game can be represented as

$$(\mathcal{G}) : \max_{a_i \in A_i} U_i(a_i, a_{-i}), \forall i \in \mathcal{V}. \quad (27)$$

In the formulated secure channel selection game $\mathcal{G}$, each user aims to maximize its utility by making the optimal channel selection decision. Next, we give two crucial definitions about this game.

Definition 7: (Pure Nash equilibrium, PNE [24]): A selection profiles $\mathbf{a} = \{a_1^*, \dots, a_i^*, \dots, a_V^*\}$ is a PNE, if and only if no player can gain more profit by deviating unilaterally. Mathematically, $U_i(a_i^*, -a_i^*) \geq U_i(a_i, -a_i^*), \forall i \in \mathcal{V}, a_i \in A_i$.

Definition 8: (Exact potential game [24]): $\mathcal{G}$ is an exact potential game, if its potential function $\Phi(a_i, -a_i)$ satisfying $U_i(a_i, -a_i) - U_i(\bar{a}_i, -a_i) = \Phi(a_i, -a_i) - \Phi(\bar{a}_i, -a_i)$, where $\bar{a}_i$ is game player i 's selection after deviation.

Theorem 1: The proposed secure channel selection game $\mathcal{G}$ is an exact potential game, which has at least one pure strategy NE maximizing the potential function.

Proof: To maintain the same optimization goal with problem (20), we set the potential function $\Phi(a_i, -a_i) = \sum_{i=1}^N C_i(a_i, a_{-i})$. Assume that an arbitrary player i changes

its selection from a_i to $\bar{a}_i$, then the corresponding change of the potential function can be expressed as

$$\begin{aligned} \Phi(a_i, -a_i) - \Phi(\bar{a}_i, -a_i) &= [C_i(a_i, a_{N_i}) - C_i(\bar{a}_i, a_{N_i})] + \\ &\left[\sum_{k \in N_i} (C_k(a_k, a_{N_k}) - C_k(a_k, \bar{a}_{N_k})) \right] + \Gamma(\mathcal{V}/(i \cup N_i)), \end{aligned} \quad (28)$$

where $\Gamma(\mathcal{V}/(i \cup N_i))$ represents the difference value of potential function for those who are independent of a_i and $\bar{a}_i$, respectively. $\Gamma(\mathcal{V}/(i \cup N_i)) = 0$ because this part will not change with the unilaterally change from a_i to $\bar{a}_i$.

We further simplify the second term in equation (27) as

$$\begin{aligned} &\left[\sum_{k \in N_i} (C_k(a_k, a_{N_k}) - C_k(\bar{a}_k, a_{N_k})) \right] = \\ &\left[\sum_{k \in N_i} C_k(a_k, a_{N_k}) \varphi_{i,k} - \sum_{k \in N_i} C_k(a_k, \bar{a}_{N_k}) \varphi_{i,k} \right] + \\ &\left[\sum_{k \in N_i} C_k(a_k, a_{N_k}) (1 - \varphi_{i,k}) - \sum_{k \in N_i} C_k(a_k, \bar{a}_{N_k}) (1 - \varphi_{i,k}) \right]. \end{aligned} \quad (29)$$

It is obvious that the last term in equation (20) equals to 0. Because when $\varphi_{i,k} = 1$, i.e., user k is interfered by i , the condition $C_k(a_k, a_{N_k}) = 0$ is always satisfied. In contrast, when $\varphi_{i,k} = 0$, i.e., user k is not interfered by i , we can get $C_k(a_k, a_{N_k}) - C_k(a_k, \bar{a}_{N_k}) = 0, \forall k \in N_i$, and thus the last term still equals to 0. Based on the above derivative process, we can get $\Phi(a_i, -a_i) - \Phi(\bar{a}_i, -a_i) = U_i(a_i, -a_i) - U_i(\bar{a}_i, -a_i)$, and thus we prove that $\mathcal{G}$ is an exact potential game, so that the PNE point constitutes the optimal solution for problem (20).

C. Learning Algorithm for Secure Content Sharing

Aiming at asymptotically converging to the NE of our formulated secure channel selection game $\mathcal{G}$, some effective learning algorithms such as spatial adaptive play (SAP) [36] and decentralized multi-person stochastic learning (DMPSL) [37] can converge to a desirable solution. However, the SAP can only update the selection profile for one user in each iteration, which decreases the convergence speed for our game model. Besides, the DMPSL updates the selection profile for all users, which also decreases the convergence speed in our dynamic network. For example, when two users interfered by each other concurrently change their selection, they may still select the same channel. Inspired by these two learning algorithms, we propose a UUCL algorithm. The uncoupled user do not have any common neighbors in undirected hypergraph. Specifically, we randomly let multiple uncoupled users update their selection profile in each iteration. This method can accelerate the convergence speed while ensuring that the selected users' selection change will not affect others' selection change in each iteration. Let $\Psi_{A_i}(k)$ denote the user i 's channel selection probability distribution following the Boltzmann-Gibbs rule, and $q_i^{a_i}(k) \in \Psi_{A_i}(k)$ denote the channel selection probability of a_i , which can be expressed as

$$q_i^{a_i}(k+1) = \frac{\exp(\epsilon U_i(a_i, a_{N_k}(k)))}{\sum_{a'_i \in A_i} \exp(\epsilon U_i(a'_i, a_{N_k}(k)))}, \quad (30)$$

where ϵ is the learning parameter satisfying that $\epsilon > 0$, which can balance the trade-off between exploration and exploitation. Smaller ϵ indicates that the users are prone to explore an suboptimal selection, whilst higher ϵ indicates that they are more willing to choose the optimal selection. In our cross-layered SIoT scenario, we assume that the context information and social trust can be obtained from social platform, and then the user can learn to cache and request until convergence. Finally, users can feedback the content sharing decision to the physical domain via server. For simplicity, the entire secure content sharing scheme embedded with channel selection and user pairing is presented in Algorithm 2.

Algorithm 2 Secure Content Sharing Algorithm (SCS)

- 1: **Step 1: Initialization:**
 - 2: BS maps the context information in physical domain into social platform. Construct the directed hypergraph model with the context information and social trust.
 - 3: **Step 2: User Pairing:**
 - 4: CHs and CRs select their partner using rotation-swap matching algorithm in [30].
 - 5: **Step 3: UUCL-based Channel Selection:**
 - 6: Initialize the $q_i^{a_i}(0) = 1/M, \forall i \in V$.
 - 7: Given the matching result of CHs and CRs, randomly select multiple uncoupled users in k -th iteration based on the directed hypergraph model.
 - 8: Let the selected users update their selection probability distribution from $\Psi_{A_i}(k)$ to $\Psi_{A_i}(k+1)$ and select one channel conditioned on $\Psi_{A_i}(k+1)$, while others' channel selection strategy maintain unchanged.
 - 9: Stop until the predefined maximum iteration number is reached or the selection probability distribution has been unchanged for each user.
 - 10: **Step 4:** Repeat **Step 1~Step 3** until the utility for each user is unchanged.
-

D. Property Analysis

Furthermore, we will provide some important theoretical analysis about convergence, optimality, and complexity properties. We omit the proof of stability here since this proof is similar to [30].

Theorem 2: UUCL can converge to the PNE point with an arbitrarily high probability when the learning parameter ϵ is sufficiently large, and thus SCS can converge within finite iterations. The final state of SCS is Pareto optimal.

Proof: Based on [36], since the SAP can achieve the global optimum and converge to the PNE point with an arbitrarily high probability, we can prove that UUCL can also achieve the same goal, because we concurrently implement SAP for multiple uncoupled users and the selected users' selection change will not affect others' selection change in each iteration. We can also prove the stability of SCS, because the utility of each user after each iteration will be at least as good as the utility before this iteration. Considering that the channel and user number are limited, the utility of each users cannot increase indefinitely and finally remain unchanged. In

this situation, we can prove that the SCS achieves the Pareto optimal since it is impossible to make any one individual better off without making at least one individual worse off.

Theorem 3: The computational complexity of the proposed UDP and SCS algorithms are formulated as $\mathcal{O}(\Lambda N|E|)$ and $\mathcal{O}(\tau(K_1 N^2 + K_2(N+M)(M+1)))$ in the worst case, respectively.

Proof: We first calculate the computational complexity of UDP algorithm in section III. Since the maximum distance in each random walk is 3, final/third step of preference propagation causes the major consumption. In the worst case, we assume that the second step of preference propagation traverses all the user nodes and social group nodes, and the corresponding complexity for all users is $\mathcal{O}(N|E|)$, where N denotes the CH/CR number and $|E|$ denotes the edge number in user-content-social group tripartite graph. Given the iteration times Λ , the sum computational complexity of UDP is $\mathcal{O}(\Lambda N|E|)$ in the worst case.

Considering the combinatorial nature, the computational complexity of each sub-algorithm included in SCS will be calculated in turn. Similar to [30], the complexity of rotation-swap matching algorithm is $\mathcal{O}(K_1 C_N^2 N^2)$ in the worst case, where K_1 is the iteration times. The complexity of finding the uncoupled user is $\mathcal{O}((N+M))$, where M represents the CU number. Considering that each user has $M+1$ selection in each iteration, the complexity of SCS is $\mathcal{O}(\tau(K_1 C_N^2 N^2 + K_2(N+M)(M+1)))$, where K_2 and τ are iteration times for UUCL and SCS, respectively. In fact, the iteration numbers are relatively fewer than the user numbers, which can be verified by the following simulation results.

V. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

In this section, we conduct simulations in different scenarios to demonstrate the validity of the theoretical analysis. we evaluate our proposed algorithm, abbreviated as “SCS” in terms of convergence and trade-off between security and QoE. The main simulation parameters are listed in Table II. We set the parameters based on the existing works and 3GPP specifications [10], [27], [38], [39], which are applicable for wireless communication of most heterogeneous cellular networks, and QoE evaluation of most video applications over wireless networks. To balance the trade-off between exploration and exploitation, the learning parameter ϵ is equal to the iteration number k and bounded by half of k_{max} according to [36]. Note that the selection of learning parameter will affect the convergence speed. Besides, Theorem 3 proved that the SCS can achieve the global optimum with arbitrarily high probability if the learning parameter is sufficiently large, which can also prove that the system performance achieved by SCS will not be affected by sufficiently large ϵ . Furthermore, we adopt different benchmark algorithms to objectively and comprehensively evaluate our proposed algorithm. We compare our proposed learning algorithm, abbreviated as “UUCL”, with SAP in [36] and DMPSL in [37] in terms of convergence rates. On the other hand, we compare our proposed secure content sharing scheme, termed as “SCS” with the “Exhaustive Search” (global optimum), undirected-hypergraph coloring

scheme in [27], random selection, and our proposed scheme without considering the social trust in constructing hyperedge, termed as "Without Social Trust". For practically, we analyze the users' social behaviors based on dataset INFOCOM 06 [40] from CRAWDAD. There are 78 active users with their 35 interested topics and contact history records¹. We randomly select active users as CUs, CHs, and CRs. To make the dataset more applicable to our paper, these 35 topics are assumed to be contents in our framework i.e., $L = 35$, and thus the cached history are derived. We believe that the above setting can make the simulation results more practical and realistic.

TABLE II: Simulation Parameters

Parameters	Value
Cell radius	500m
Maximum distance between D2D users	50m
The storage space of CHs	100-1000Mbits
Size of each video	10-100Mbits
Threshold η_d and η_c	20dB
Transmission power of CUs and D2D users	23dBm, 13dBm
Noise power σ^2	-174dbm/Hz
Transmission Bandwidth Block B	180kHz [39]
Pass-loss exponent	4
The width of the Gaussian kernel σ	2 [32]
Maximum iteration number k_{max}	100 [38]
Frame rate and packet loss rate	10fps, 0.1 [38]
Parameters $c_1 - c_5$ in E.q. (3)	2.797, -0.0065, 0.2498, 2.2073, 7.1773 [38]
Simulation times	10000

A. Convergence Behavior

In Fig. 4, we randomly select three users in a directed hyperedge and present their strategy update state in the learning process of UUCL. It is obvious that only one user updates their channel selection in each iteration, since they are coupled with another. All of them will avoid selecting the same channel to secure their content sharing. To test the convergence performance, we change the number of users and compare the change of iteration numbers with other benchmarks in Fig. 5. It is obviously that the average iteration numbers increases as D2D user number and CU number increase, because the increasing number of hyperedges will reduce the convergence speed. Compared with other benchmarks, the convergence rate of UUCL increases dramatically. It is because SCS can both reduce the unnecessary updates with respect to DMPSL, and improve the learning efficiency in each iteration with respect to SAP.

To demonstrate the convergence behavior of SCS, we investigate the cumulative distribution function (CDF) versus the iteration numbers. In Fig. 6, we plot the CDF of iteration number asymptotically converging to the stable state, thereby demonstrating the validity of Theorem 2. Meanwhile, we note that the needed iteration number of SCS grows with the D2D user and CU numbers. It is because the number of users will affect the interplay between channel allocation and user pairing. The probability of deviating to other better choice will increase in both channel selection and user pairing processes. In addition, Fig. 6 further reveals that the needed iteration number is relatively small with respect to the D2D user

¹There are originally 98 experimental devices, but the interest information for 20 of them is missing. Therefore, only 78 active users can provide valid information for our analysis.

Fig. 4: Channel selection update of users in the same hyperedge, with N=10 and M=5

Fig. 5: Comparison of the convergence rates, in terms of the average number of iterations

number and thus demonstrating the validity of the theoretical analysis in Theorem 3.

B. The Trade-off between Security and QoE

Fig. 7 compares the normalized secure content sharing capacity attained by our proposed SCS scheme with other benchmarks. In this figure, we set the number of CUs to 10, and the number of D2D pairs from 20 to 30, which can guarantee the complexity of the constructed hypergraph model. It is observed that normalized secure content sharing capacity of "Exhaustive Search", SCS, and hypergraph coloring scheme increase as D2D number increases. And the increase trend is fast when the number of D2D pairs is below 24. Because the social trust are dominant in calculating the capacity due to weak interference at this period. Therefore, the benchmark "Without Social Trust" cannot utilize this information, which decreases the performance. When D2D users' number exceeds 24, the stronger cumulative interference plays more important role, and thus the growth trend is flattening out. In addition, SCS can achieve the near-optimal solution than coloring scheme, because it comprehensively models the asymmetric and cumulative interference in graph construction. It is noticed that the "Random Selection" scheme is always fluctuant. This is because it randomly pairs the D2D users. As a result, the normalized secure content sharing capacity

Fig. 6: Distribution of the iteration numbers in SCS

Fig. 7: Average normalized secure content sharing capacity versus D2D user numbers, with $M=10$

Fig. 8: Average ratio of users in different MOS, with $M=10$

Fig. 9: Average normalized secure content sharing capacity and MOS versus threshold η , with $N=30$ and $M=10$

shows the fluctuant trend. In other words, SCS can achieve the near-optimal solution by comprehensively considering the interference relationship and social trust information.

In Fig. 8, we adopt the modified MOS method in [31] to evaluate the the integrated impact of network measurements on QoE. It can be seen from this figure that the MOS decreases with the number of D2D users, due to the reduced spectrum efficiency. Note that SCS can achieve the near-optimal performance in satisfying users' QoE. Both the benchmark "Without Social Trust" and "Random Selection" achieve the poor performance, because the ignorance of social trust will reduce the hit ratio, and thus the ratio of score "0" is high. Based on Fig. 7 and Fig. 8, our proposed scheme can be viewed to achieve a better trade-off between security and QoE.

In Fig. 9, we investigate the impact of threshold η in hyperedge construction on the performance of security and QoE achieved by SCS. On the one hand, we noted that the security performance decreases as the value of η increases, because the increasing η would make it easier to form a hyperedge, and thus the social interference increases according to E.q. (18). Therefore, CU will share spectrum with fewer D2D users, and only CU can ensure their security in the end. On the other hand, the QoE curve tends to increase first and then decrease. When the threshold is below 20dB, more hyperedges will enable D2D users to select the appropriate channel, and thus the QoE performance increases. In this stage, less hyperedges

will reduce the QoE performance, since more D2D users will share the same channel without the constraint. When the threshold is above 20dB, i.e., the number of hyperedges is sufficiently large, fewer D2D users will be allocated to channels, and thus the QoE performance decreases. Finally, no D2D users can share the cellular spectrum, so that the average MOS equals to 0.

We further analyze the impact of file number L on the performance of security and QoE achieved by SCS. In this simulation, each user is assumed to randomly have interest in 10% of L files. Fig. 10 shows that both the security and QoE performance will decrease with L . The reason is that the probability of quantifying sharing willingness will decrease with L , and thus the reduced social trust will make it easier to form a hyperedge. Therefore, both the security and QoE performance will decrease. Besides, when L becomes sufficiently large, the probability of quantifying share willingness has almost no influence on the value of social trust, and thus the downward trend tends to be flat.

VI. CONCLUSION

In this paper, we have investigated the secure content sharing problem to strike a trade-off between security and QoE for SIoT. Specifically, we first proposed a UPP algorithm to predict the social trust metrics based on the realistic dataset. Then, the undirected hypergraph model was formulated to

Fig. 10: Average normalized secure content sharing capacity and MOS versus file number L , with $N=30$ and $M=10$

accurately characterize the cumulative and asymmetric social interference. In general, we formulated the optimization problem as a hierarchical game model to decouple the optimization problem as a user pairing sub-problem and a channel selection sub-problem, respectively. We formulated the user pairing sub-problem as a one-to-one matching sub-game with peer effect and the channel selection sub-problem as a secure channel selection sub-game. For the first sub-game, the embedded rotation-swap matching algorithm can smoothen out the instability caused by dynamically changing co-channel interference. For the second sub-game, we designed a UUCL algorithm, which can converge to the optimal pure Nash equilibrium and thus maximizing the normalized secure capacity. The simulation results show that our proposed algorithms could achieve a near optimal performance compared with the Exhaustive Search, and outperform the benchmark scheme under various simulation scenarios. We believe that this study has opened a new paradigm for designing secure content sharing scheme in SIoT and has provided effective implementation methods by leveraging social trust to enhance the security in physical domain.

REFERENCES

- [1] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012.
- [2] M. Nitti, L. Atzori, and I. P. Cvijikj, "Network navigability in the social internet of things," in *Proc. IEEE WF-IoT*, Mar. 2014, pp. 405–410.
- [3] M. Ji, G. Caire, and A. F. Molisch, "Fundamental limits of caching in wireless D2D networks," *IEEE Trans. Inform. Theory*, vol. 62, no. 2, pp. 849–869, Feb. 2016.
- [4] X. Lin, J. G. Andrews, and A. Ghosh, "Spectrum sharing for device-to-device communication in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6727–6740, Dec. 2014.
- [5] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surv. Tut.*, vol. 19, no. 2, pp. 1054–1079, Secondquarter 2017.
- [6] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.
- [7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surv. Tut.*, vol. 16, no. 3, pp. 1550–1573, Thirdquarter 2014.
- [8] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE ISIT*, Seattle, WA, Jul. 2006, pp. 356–360.
- [9] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
- [10] X. Chen, Y. Zhao, Y. Li, X. Chen, N. Ge, and S. Chen, "Social trust aided D2D communications: Performance bound and implementation mechanism," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1593–1608, Jul. 2018.
- [11] M. Ahmed, Y. Li, Z. Yinxiao, M. Sheraz, D. Xu, and D. Jin, "Secrecy ensured socially aware resource allocation in device-to-device communications underlying hetnet," *IEEE Trans. Veh. Technol.*, vol. 68, no. 5, pp. 4933–4948, May. 2019.
- [12] K. Zheng, J. Zhang, X. Liu, L. Fu, X. Wang, X. Jiang, and W. Zhang, "Secrecy capacity scaling of large-scale networks with social relationships," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2688–2702, Mar. 2017.
- [13] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Social trust and social reciprocity based cooperative D2D communications," in *Proc. ACM MobiHoc*. New York, NY, USA: ACM, Jul. 2013, pp. 187–196.
- [14] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5651–5663, Aug. 2016.
- [15] Z. H. Awan and A. Sezgin, "Fundamental limits of caching in D2D networks with secure delivery," in *Proc. IEEE ICCW*, London, Jun. 2015, pp. 464–469.
- [16] J. Y. Ryu, J. Lee, and T. Q. S. Quek, "Confidential cooperative communication with trust degree of potential eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3823–3836, Jun. 2016.
- [17] X. Wang, M. Chen, T. Taleb, A. Ksentini, and V. C. M. Leung, "Cache in the air: exploiting content caching and delivery techniques for 5G systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 131–139, Feb. 2014.
- [18] D. Wu, Q. Liu, H. Wang, Q. Yang, and R. Wang, "Cache less for more: Exploiting cooperative video caching and delivery in D2D communications," *IEEE Trans. Multimedia*, vol. 21, no. 7, pp. 1788–1798, Jul. 2019.
- [19] C. Ma, M. Ding, H. Chen, Z. Lin, G. Mao, Y. Liang, and B. Vucetic, "Socially aware caching strategy in device-to-device communication networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4615–4629, May. 2018.
- [20] F. Jameel, S. Wyne, D. N. K. Jayakody, G. Kaddoum, and R. O'Kennedy, "Wireless social networks: A survey of recent advances, applications and challenges," *IEEE Access*, vol. 6, pp. 59 589–59 617, 2018.
- [21] L. Xiang, Q. Yuan, S. Zhao, L. Chen, X. Zhang, Q. Yang, and J. Sun, "Temporal recommendation on graphs via long- and short-term preference fusion," in *Proc. ACM KDD*. Washington, DC, USA: ACM, Aug. 2010, pp. 723–732.
- [22] J. Ma, H. Chen, S. Jiang, and Z. Huang, "A dynamic recommendation approach in online social networks," in *Proc. IEEE ICIEA*, Wuhan, May. 2018, pp. 364–369.
- [23] R. Diestel, "Graph theory," *Math. Gaz.*, vol. 173, no. 502, pp. 67–128, 2011.
- [24] H. Zhu, D. Niyato, W. Saad, T. Baar, and A. Hjrungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge University Press, 2012.
- [25] Y. Gu, W. Saad, M. Bennis, M. Debbah, and Z. Han, "Matching theory for future wireless networks: fundamentals and applications," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 52–59, May. 2015.
- [26] D. Tsolkas, E. Liotou, N. Passas, and L. Merakos, "A graph-coloring secondary resource allocation for d2d communications in lte networks," in *Proc. IEEE CAMAD*, Sep. 2012, pp. 56–60.
- [27] H. Zhang, L. Song, and Z. Han, "Radio resource allocation for device-to-device underlay communication using hypergraph theory," *IEEE Trans. Wireless Commun.*, vol. 15, no. 7, pp. 4852–4861, Jul. 2016.
- [28] Y. Sun, Q. Wu, Y. Xu, Y. Zhang, F. Sun, and J. Wang, "Distributed channel access for device-to-device communications: A hypergraph-based learning solution," *IEEE Commun. Letters*, vol. 21, no. 1, pp. 180–183, Jan. 2017.
- [29] Y. Sun, Z. Du, Y. Xu, Y. Zhang, L. Jia, and A. Anpalagan, "Directed-hypergraph-based channel allocation for ultradense cloud D2D communications with asymmetric interference," *IEEE Trans. Veh. Technol.*, vol. 67, no. 8, pp. 7712–7718, Aug. 2018.
- [30] B. Wang, Y. Sun, S. Li, and Q. Cao, "Hierarchical matching with peer effect for low-latency and high-reliable caching in social IoT," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 1193–1209, Feb. 2019.
- [31] X. Chen, Y. Zhao, and Y. Li, "QoE-aware wireless video communications for emotion-aware intelligent systems: A multi-layered collaboration approach," *Inform. Fusion*, vol. 47, pp. 1 – 9, 2019.

- [32] B. Ying and A. Nayak, "A power-efficient and social-aware relay selection method for multi-hop D2D communications," *IEEE Commun. Letters*, vol. 22, no. 7, pp. 1450–1453, Jul. 2018.
- [33] J. Yan, D. Wu, and R. Wang, "Socially aware trust framework for multimedia delivery in D2D cooperative communication," *IEEE Trans. Multimedia*, vol. 21, no. 3, pp. 625–635, Mar. 2019.
- [34] A. Bretto, *Hypergraph Theory: An Introduction*. Springer Publishing Company, Incorporated, 2013.
- [35] G. Gallo, G. Longo, S. Pallottino, and S. Nguyen, "Directed hypergraphs and applications," *Discrete Appl. Math.*, vol. 42, no. 2-3, pp. 177–201, Apr. 1993.
- [36] Y. Xu, J. Wang, Q. Wu, A. Anpalagan, and Y. Yao, "Opportunistic spectrum access in cognitive radio networks: Global optimization using local interaction games," *IEEE J-STSP*, vol. 6, no. 2, pp. 180–194, Apr. 2012.
- [37] P. S. Sastry, V. V. Phansalkar, and M. A. L. Thathachar, "Decentralized learning of nash equilibria in multi-person stochastic games with incomplete information," *IEEE Trans. Syst. Man. Cyb.*, vol. 24, no. 5, pp. 769–777, May. 1994.
- [38] A. Khan, L. Sun, E. Jammeh, and E. Ifeachor, "Quality of experience-driven adaptation scheme for video applications over wireless networks," *IET Commun.*, vol. 4, no. 11, pp. 1337–1347, Jul. 2010.
- [39] 3GPP, "3rd generation partnership project; technical specification group radio access network; evolved universal terrestrial radio access (E-UTRA) physical channels and modulation; protocol specification (release 15)," Dec. 2017.
- [40] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau, "CRAWDAD dataset cambridge/haggle/imote/infocom2006 (v. 2009-05-29)," Downloaded from <https://crawdad.org/cambridge/haggle/20090529>, May. 2009.

Bowen Wang received the B.S. degree in School of Electronics and Communication Engineering of China University of Mining and Technology, Xuzhou, China, in 2016. He is now working towards the Ph.D degree in School of Information and Control Engineering of China University of Mining and Technology. He was also a visiting Ph.D student at the School of Electronics from 2018 to 2019, Electrical Engineering and Computer Science, Queen's University Belfast. He was awarded the best paper award in INISCOM 2019. His research interests

include matching theory, graph theory, UAV communications, and Social Internet of Things (SIoT).

Yanjing Sun (M'16) received the Ph.D. degree in information and communication engineering from China University of Mining and Technology, Xuzhou, China, in 2008. He is currently a Professor of the School of Information and Control Engineering and the director of Network Information Center, China University of Mining and Technology. His current research interests include IBFD communications, embedded real-time system, wireless sensor networks and cyber-physical systems.

Long D. Nguyen received his B.S. degree in Electrical and Electronics Engineering and M.S. degree in Telecommunication Engineering from Ho Chi Minh City University of Technology (HCMUT), Vietnam, in 2013 and 2015, respectively. He received his Ph.D. degree in Electronics and Electrical Engineering from Queen's University Belfast (QUB), UK, in 2018. He is currently with Duy Tan University as an Adjunct Assistant Professor and Dong Nai University in Vietnam as an Assistant Professor.

Dr. Nguyen was awarded the Best Paper Award at the IEEE Digital Signal Processing (DSP) 2017, the IEEE International Conference on Recent Advances in Signal Processing, Telecommunication and Computing (Sigtelcom) 2018, the IEEE International Conference on Communications (ICC) 2019, the International Wireless Communications & Mobile Computing Conference (IWCMC) 2019 and the IEEE Global Communications Conference (GLOBECOM) 2019. He was also awarded the Exemplary Reviewer Award in IEEE Communications Letters 2018.

Trung Q. Duong (S'05, M'12, SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Currently, he is with Queen's University Belfast (UK), where he was a Lecturer (Assistant Professor) from 2013 to 2017 and a Reader (Associate Professor) from 2018. His current research interests include Internet of Things (IoT), wireless communications, molecular communications, and signal processing. He is the author or co-author of 290 technical papers published in scientific journals

(165 articles) and presented at international conferences (125 papers).

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, IET COMMUNICATIONS, and a Lead Senior Editor for IEEE COMMUNICATIONS LETTERS. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014, IEEE Global Communications Conference (GLOBECOM) 2016, and IEEE Digital Signal Processing Conference (DSP) 2017. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2016-2021) and has won a prestigious Newton Prize 2017.

Nan Zhao (S'08-M'11-SM'16) is currently a Professor at Dalian University of Technology, China. He received the Ph.D. degree in information and communication engineering in 2011, from Harbin Institute of Technology, Harbin, China.

Dr. Zhao is serving or served on the editorial boards of 9 SCI-indexed journals, including IEEE Transactions on Green Communications and Networking and IEEE Wireless Communications Letters. He won the best paper awards in IEEE VTC 2017 Spring, MLICOM 2017, ICNC 2018, WCSP 2018 and CSPA 2018. He also received the IEEE Communications Society Asia Pacific Board Outstanding Young Researcher Award in 2018.