IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 30, 2018, accepted November 13, 2018, date of publication November 27, 2018,
date of current version December 19, 2018.

*Digital Object Identifier 10.1109/ACCESS.2018.2881953*

# Blockchain Consensus Based User Access Strategies in D2D Networks for Data-Intensive Applications

**DI LIN AND YU TANG**
School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610000, China
Corresponding authors: Di Lin (lindi@uestc.edu.cn) and Yu Tang (yutang@uestc.edu.cn)

This work was supported by the National Natural Science Foundation of China 61601082.

**ABSTRACT** A device-to-device (D2D) underlying cellular network is pervasive to support various wireless applications. However, due to the dramatic increase of data transmission in the network with limited amount of wireless resource, a few users may be required to temporarily disconnect from the network to avoid the interruption of data transmission in the whole network. A critical issue of determining the user access in D2D underlying networks is the authenticity of channel state information (CSI), and usually, a user with a higher CSI can be allocated a larger amount of wireless resource or have a higher probability of staying in the network. In this paper, we propose a blockchain consensus-based scheme to verify the authenticity of CSI and add the users who intentionally advocate a higher value of CSI into a fraud chain. Also, we consider both the cross-tier interference caused by a mobile user and the presence of a user in the fraud chain to determine the access of a user. The analysis results show that our proposed user access scheme can enhance the network performance by efficiently controlling the use access in mobile applications.

**INDEX TERMS** Device-to-device (D2D), user access control, blockchain, channel state information (CSI), cross-tier interference (CTI).

## I. INTRODUCTION

Device-to-device (D2D) assisted cellular networks can improve the network performance by completing the high data-rate services through direct communication [1], [2]. However, in the data-intensive service scenarios where a large amount of data is required to be transmitted, D2D assisted cellular networks cannot support a large number of mobile users, and the scheme of user-access control in the network is quite important. Specifically, the user-access control in a D2D network is challenging due to the following difficulties: (1) The coexistence of D2D and cellular users in the same spectrum for communication can lead to cross-tier interference (CTI). The D2D users can cause CTI to cellular users, while the D2D users are influenced by the CTI from both cellular users and the other D2D users. Thus, the management of CTI between D2D and cellular users is critical to guarantee the success of designing a D2D assisted cellular network. (2) The CSI value of a user can determine the amount of resources allocated to this user, and thus the authenticity of CSI needs to be verified in order to guarantee a reasonable user access strategy. Thus, a reasonable user-access control scheme by authenticating the CSI values of each user as well as evaluating the amount of CTI caused by each user should be investigated in a D2D based cellular network.

### A. MOTIVATION

A couple of works present the issue of dynamic power and user access control for D2D-underlying cellular networks to manage the CTI between D2D and cellular users [3],10,11,12,sun. Gu *et al*. [3] propose a dynamic power control algorithm, which addresses the control of D2D transmission power in order to protect cellular transmissions. Yu *et al*. [4] present a D2D power-allocation algorithm to maximize the network throughput by restricting the transmission power of D2D users and the distance between D2D users. Specifically, Yu *et al*. [4] address a fixed booster to restrict D2D transmission power and mitigate the CTI between D2D users. Lee *et al*. [5] and Chen and Kountouris [6] address the issue of imperfect CSI, and propose statistical CSI based algorithms to mitigate CSI. Also Sun *et al*. [7] generalize the transmission power from two levels (i.e. zero or peak power) in 5 and 6 to multiple levels,



2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

and optimize the energy efficiency of a network by reducing the CTI.

All these above-mentioned works assume that the CSI provided by each user is authentic, and do not discuss the issue when a higher value of CSI is intentionally advocated. Also the above-mentioned works focus on power control schemes. However, when a network has accessed a large number of users who have data-intensive services, we cannot ensure that all the users in a network can meet their own QoS requirements even using the optimal power allocation. In this case, we need to temporarily disconnect a few users from the networks and recover their connections after the network is in a good condition again. In other words, we need to consider user access control instead of power control. To the best of our knowledge, no study addresses the problem of user access control in a network in consideration of the authenticity of CSI. *The importance of user access control in a D2D underlying cellular network motivates us to investigate how to optimize the network performance (e.g., the spectral efficiency) while guaranteeing the authenticity of CSI among users.*

### B. MAIN CONTRIBUTIONS

In this paper, we present the problem of user access control for network optimization in a data-intensive service application. The objectives of our paper are to i) achieve certain goals (e.g., the spectral efficiency) of mobile users; ii) authenticate the CSI of each user. *To the best of our knowledge, this work is the first study presenting the optimization of user access control for D2D networks in view of the authenticity of CSI with blockchain consensus methods. The primary contributions of this paper include*: i) presenting the framework of D2D underlying cellular networks for the authenticity of CSI; ii) studying the scheme of user-access control among the users in a data-intensive service application.

## II. BACKGROUND OF BLOCKCHAIN

This section addresses a few basic concepts of blockchain which will be used in the system model in the following sections. Fig. 1 shows the architecture of blockchain, which is composed of five layers: data layer, network layer, consensus layer, contract layer, application layer [8]. The data layer focuses on the data structure in order to protect the data, and it includes hash chains, digital signature, Merkle tree; The network layer focuses on the mechanism of communications in a blockchain, and it is composed of P2P network, transmission mechanism, verification mechanism; The consensus layer focuses on the consensus protocols in a blockchain to reject or accept a message; The contract layer focuses on the ways of formalizing an online business relationship; The application layer includes various blockchain applications, including finance, law, audit, healthcare, etc. [9]. To familiarize the readers, we present a few key concepts of blockchain, including ledger, consensus, cryptography.

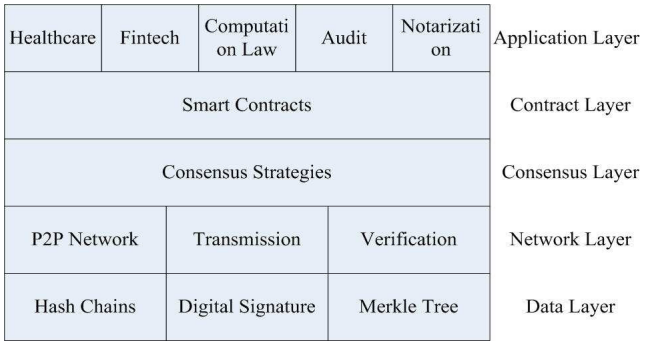


**FIGURE 1.** The Figure shows the architecture of blockchain.

### A. LEDGER

In the blockchain, a ledger is a kind of data structure which represents a list of transactions in a certain order [10]. For instance, a ledger may refer to financial transactions among a few banks, or the exchange of goods between a few parties. In a blockchain, a ledger is supposed to be replicated among all the nodes. In addition, we group the transactions together within a few chained blocks. Thus, the leger in the distributed form is actually a replicated data structure. A blockchain initially stays in a certain state, and all the updates of states will be recorded by the ledger.

### B. CONCENSUS

A ledger records the maintenance of blockchain states, and it is replicated among all the nodes in the blockchain. An update to the ledger cannot be operated if the parties do not reach an agreement, i.e all the parties must achieve a consensus before the ledger is updated [11].

A primary feature of a blockchain is that no trust exists among the nodes, and the nodes operate in the Byzantine manner. The design of consensus in a blockchain needs to tolerate the failures in the Byzantine manner [12]. Quite a few literatures have discussed the protocols of consensus in a blockchain [13], 014, 015,016, 017, 018,019, 020, 021. These consensus protocols are primarily classified into two types, one type of protocols is based on the pure computation, i.e. these protocols randomly select a node which uses the proof of computation to determine the following operation, e.g., Bitcoin's proof-of-work (PoW) [13],014. The other type of protocols is based on the pure communications between nodes, i.e. the nodes owning the same number of votes reach the consensus by experiencing multiple rounds of communications [15]. Also a few consensus protocols consider a mixture of computation and communication. The Proof-of-Elapsed-Time (PoET) protocol replaces PoW by using a trusted hardware, e.g, Intel SGX [16]. Hydrachain and Openchain in [17], [18] improve the PoW by randomly selecting a few nodes in each round of communications. Proof-of-Authority (PoA) in [19], 020, 021 employ blockchains to improve PBFT by operating consensus in a small-scaled network.

### C. CRYPTOGRAPHY

A blockchain system employs cryptographic schemes in order to guarantee the integrity of ledgers, which refers to the capacity of detecting the tamper of data in the blockchain. This feature is quite critical in a public setting where no trust is pre-established. For instance, the currency value of a Bitcoin is predicated by the integrity of a ledger, and a leger can detect the multiple spending of a Bitcoin [22].

In the blockchain, we need to consider the protection of integrity at two levels. Firstly, a hash (Merkle) tree protects the blockchain states by storing a root hash in a block, and any change of states can lead to an update of the root hash. The tree is composed of a few internal nodes as well as a few leave nodes. A leave node contains the blockchain states, while an internal node owns the hash of its children nodes. For example, Hyperledger employs a bucket-hash tree by hashing the states into a few buckets [23]. Secondly, the history of a block is immutable once the block is attached to the blockchain through a cryptographic hash-pointer chain. The block $n+1$ owns the hash of block $n$, and any change in block $n$ can immediately lead to the invalidity of all the subsequent blocks [24], [25].

## III. AUTHENTICITY OF CSI

In this section, we discuss the authenticity of CSI at each mobile user to detect the users who intentionally advocate their CSI for a larger amount of allocated resource.

### A. AUTHENTICITY OF CSI WITH BLOCKCHAIN CONCENSUS

A blockchain consensus based D2D network is composed of a few mobile users who can be either cellular users or D2D users. Also the network has two blockchains, integrity chain (I-chain) and fraud chain (F-chain), shown in Fig. 2. The CSI of a mobile user needs to be recorded onto a ledger and the replicated ledger must be broadcast through the mobile gateway to all the users in the same cell. Each mobile takes the role of a blockchain node, and these mobile users can employ the consensus protocols and cryptographic schemes to maintain the two blockchains. When a broadcast CSI message arrives at the mobile users, they will use the consensus mechanism to check its authenticity. Once a message is verified to be authentic, this message will be placed on the I-chain by signing it. Otherwise, if more than a half of the blockchain nodes vote the non-authenticity of a message, blockchain nodes will place the messages on the F-chain.

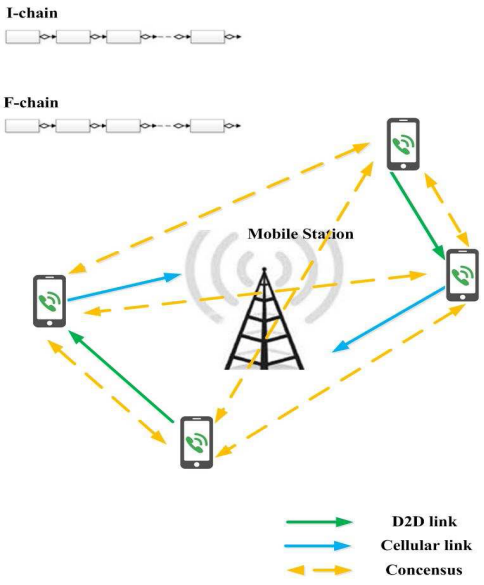


**FIGURE 2.** The Figure shows the blockchain consensus based D2D network.

*Remark 1:* If the CSI of a user appears on the F-chain, the mobile user can be suspected to be a fraud user (Byzantine node).

Such a blockchain consensus has two questions to consider: (1) Whether the blockchain nodes are able to reach an agreement given a few fraud nodes; (2) If the blockchain nodes cannot reach a Byzantine agreement, what additional information is required to detect the fraud users (Byzantine nodes). We can answer the first question by using the property of an asynchronous Byzantine agreement in Section II.D: If the fraction of fraud nodes is strictly less than $\frac{1}{3}$, we can guarantee an asynchronous Byzantine agreement to detect the fraud nodes. However, if the blockchain nodes cannot reach a Byzantine agreement when the fraction of fraud nodes is above $\frac{1}{3}$, we need the additional information to detect the fraud nodes. In the following, we discuss the detection of fraud nodes by predicting the CSI of each node, and with the aid of predicted CSI, the fraud users can be detected by comparing the predicted value and the signed value by a user.

### B. PREDICTION OF CSI WITH DEEP LEARNING NETWORKS

The CSI of a wireless communication link between nodes is relevant to a few factors, including the operating bands, the number of spatial clusters, power angular spectrum per cluster, angular spread, power delay profile, delay spread, Doppler shift, supported channel models, controllable spatial characteristics of BS antennas, etc. [26], 027. By collecting the sample data through the COST 2100 MIMO channel model, we employ the recently most popular conventional neural networks (CNNs) to establish both the encoder and the decoder in view of the spatial correlation between the neurons in adjacent layers. At the encoder end, our CNN transforms the original CSI to a codeword by compressing the original information. At the decoder end, our CNN inversely transforms the codewords to the original CSI. The architecture of the CNN is shown in Fig. 3.

The first layer of the encoder is a convolutional layer of CNN, and the input of this encoder is the original CSI. In this layer, we employ a kernel with the dimension of $3\times3$ to establish two feature maps, and transform the original CSI into a vector using the maps. Afterwards, the vector passes through a fully-connected layer to be transformed into a codeword $c$. The above-mentioned two layers represent the transformation of CSI at the encoder end. Instead of randomly projecting

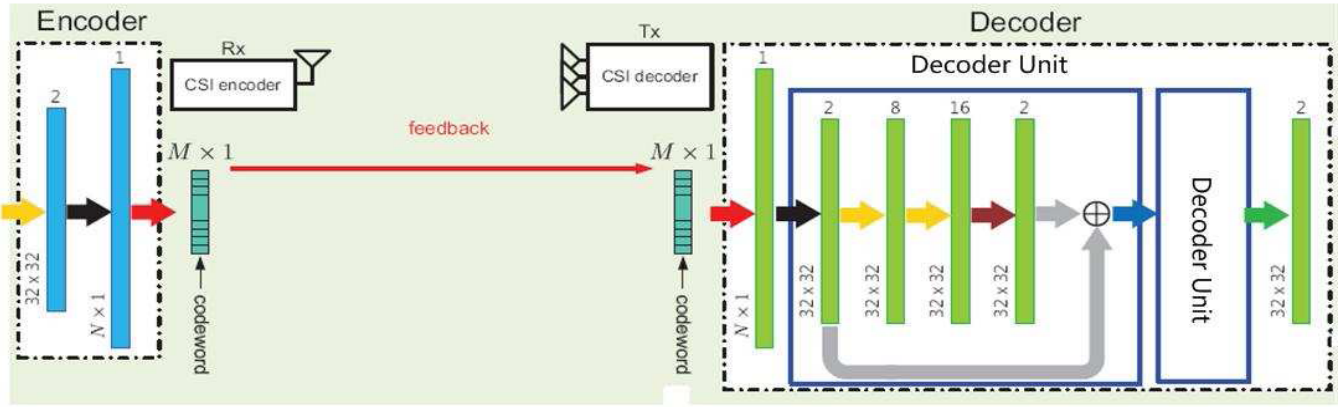


**FIGURE 3.** The Figure illustrates the structure of CNN networks for CSI prediction.

the CSI, our CNN extracts feature maps and transforms the extracted maps into codewords.

After receiving the codeword $s$, we will establish a few layers at the decoder end to reversely transform the codeword back into the CSI. At the first layer of the decoder, we use a fully-connected layer to transform the codeword $s$ in the form of a vector as the input, and its output is an initially estimated CSI matrix with the size of $N_c \times N_t$. The initial output then passes through a few units to continuously adjust the reverse construction of CSI. Each unit is composed of four layers, with the first layer as an input layer and with the other three layers generated by $3 \times 3$ kernels. In the second and third layers, the unit produces 8 and 16 feature maps, respectively, and the final layer produces the inverse construction of CSI. Using the approach of zero padding, we can generate the feature maps via three convolutional layers in the same size of $N_c \times N_t$. At each layer, we employ the rectified linear unit (ReLU) as the activation function.

A unit at the decoder end has two primary features: Firstly, the size of unit output equals to the size of a channel matrix. Instead of using a pooling layer as the implementation of a conventional CNN to reduce its network dimensionality, we avoid this down-sampling operation in the design of our CNN for a better reconstruction of CSI. Secondly, we employ identity-shortcut connections which can transmit data flow to the following layers, and this approach can avoid the vanishing-gradient problem due to the multiple nonlinear transformations. By running several experiments with different parameters, we realize that two units can achieve a fairly good level of performance. Adding a few more units cannot significantly improve the performance of reverse construction of CSI at the cost of increasing the computational complexity. After the CSI is reconstructed by a few units, it will pass through the final convolutional layer with the scaled sigmoid function in the range of [0, 1].

In the process of training our CNN, we use an end-to-end learning at each kernel of the encoder and the decoder. Specifically, we employ the original CSI of user $i$ (i.e. $h_i$) as the input and the predicted CSI as the output of user $i$ as (i.e. $\hat{h}_i$). Both the input and output of CSI are scaled in the range of [0, 1] by normalizing the original CSI. Similar to an autoencoder, we use the adaptive moment estimation (ADAM) algorithm to update the parameters of our CNN, and its loss function is denoted as the mean squared error (MSE) between the actual CSI and the predicted CSI.

*Remark 2:* If the loss function is higher than a threshold, i.e. the predicted CSI is obviously different from the actual CSI, the mobile user can be suspected to be a fraud user (Byzantine node).

## IV. OPTIMAL USER ACCESS CONTROL ALGORITHMS

### A. CHANNEL RATE

In this section, we consider this scenario: multiple cellular users (CU) and D2D users (DU) are randomly distributed in a single cell. Cellular users transmit their data through a base station, while D2D users establish direct links for their data transmission.

The signal to interference and noise ratio (SINR) of $j$th CU (denoted as $\gamma_j^C$) can be expressed as

$$\gamma_j^C = \frac{p_j h_{jj}}{\sum_{l \in D_k} p_l h_{lj} + N_0} \tag{1}$$

where $p_j$ represents the transmission power of CU $j$, $p_l$ represents the transmission power of DU $l$. $h_{jj}$ is the channel gain of the $j$th CU and the base station. $h_{lj}$ represents the channel gain between CU $j$ and DU $l$. $N_0$ represents the power of thermal noise at the receiver. $\sum_{l \in D_k} p_l h_{lj}$ in (1) represents the power of interference from the D2D pairs in $D_k$.

The SINR of $i$th DU (denoted as $\gamma_i^D$) can be expressed as

$$\gamma_i^D = \frac{p_i h_{ii}}{p_k h_{ki} + \sum_{q \in D_k / i} p_q h_{qi} + N_0} \tag{2}$$

where $p_i$ represents the transmission power of DU $i$. $h_{ii}$ is the channel gain of the $i$th DU. $h_{qi}$ represents the channel gain between DU $q$ and DU $i$. $\sum_{q \in D_k / i} p_q h_{qi}$ in (2) represents the

power of interference from CU $q$ and the other D2D pairs in $D_k$ except user $i$.

The channel rate of $j$th CU (denoted as $R_j^C$) can be expressed as

$$R_j^C = log_2(1 + \frac{p_j h_{jj}}{\sum_{l \in D_k} p_l h_{lj} + N_0}) \tag{3}$$

The channel rate of $i$th DU of the cell (denoted as $R_i^D$) can be expressed as

$$R_i^D = log_2(1 + \frac{p_i h_{ii}}{p_k h_{ki} + \sum_{q \in D_k / i} p_q h_{qi} + N_0}) \tag{4}$$

Assuming that the channel experiences small-scaled Rayleigh fading, we have $h_{lj} = \bar{h}_{lj} d_{lj}^{-\alpha}$, where $d_{lj}$ is the distance from user $l$ to user $j$, $\alpha$ is the path-loss exponent, $\bar{h}_{lj}$ is the small-scale fading in a Rayleigh channel. By setting $h_{lj} = \bar{h}_{lj} d_{lj}^{-\alpha}$ for any $l$ and $j$, we can rewrite (3) and (4) as

$$R_j^C = log_2(1 + \frac{p_j \bar{h}_{jj} d_{jj}^{-\alpha}}{\sum_{l \in D_k} p_l \bar{h}_{lj} d_{lj}^{-\alpha} + N_0}) \tag{5}$$

$$R_i^D = log_2(1 + \frac{p_i \bar{h}_{ii} d_{ii}^{-\alpha}}{p_k \bar{h}_{ki} d_{ki}^{-\alpha} + \sum_{q \in D_k / i} p_q \bar{h}_{qi} d_{qi}^{-\alpha} + N_0}) \tag{6}$$

For a pair of cellular users, the distance between a transmitter and a receiver in a Rayleigh fading can be shown as

$$f(D_c) = 2\pi \lambda_c D_c e^{-\pi \lambda_c D_c^2}, \quad 0 < D_c < \infty \tag{7}$$

where $\lambda_c$ denotes the cellular user density, and $D_c$ is the distance between a transmitter and a receiver for a cellular user.

In a D2D network, we assume that the receivers are uniformly located in a region with a radius $D_{max}$, and the cumulative distribution function (CDF) is $F(D_d) = \frac{\pi D_d^2}{\pi D_{max}^2} = \frac{D_d^2}{D_{max}^2}, 0 < D_d < D_{max}$. Then, we can denote the Probability Density Function (PDF) as

$$f(D_d) = \frac{2D_d}{D_{max}^2}, \quad 0 < D_d < D_{max} \tag{8}$$

where $D_d$ is the distance between a transmitter and a receiver for a D2D user.

The number of D2D users who can be supported by a limited amount of bandwidth per unit area is defined as area spectral efficiency, and we can present its detailed definition as

$$S(\gamma) = P_A \lambda_D Pr(\gamma_i^D > \gamma_D) log_2(1 + \gamma_D) \tag{9}$$

where $P_A$ denotes the mean of D2D access probability, $\lambda_D$ denotes the D2D user density, $\gamma_D$ is the minimal SINR requirement for data transmission, $Pr(\gamma_i^D > \gamma_D)$ denotes the mean of D2D success probability.

### B. OPTIMIZATION OF USER-ACCESS STRATEGIES

In the following, we characterize the optimization problem as maximizing the area spectral efficiency $S(\gamma)$, and mathematically, the problem can be expressed as

$$\min_{P_A} S(\gamma) = P_A \lambda_D Pr(\gamma_i^D > \gamma_D) log_2(1 + \gamma_D)$$
$$s.t.\ 0 < P_A \leq 1 \tag{10}$$

*Lemma 3:* For any D2D user $i$ with his/her transmission power $p_i$, we denote the transmission power of D2D user $q$ as $p_q$ and the transmission power of $k$th cellular user as $p_k$. Then, we can characterize $Pr(\gamma_i^D > \gamma_D)$ as

$$Pr(\gamma_i^D > \gamma_D) = e^{-\alpha_1 p_i^{-1} - \alpha_2 p_i^{-\frac{2}{\alpha}}} f(p_i^{-\frac{2}{\alpha}}) \tag{11}$$

where

$$\alpha_1 = N_0 \gamma d_{ii}^{\alpha}, \quad \alpha_2 = P_A \frac{\pi \lambda}{sinc(\frac{2}{\alpha})} (p_q)^{\frac{2}{a}} \gamma^{\frac{2}{a}} d_{ii}^2,$$
$$f(x) = \frac{1}{1 + x(\gamma d_{ii}^{\alpha} p_k)^{\frac{2}{\alpha}} (\frac{128 D_{max}}{45\pi})^{-2}}.$$

*Proof:* According to (2) and the D2D access probability

$$P_A, Pr(\gamma_i^D > \gamma_D)$$
$$= Pr(\frac{p_i h_{ii}}{p_k h_{ki} + \sum_{q \in D_k / i} p_q h_{qi} + N_0} > \gamma_D)$$
$$= Pr(\bar{h}_{ii} > \frac{\gamma_D d_{ii}^{\alpha} (p_k h_{ki} + \sum_{q \in D_k / i} p_q h_{qi} + N_0)}{p_i}).$$

Since $\bar{h}_{ii}$ is in exponential distribution [28], we have

$$Pr(\bar{h}_{ii} > \frac{\gamma_D d_{ii}^{\alpha} (p_k \bar{h}_{ki} + \sum_{q \in D_k / i} p_q \bar{h}_{qi} + N_0)}{p_i})$$
$$= E[e^{-\frac{\gamma_D d_{ii}^{\alpha} (p_k \bar{h}_{ki} + \sum_{q \in D_k / i} p_q \bar{h}_{qi} + N_0)}{p_i}}]$$
$$= e^{-\epsilon N_0} E[e^{-\epsilon p_k \bar{h}_{ki}}] E[e^{-\epsilon \sum_{q \in D_k / i} p_q \bar{h}_{qi}}]$$

where $\epsilon = \frac{\gamma_D d_{ii}^{\alpha}}{p_i}$ and $E[x]$ represents the expectation of $x$.

Also we can further derive $E[e^{-\epsilon p_k \bar{h}_{ki}}]$ and $E[e^{-\epsilon \sum_{q \in D_k / i} p_q \bar{h}_{qi}}]$ as [28]

$$E[e^{-\epsilon p_k \bar{h}_{ki}}] = exp(-\frac{\pi \lambda}{sinc(2/\alpha)} p_q^2 \epsilon^{\frac{2}{\alpha}})$$
$$E[e^{-\epsilon \sum_{q \in D_k / i} p_q \bar{h}_{qi}}] = P_A \frac{1}{1 + \frac{(\epsilon p_k)^{2/\alpha}}{128 D_{max}/45\pi}} \tag{12}$$

Given $\alpha_1 = N_0 \gamma d_{ii}^{\alpha}$, $\alpha_2 = P_A \frac{\pi \lambda}{sinc(\frac{2}{\alpha})} (p_q)^{\frac{2}{a}} \gamma^{\frac{2}{a}} d_{ii}^2$, $f(x) = \frac{1}{1 + x(\gamma d_{ii}^{\alpha} p_k)^{\frac{2}{\alpha}} (\frac{128 D_{max}}{45\pi})^{-2}}$, we have $Pr(\gamma_i^D > \gamma_D) = e^{-\alpha_1 p_i^{-1} - \alpha_2 p_i^{-\frac{2}{\alpha}}} f(p_i^{-\frac{2}{\alpha}})$. The proof follows. ■

According to Lemma 1, the optimization problem of (10) can be transformed into

$$\min_{P_A} S(\gamma) = P_A \lambda_D e^{-\alpha_1 p_i^{-1} - \alpha_2 p_i^{-\frac{2}{\alpha}}} f(p_i^{-\frac{2}{\alpha}}) log_2(1 + \gamma_D)$$
$$s.t.\ 0 < P_A \leq 1 \tag{13}$$

By calculating the derivative of equation (13), we can attain its optimal solution as

$$\frac{d\{P_A\lambda_D e^{-\alpha_1 p_i^{-1}-\alpha_2 p_i^{-\frac{2}{\alpha}}} f(p_i^{-\frac{2}{\alpha}}) log_2(1+\gamma_D)\}}{d\{P_A\}} = 0 \quad (14)$$

*Theorem 4:* The optimal access probability of a D2D user can be expressed as $P_A = min\{\frac{p_i^{\frac{2}{\alpha}}}{Cd_{ii}^2}, 1\}$. *Proof:* Equation (14) is equivalent to

$$\frac{d\{P_A\lambda_D e^{-\alpha_1 p_i^{-1}-\alpha_2 p_i^{-\frac{2}{\alpha}}} f(p_i^{-\frac{2}{\alpha}}) log_2(1+\gamma_D)\}}{d\{P_A\}} = 0 \quad (15)$$

Let $C = (p_q)^{\frac{2}{\alpha}}\gamma^{\frac{2}{\alpha}}\frac{\pi\lambda}{sinc(\frac{2}{\alpha})}$, we have

$$CP_A d_{ii}^2 p_i^{-\frac{2}{\alpha}} = 1 \quad (16)$$

Thus, we can achieve the optimal access probability as

$$P_A = min\{\frac{p_i^{\frac{2}{\alpha}}}{Cd_{ii}^2}, 1\} \quad (17)$$

The proof follows. ■

Based on (17), we can find that the optimum of $P_A$ is determined by the optimal transmission power $p_i$ of a D2D user $i$. Also given the optimal $P_A^*$ and $p_i^*$, we can derive the distance $d_{ii}^*$ as $d_{ii}^* = \sqrt{\frac{(p_i^*)^{\frac{2}{\alpha}}}{CP_A^*}}$ and compute the optimal $\hat{R}_i^D$ using (6).

In consideration of Remark 1 as well as Theorem 2, we propose the algorithm of user access as Algorithm 1.

**Algorithm 1** Algorithm of Optimizing User Access

**while** The CSI of user $i$ does not appear in the F-chain **do**
  Compute $C = (p_q)^{\frac{2}{\alpha}}\gamma^{\frac{2}{\alpha}}\frac{\pi\lambda}{sinc(\frac{2}{\alpha})}$.
  Broadcast the value of $C$ to each of the $N_u$ D2D users.
  **while** $1 \le i \le N_u$ **do**
    Estimate the communication distance $d_{ii}^*$ as well as the $\hat{R}_i^D$ using (4)
    **if** $\hat{R}_i^D > R_D$ **then**
      User $i$ is allowed to access the network.
    **end if**
  **end while**
**end while**
User $i$ is refused to access the network.
Output the results of user access in the network.

## V. SIMULATION RESULTS

In each of the simulation scenarios, we consider a network administrator which can gather the user's information, including the CSI of mobile users, the distance between mobile users, etc. The above-mentioned information can be captured through a few typical devices, such as signal strength meters and global positioning systems (GPS). Also we can operate the proposed algorithms by referring to the information from a typical cellular network, such as universal mobile telecommunication system (UMTS) Network.

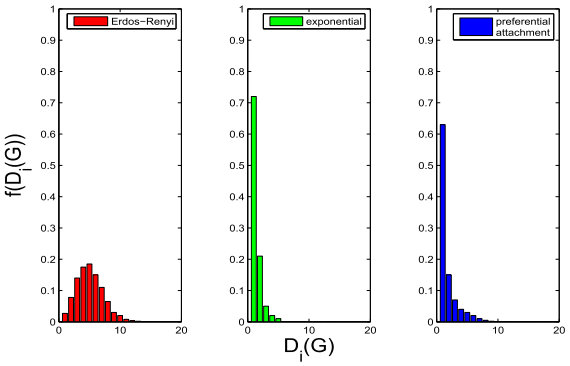


**FIGURE 4.** The Figure illustrates representative vertex degree distributions for Erdös-Rényi (left) with $p = 0.3$, Exponential (center) with $\alpha = 2.5$, and preferential attachment (scale-free) graphs (right) with $\gamma = 15$. $f(D(G))$ is the frequency of the vertex degree $D(G)$.

In the simulation, we consider a few typical empirical networks for D2D underlying cellular networks, and a connection in the network represents a transmitting-receiving pair of users. Specifically, we consider the networks including Erdös-Rényi network, Exponential network and preferential attachment network [29], and we show the distributions of their vertex degrees in Fig. 4. In each network, we consider 50 nodes, and the average distance between terminals is 8 meters. Each terminal is moving with an arbitrary direction at a speed of 2.5m/s (9km/h). When a terminal is a cellular user, his/her average distance to the other users can be characterized as (7). When a terminal is a D2D user, his/her average distance to the other users can be characterized as (8), and the detailed parameters refer to section IV.A. Also we perform about 100000 Matlab-based experiments to present the results.

### A. CHARACTERISTICS OF CHANNEL MODELS

We select a few widely used Rayleigh channel models for mobile users (shown in (7)), which are recommended by ITU-R M.1225 [30]. A typical ITU-R M.1225 model characterizes the testing scenarios in urban and suburban areas where no high-rise buildings are located. Each of the testing scenarios can be modeled as a tapped-delay line. Specifically, the model can be characterized by the number of taps, the time delay of each tap, the average power of each tap, and the Doppler spectrum of each tap. Table 1 identifies the propagation model for each of 6 testing cases, and the primary parameters of this model include: (1) Time-delay spread and its statistical variability; (2) Multipath fading characteristics for the envelope of channels.

### B. CONVERGENCE OF THE PROPOSED ALGORITHM

In this section, we address the convergence rate of our algorithm (Algorithm 1) in various random networks and various testing scenarios. For simplicity, we set the target SINR $\gamma_D$ of each user as 10dB, and investigate the convergence rate to the optimum of spectral efficiency in different networks.

**TABLE 1. Parameters of Rayleigh channel models in ITU-R recommendation M.1225 [30].**

| Tap | Relative delay (ns) | Average power (dB) | Doppler spectrum |
|---|---|---|---|
| 1 | 0 | 0.0 | Rayleigh |
| 2 | 310 | -1.0 | Rayleigh |
| 3 | 710 | -9.0 | Rayleigh |
| 4 | 1090 | -10.0 | Rayleigh |
| 5 | 1730 | -15.0 | Rayleigh |
| 6 | 2510 | -20.0 | Rayleigh |

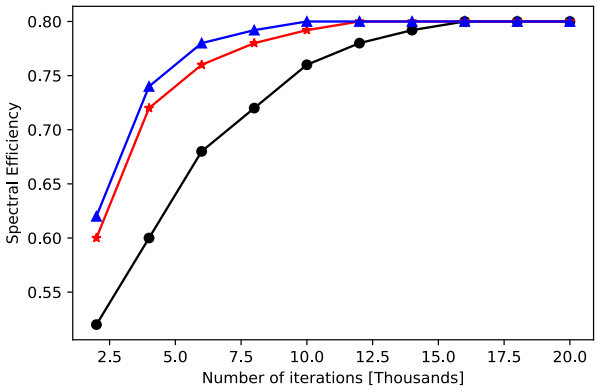


**FIGURE 5. The Figure illustrates the rate of convergence to the optimum of our algorithm under different random networks. Blue line with '∆' represents Exponential network; Red line with '·' represents preferential attachment (scale-free) network; Dark line with 'o' represents Erdös-Rényi network.**

As shown in Fig. 5, our algorithm in the networks with highly concentrated transmitting/receiving nodes (e.g., Exponential network) is capable of converging to the optimum at a high speed, while the algorithm in the networks without highly concentrated transmitting/receiving nodes (e.g., Erdös-Rényi network) slowly converges to the optimum. Indeed, the algorithm in the Exponential network achieves the optimum after 9000 iterations, while its counterpart achieves the optimum after 15000 iterations in the Erdös-Rényi network.

A highly-concentrated user is easy to establish his/her transmitting/receiving pairs with the users in the Erdös-Rényi network, and thus a data transmission is easily impacted by the other transmissions. However, in the Exponential network, a mobile user builds up transmitting/receiving pairs with few users, and thus he/she suffers a lower level of interference from the others.

### C. OPTIMAL SPECTRAL EFFICIENCY OF PROPOSED ALGORITHM

In this section, we compare the optimal spectral efficiency with various algorithms, including the exhaustive-search algorithm, the proposed algorithm, the Q-learning algorithm, and the random-search algorithm.

Fig. 6 shows the optimal spectral efficiency in a network with various algorithms. Fig. 6 illustrates that our proposed algorithm can achieve a higher level of spectral efficiency than the Q-learning algorithm and the random-search algorithm. As expected, the exhaustive-search algorithm can achieve the highest spectral efficiency, but it cannot be applied in reality due to a large consumption of running time.

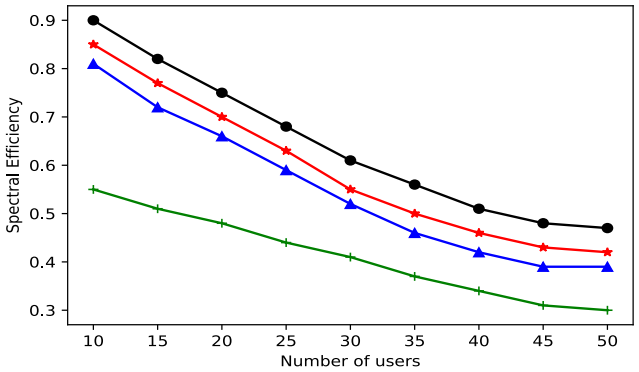


**FIGURE 6. The Figure investigates the optimal spectral efficiency with various algorithms. Dark line with 'o' represents the exhaustive-search algorithm; Red line with '⋆' represents the proposed algorithm; Blue line with '∆' represents the Q-learning algorithm; Green line with '+' represents the random-search algorithm.**

### D. IMPACT OF CSI AUTHENTICITY

In the following, we address the benefits of using the blockchain consensus protocol to verify the authenticity of CSI. If the CSI is not checked, a few users may advocate a higher value of CSI, and unfairly gain a higher probability of staying in the network. However, these users cannot achieve the expected channel data rate, and the network performance will be actually degraded. In the following, we assume that each mobile user has a probability of 10% to advocate a higher value of CSI. Fig. 7 shows the comparison of spectral efficiency by our algorithm and by the algorithm without verifying the authenticity of CSI. Fig. 7 implies that our proposed algorithm can dramatically improve the spectral efficiency when using the blockchain consensus protocol to verify the authenticity of CSI.

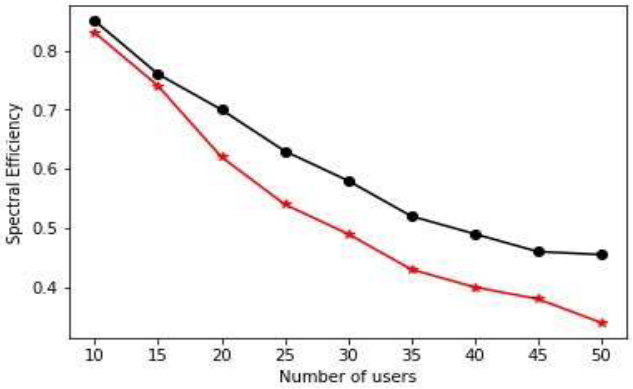


**FIGURE 7. The Figure shows the impact of verifying the CSI authenticity on the spectral efficiency. Dark line with 'o' represents the proposed algorithm; Red line with '⋆' represents the algorithm without verifying the CSI authenticity.**

## VI. CONCLUSION

We consider the scenario of optimizing spectral efficiency in a D2D assisted cellular network for mobile applications, in which a user can establish a D2D connection with the other users. In view of checking the authenticity of CSI among users, we address the optimization of spectral efficiency by proposing a novel algorithm to control the user access. A few primary inferences drawn include

- Our proposed algorithm can dramatically improve the spectral efficiency than the Q-learning algorithm in [31], which is the most widely-used user-access control algorithm. Also our proposed algorithm can reduce the convergence time than the exhaustive-search algorithm, which can achieve the optimal offline user-access strategy.
- Our proposed algorithm can dramatically improve the spectral efficiency than without using the blockchain consensus protocol to check the authenticity of CSI.
- Under the networks with highly concentrated transmitting/receiving pairs, our proposed algorithm can converge to the optimum at a higher rate than under the networks in which transmitting/receiving pairs are uniformly distributed among wireless users.

We will generalize our research to a non-cooperative scenario for mobile users, and study the design of a optimization strategy in a scenario when the users are non-cooperative and each of the users can refuse to accept the access of a network.

## REFERENCES

[1] D. Lin, Y. Tang, and A. V. Vasilakos, "User-priority-based power control in D2D networks for mobile health," *IEEE Syst. J.*, to be published. [Online]. Available: http://ieeexplore.ieee.org/document/7879233/
[2] D. Lin, Y. Tang, Y. Yao, and A. V. Vasilakos, "User-priority-based power control over the D2D Assisted Internet of vehicles for mobile health," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 824–831, Jun. 2017.
[3] J. Gu, S. J. Bae, B.-G. Choi, and M. Y. Chung, "Dynamic power control mechanism for interference coordination of device-to-device communication in cellular networks," in *Proc. 3rd Int. Conf. Ubiquitous Future Netw.*, 2011, pp. 71–75.
[4] C.-H. Yu, K. Doppler, C. B. Ribeiro, and O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2752–2763, Aug. 2011.
[5] N. Lee, X. Lin, J. G. Andrews, and R. W. Heath, Jr., "Power control for D2D underlaid cellular networks: Modeling, algorithms, and analysis," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 1–13, Jan. 2015.
[6] Z. Chen and M. Kountouris, "Distributed SIR-aware opportunistic access control for D2D underlaid cellular networks," in *Proc. IEEE Global Commun. Conf.*, Dec. 2014, pp. 1540–1545.
[7] P. Sun, K. G. Shin, H. Zhang, and L. He, "Transmit power control for D2D-underlaid cellular networks based on statistical features," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4110–4119, May 2017.
[8] T. T. A. Dinh, J. Wang, G. Chen, L. Rui, B. C. Ooi, and K.-L. Tan, "BLOCKBENCH: A framework for analyzing private blockchains," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, 2017, pp. 1085–1100.
[9] J. Wang, L. Gao, A. Dong, S. Y. Guo, H. Chen, and X. Wei, "Block chain based data security sharing network architecture research," *J. Comput. Res. Develop.*, vol. 54, no. 4, pp. 742–749, 2017.
[10] D. Kraff, "Difficulty control for blockchain-based consensus systems," *Peer Netw. Appl.*, vol. 9, no. 2, pp. 397–413, 2016.
[11] K. Fanning and D. P. Centers, "Blockchain and its coming impact on financial services," *J. Corporate Accounting Finance*, vol. 27, no. 5, pp. 53–57, 2016.
[12] C. Copeland and H. Zhong. (2017). *Tangaroa: A Byzantine Fault Tolerant Raft*. [Online]. Available: https://github.com/chrisnc/tangaroa
[13] M. Vukolic, "The quest for scalable blockchain fabric: Proof-ofwork versus BFT replication," in *Proc. Int. Workshop Open Problems Netw. Secur.*, 2015, pp. 112–125.
[14] L. Luu, V. Narayanan, C. Zhang, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2016, pp. 17–30.
[15] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies," in *Proc. 26th ACM Symp. Oper. Syst. Principles*, 2017, pp. 51–68.
[16] JPMorgan. (2017). *Enterprise-Ready Distributed Ledger and Smart Contract Platforms*. [Online]. Available: https://github.com/jpmorganchase/quorum
[17] Hydrachain. (2017). *Permissioned Distributed Ledger Based on Ethereum*. [Online]. Available: https://github.com/HydraChain/hydrachain
[18] Openchain. (2017). *Enterprise-Ready Blockchain*. [Online]. Available: https://github.com/openchain
[19] Tendermint. (2017). *Blockchain App Development Simplified*. [Online]. Available: http://tendermint.com/
[20] Dfinity. (2017). *Commercial Use Cases*. [Online]. Available: https://dfinity.network/
[21] Ripple. (2017). *Commercial Use Cases*. [Online]. Available: https://ripple.com
[22] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, "The blockchain-based digital content distribution system," in *Proc. IEEE 5th Int. Conf. Big Data Cloud Comput.*, Dalian, China, Aug. 2016, pp. 187–190.
[23] S. Fujimura, H. Watanabe, and A. Nakadaira, T. Yamada, A. Akutsu, and J. J. Kishigami, "BRIGHT: A concept for a decentralized rights management system based on blockchain," in *Proc. 5th IEEE Int. Conf. Consum. Electron.*, Berlin, Germany, Sep. 2016, pp. 345–346.
[24] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, San Jose, CA, USA, May 2015, pp. 180–184.
[25] F. Bonnet, X. Defago, T. D. Nguyen, and M. Potop-Butucaru, "Tight bound on mobile Byzantine agreement," *Theor. Comput. Sci.*, vol. 609, no. 2, pp. 361–373, 2016.
[26] C. K. Wen, W. T. Shih, and S. Jin, "Deep learning for massive MIMO CSI feedback," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 748–751, Oct. 2018.
[27] H. Jiang and E. Learned-Miller, "Face detection with the faster R-CNN," in *Proc. IEEE Int. Conf. Autom. Face Gesture Recognit.*, May/Jun. 2017, pp. 650–657.
[28] 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.
[29] J. Corbo and D. Lin, "Optimal pricing with positive network effects: The big benefits of just a little discrimination," ICIS, Orlando, FL, USA, 2012. [Online]. Available: https://aisel.aisnet.org/icis2012/proceedings/DigitalNetworks/20/
[30] M. Bashar, A. Burr, K. Haneda, and K. Cumanan, "User scheduling with COST 2100 channel model for massive MIMO networks," *IET Microw. Antennas Propag.* vol. 12, no. 11, pp. 1786–1792, 2018.
[31] W. Lu, Y. Gong, X. Liu, J. Wu, and H. Peng, "Collaborative energy and information transfer in green wireless sensor networks for smart cities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1585–1593, Apr. 2018.

**DI LIN** received the Ph.D. degree from McGill University in 2013. From 2013 to 2014, he was a Research Associate with Ottawa University. He is currently an Associate Professor with the department of the University of Electronic Science and Technology of China. He has published over 20 papers in refereed journals and conferences in these areas. His research interests include wireless communications and its applications in health and social network analysis.

**YU TANG** received the Ph.D. degree in computer science from George Washington University in 2008. He was a Lead Engineer with DRS Electronic Systems, Raytheon, for 10 years. He is currently a Professor with the department of the University of Electronic Science and Technology of China. His research interests include distributed computation in wireless networks and intelligent routing algorithms. He has published over 20 papers in refereed journals and conferences in these areas.