Secure Transmission Scheme Based on the Artificial Noise in D2D-Enabled Full-Duplex Cellular Networks

Chen Yajun[1*], Yi Ming[1], Zhong Zhou[1], Ma Keming[1], Huang Kaizhi[1], Ji Xinsheng[1,2,3]
1. China National Digital Switching System Engineering and Technological R&D Center, Zhengzhou 450002, P.R. China
2. National Mobile Communications Research Laboratory, Southeast University, Nanjing 211189, P.R. China;
3. National Engineering Lab for Mobile Networking Security, Beijing 100876, P.R. China
[e-mail: chenyajun_cool@126.com]
*Corresponding author: Chen Yajun

Received December 11, 2018; revised February 20, 2019; accepted April 8, 2019; published October 31, 2019

Abstract

In this paper, a secure transmission scheme based on the artificial noise is proposed for D2D communications underlaying the full-duplex cellular network, and a secure power allocation scheme to maximize the overall secrecy rate of both the cellular user and D2D transmitter node is presented. Firstly, the full-duplex base station transmits the artificial noise to guarantee the secure communications when it receives signals of cellular uplinks. Under this secure framework, it is found that improving the transmission power of the cellular user or the D2D transmitter node will degrade the secrecy rate of the other, although will improve itself secrecy rate obviously. Hence, a secure power allocation scheme to maximize the overall secrecy rate is presented subject to the security requirement of the cellular user. However, the original power optimization problem is non-convex. To efficiently solve it, we recast the original problem into a convex program problem by utilizing the proper relaxation and the successive convex approximation algorithm. Simulation results evaluate the effectiveness of the proposed scheme.

Keywords: D2D Communications, Artificial Noise, Secrecy Capacity, Successive Convex Approximation, Secure Power Allocation

This work is supported in part by the National Keypoint Research and Invention Program(2017YFB0801903); the open research fund of National Mobile Communications Research Laboratory, Southeast University (No.2013D09) and National Natural Science Foundation of China under Grants No. 61521003, 61871404, 61701538.

http://doi.org/10.3837/tiis.2019.10.006 **ISSN : 1976-7277**

1. Introduction and Related Work

In recent years, D2D-enabled cellular networks have attracted widely attentions due to their advantages including increasing spectrum efficiency and cellular capacity, offloading traffic[1-3]. Consequently, D2D communications are emerging as a potentially important technology component for 5G to satisfy ever-increasing demand for wireless services. However, as well as other wireless systems, D2D communications are more vulnerable to being eavesdropped by unauthorized users (Eavesdroppers) due to the inherent openness of the wireless channel.

To overcome this issue, physical-layer security (PLS) [4-9] has been recently proposed to employ the opening characters of wireless channels to achieve secret communication, resulting in achieving "absolute" security from the concept of information theory. There has been some work to exploit PLS for D2D communications. Security threats were analyzed for D2D communications underlaying LTE-A cellular networks in [10]. D2D mode having more advantages in reducing the interruption probability was depicted in [11]. The interference caused by D2D communications against Eves was exploited in [12-14]. To the best of our knowledge, the security requirement of D2D pairs remains elusive. The authors take the interference caused by D2D links against eavesdroppers in [12-14]. Unfortunately, the eavesdropper may have the most powerful ability to distinguish superimposition signals by successive interference cancellation [15]. The secure uplink communication has not been studied in this worst case, which is even harder to achieve due to the uplink limitations, such as terminals having no multi-antennas. But the downlink has a rich collection of resources, especially for 5G with the full-duplex and Massive MIMO (multiple-input multiple-output). So, we need to fully exploit that how we utilize the downlink redundant to guarantee the secure uplink communication.

On the other hand, the full-duplex transmission, which can transmit and receive signals simultaneously on the same frequency band, has received much attention recently [16-17]. Breakthroughs in self-interference mitigation techniques [18-19] make the full-duplex transmission being attracted tremendous attention. In [20-22], the authors exploit the full-duplex transmission to guarantee the secure communication in different scenarios.

Inspired by the prior works, an artificial noise-enabled secure transmission scheme is proposed for D2D-enabled cellular networks, which can guarantee the secure communication for both cellular users and D2D users simultaneously. The full-duplex base station transmits the artificial noise when it receives signals of cellular uplinks to guarantee their secure communications for both cellular links and D2D links. Furthermore, a secure power allocation scheme to maximize the overall secrecy rate is presented subject to the security requirement of cellular users. Unfortunately, the original power optimization problem is non-convex. To efficiently solve it, we recast the original problem into a convex program by utilizing proper relaxation and the successive convex approximation algorithm. Simulation results evaluate the effectiveness of the proposed scheme. Specially, our contributions can be summarized as follows:

1) In order to fully exploit that how we utilize the downlink redundant to guarantee the secure uplink communication, we propose an artificial noise-enabled secure transmission scheme for D2D-enabled cellular networks, which can guarantee the secure communication for different users.

2) Furthermore, based on the proposed secure transmission scheme, we can find that improving the transmission power of cellular users or D2D pairs will degrade the secrecy rate of the other kind user, although it will improve itself secrecy rate obviously. Hence, we formulate a secure power allocation problem, which maximizes the overall secrecy rate subject to the security requirement of cellular users.

3) Unfortunately, the original power optimization problem is non-convex. To efficiently solve it, we recast the original problem into a convex program by utilizing proper relaxation and the successive convex approximation algorithm. Simulation results evaluate the effectiveness of the proposed scheme.

We use the following notations in this paper. Bold letters denote matrices or vectors. We use $CN\left(\mu,\sigma^2\right)$ to denote the circularly symmetric complex Gaussian noise with mean μ and variance σ^2. $[\bullet]^+$ is the maximum value compared with zero (i.e., $[\bullet]^+ = \max\{\bullet,0\}$). $\|\bullet\|$ returns the Frobenius norm of a vector or matrix. $|\bullet|$ denotes the mold of a complex number. $\nabla f(x)$ and $\nabla^2 f(x)$ are the gradient and Hess matrix of the function $f(x)$, respectively. We write $\triangleq$ for equality in definition.

2. System Model and Problem Formulation

2.1 System Model

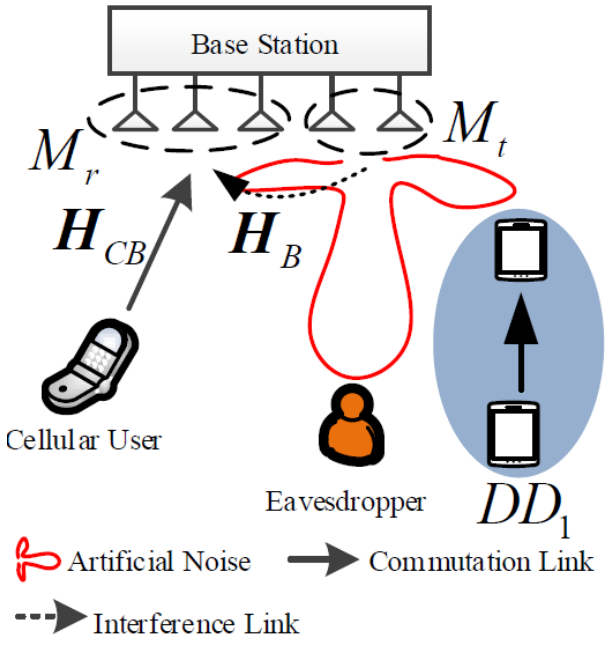

Fig. 1. System Model

The proposed system model for D2D secure communication underlaying full-duplex cellular networks is shown in **Fig. 1**, where there is a base station, a traditional cellular user, a D2D pair and an eavesdropper Eve. The D2D pair DD_1 is comprised of a transmitter node T and an intended destination node D. The service of the cellular user is provided through the base station. Meanwhile, one D2D pair attempts to use the same cellular resource to establish

the direct link between its transmitter node and its destination node. The eavesdropper Eve tries to overhear the signals of all users. It is assumed that Eve works in a passive way. The full-duplex base station is equipped with multi-antennas for sending and receiving signals simultaneously. Furthermore, it is assumed that the number of downlink transmission antennas must satisfy $N_t \geq \max\{N_r, 2\}$, where N_r is the reception antennas number. All the users are equipped with single antenna. We allow at most one D2D user to share the same channel with the given cellular user. Let p_1 and p_2 be the transmission power of the cellular user and D2D pair, respectively. Then, we denote $\boldsymbol{P} = [p_1, p_2]^T$ for simplicity.s

Furthermore, in order to achieve secure communication for legitimate users, the full-duplex base station will transmit the artificial noise to disturb the passive Eve [23], while receiving the uplink cellular signals.

The received signals at the base station, the destination node D of the D2D pair and Eve can be, respectively, represented as:

$$y_B = \sqrt{p_1}\boldsymbol{H}_{CB}\boldsymbol{x}^c + \sqrt{p_2}\boldsymbol{H}_{DB}x^d + \sqrt{\rho P_B}\boldsymbol{H}_B\boldsymbol{w}\boldsymbol{s} + n_b \tag{1}$$

$$y_D = \sqrt{p_2}H_D x^d + \sqrt{p_1}H_{CD}x^c + \sqrt{P_B}\boldsymbol{H}_{BD}\boldsymbol{w}\boldsymbol{s} + n_d \tag{2}$$

$$y_E = \sqrt{p_1}H_{CE}x^c + \sqrt{p_2}H_{DE}x^d + \sqrt{P_B}\boldsymbol{H}_{BE}\boldsymbol{w}\boldsymbol{s} + n_e \tag{3}$$

where $\boldsymbol{H}_{CB}$、H_{CD}、H_D、$\boldsymbol{H}_{BD}$、$\boldsymbol{H}_{DB}$、H_{CE}、H_{DE}、$\boldsymbol{H}_B$ and $\boldsymbol{H}_{BE}$ denote the channel gains for $C \to B$, $C \to D$, $T \to D$, $B \to D$, $T \to B$, $C \to E$, $T \to E$, $B \to B$, $B \to E$, respectively. P_B is the artificial noise power of the full-duplex base station. n_c, n_d and n_e denote the additive gaussian noise at the base station, the destination node D and Eve with the distribution $CN(0, \delta^2)$, respectively. x^c and x^d are the confidential information for the legitimate base station and destination node. $\boldsymbol{s}$ is a noise vector artificially generated by the base station to confuse Eve. $\boldsymbol{w}$ is the transmit weight vector corresponding to $\boldsymbol{s}$. The effect of the self-interference suppression is modeled as the parameter $\rho(\rho \in [0,1])$, especially, where $\rho = 0$ refers to the ideal case with no self-interference. In order to avoid the interference caused by the artificial noise, the artificial noise is designed within the null space of the joint channels, which could be denoted as $[\boldsymbol{H}_B, \boldsymbol{H}_{BD}]\boldsymbol{w}\boldsymbol{s} = \boldsymbol{0}$. That is to say, there is no self-interference generated by the artificial noise for base station.

We consider a worst case where the eavesdropper has powerful multi-user decidability. In other words, the eavesdropper could distinguish every data stream. Thus, they could subtract the interference induced by the information-bearing signals by employing multiuser detection techniques, just as done in [15]. Hence, there is no other interference when Eve chooses one of the received signals to overhear in this worst case, the achievable secrecy rates for the cellular user and the D2D tranmitter are given in (4) and (5), respectively:

$$C_C = \left[\log_2\left(1 + \frac{p_1\left\|\boldsymbol{H}_{CB}\right\|^2}{\delta^2 + p_2\left\|\boldsymbol{H}_{DB}\right\|^2}\right) - \log_2\left(1 + \frac{p_1\left|H_{CE}\right|^2}{\delta^2 + P_B\left\|\boldsymbol{H}_{BE}\right\|^2}\right)\right]^+ \tag{4}$$

$$C_D = \left[\log_2\left(1 + \frac{p_2\left|H_{DD}\right|^2}{\delta^2 + p_1\left|H_{CD}\right|^2}\right) - \log_2\left(1 + \frac{p_2\left|H_{DE}\right|^2}{\delta^2 + P_B\left\|\boldsymbol{H}_{BE}\right\|^2}\right)\right]^+ \tag{5}$$

In the practical system, the channel state information of the passive eavesdropper is very difficult to be obtained. Hence, we use the ergodic secrecy rates of the cellular users and D2D

users to characterize their respective security performances, which are denoted as $\overline{C}_C=\mathbb{E}_{H_{CE},\boldsymbol{H}_{BE}}\{C_C\}$ and $\overline{C}_D=\mathbb{E}_{H_{DE},\boldsymbol{H}_{BE}}\{C_D\}$. Furthermore, the sum ergodic secrecy rate is used to judge the security performance of this hybrid network in the above scenario.

2.2 Problem Formulation

The sum ergodic secrecy rate can be expressed as:

$$C=\overline{C}_C+\overline{C}_D \tag{6}$$

When the secrecy rates in (4), (5) are positive values, substituting (4) and (5) into (6), we can obtain:

$$\begin{aligned} C=&\log_2\left(1+\frac{p_1\left\|\boldsymbol{H}_{CB}\right\|^2}{\delta^2+p_2\left\|\boldsymbol{H}_{DB}\right\|^2}\right)-\mathbb{E}_{H_{CE},\boldsymbol{H}_{BE}}\left\{\log_2\left(1+\frac{p_1\left|H_{CE}\right|^2}{\delta^2+P_B\left\|\boldsymbol{H}_{BE}\right\|^2}\right)\right\}\\ &+\log_2\left(1+\frac{p_2\left|H_D\right|^2}{\delta^2+p_1\left|H_{CD}\right|^2}\right)-\mathbb{E}_{H_{DE},\boldsymbol{H}_{BE}}\left\{\log_2\left(1+\frac{p_2\left|H_{DE}\right|^2}{\delta^2+P_B\left\|\boldsymbol{H}_{BE}\right\|^2}\right)\right\} \end{aligned} \tag{7}$$

From (7), we can find that their transmission power will directly determine their security performance. For instance, improving the transmission power of the cellular user will improve itself secrecy rate obviously. However, it will degrade the ergodic secrecy rate of the D2D pair. It will be the same when the D2D transmission power is improved. Therefore, each user should carefully choose its transmission power to maximize the sum secrecy rate for this hybrid network. On the other hand, the interference from D2D links reused the same resource with cellular users will degrade the communication quality of the cellular user. Hence, we must firstly guarantee the performance of the cellular user before allowing the D2D transmitter node to reuse its same resource. In summary, to maximize the sum secrecy rate, the power optimization problem can be formulated as:

$$\begin{aligned} &\max_{\boldsymbol{P}}\ C\\ &s.t\\ &\quad \mathrm{C1}: C_C\geq\beta\\ &\quad \mathrm{C2}: 0\leq p_1\leq P_1^{\max}\\ &\quad \mathrm{C3}: 0\leq p_2\leq P_2^{\max} \end{aligned} \tag{8}$$

Since the function $\log(1+x)$ is non-convex, the optimization problem in (8) is a non-convex programming problem for both p_1 and p_2, which is difficult to directly derive the global optimal solution. In order to get the optimal transmission power, we must firstly convert the original problem to an equivalent convex optimization problem which would be easy to be solved. To solve the non-convex programming problem in (8), next we will firstly convert it to be a concave function.

3. Joint Power Optimization

Next, we firstly design a suboptimal solution to handle the non-convex power optimization problem in (8) with the appropriate relaxation and the SCA algorithm [18]. After converting the optimization problem in (8) to two strictly convex optimization problems, we further present a joint iterative power optimization algorithm for both the cellular user and D2D transmitter node.

3.1 SCA Algorithm

Firstly, we briefly introduce its core idea of the SCA algorithm, which could convert the non-convex constraint in the original problem to the conservative convex constraint. Then, the original problem can be solved by the converted convex problem recursively. The details could be found in [24]. Here, we just explain the SCA algorithm mathematically.

It is assumed that there is a non-convex constraint $g(\psi) \le 0$ in an optimization problem. Now we mainly need to change the non-convex constraint $g(\psi) \le 0$ with the SCA algorithm to solve the original problem as follow. Firstly, it assumed that we find a convex upper bound function of $g(x)$, denoted as $G(\psi,\varsigma)$, where the parameter ς is given. In addition, the convex upper bound function should hold that when $\varsigma = \varphi(\psi)$:

$$\begin{aligned} g(\psi) &= G(\psi,\varphi(\psi)) \\ \nabla g(\psi) &= \nabla G(\psi,\varphi(\psi)) \end{aligned} \tag{9}$$

where $\nabla g(\psi)$ denotes the gradient of $g(\psi)$. Then, in $n-th$ recursive, the non-convex function $g(\psi)$ is replaced by the convex function $G\left(\psi,\varsigma^{(n)}\right)$. That is to say, we use the convex constraints $G(\psi,\varsigma) \le 0$ to replace the original non-convex constraints $g(\psi) \le 0$. In the $n-th$ recursive, the parameter $\varsigma^{(n)}$ updates with the optimal solution $\psi^{(n-1)}$ in the $(n-1)-th$ recursive, i.e. : $\varsigma^{(n)} = \varphi\left(\psi^{(n-1)}\right)$.

3.2 Power Optimization for the Cellular User

To optimize the transmission power of the cellular user, we fistly assume the one of the D2D transmitter node is a constant. For simplicity, we define $A_1 = \|\boldsymbol{H}_{CB}\|^2$, $B_1 = |H_{CE}|^2$, $C_1 = \|\boldsymbol{H}_{DB}\|^2$, $A_2 = |H_D|^2$, $B_2 = |H_{DE}|^2$, $C_2 = |H_{CD}|^2$. Thus, (7) can be rewritten as:

$$C = \log_2\left(1+\frac{p_1 A_1}{\delta^2 + p_2 C_1}\right) - \log_2\left(1+\frac{p_{n,1} B_1}{\delta^2 + D_1}\right) + \log_2\left(1+\frac{p_2 A_2}{\delta^2 + p_1 C_2}\right) - \log_2\left(1+\frac{p_2 B_2}{\delta^2 + D_1}\right) \tag{10}$$

Then, the first constraint C1 in (8) can be rewritten as:

$$\log_2\left(1+\frac{p_1 A_1}{\delta^2 + p_2 C_1}\right) - \log_2\left(1+\frac{p_1 B_1}{\delta^2 + D_1}\right) \ge \beta \tag{11}$$

We can obtain:

$$p_1 \ge \frac{\left(2^{\beta}-1\right)\left(\delta^2 + p_2 \bullet C_1\right)\left(\delta^2 + D_1\right)}{A_1 \bullet \left(\delta^2 + D_1\right) - 2^{\beta} \bullet B_1 \bullet \left(\delta^2 + p_2 \bullet C_1\right)} \tag{12}$$

From (12), we can see that it is a convex constraint. Next, we must convert the function in (10) to be a concave one, whose difficulty is how to relax the function $\log_2(1+z)$ where $z \ge 0$. A number of lower-bounds having the concave property could relax $\log_2(1+z)$ to be a concave function with respect to z. However, the tighter of the lower-bound, the faster the lower-bound converges to a KKT point of the original problem. We need to derive and apply the tightest relaxation of C to obtain the optimal solution for the optimization problem. The following **Lemma 1**[25] gives the tightest lower-bound of the function

$\log_2(1+z)$.

Lemma1： The very tight lower-bound of $\log_2(1+z)$ where $z \geq 0$ can be given by

$$\alpha \log_2 z + \beta \quad . \tag{13}$$

where the lower-bound coefficients α and β are denoted as:

$$\begin{cases} \alpha = \dfrac{z_0}{1+z_0} \\ \beta = \log_2(1+z_0) - \dfrac{z_0}{1+z_0}\log_2 z_0 \end{cases} \tag{14}$$

where $z_0 \in [0,\infty)$ is a positive real number. We can find that the lower-bound $\alpha \log_2 z + \beta$ equals to $\log_2(1+z)$ at $z = z_0$. More details, such the update of the lower-bound coefficients, are discussed in [25].

Based on **Lemma1**, we can get the tightest lower-bound of the third term in (10) as follows:

$$G_1(p_1) \approx \frac{1}{\ln 2}\left(\alpha_1 \ln(A_2 \bullet p_2) - \alpha_1 \ln\left(\delta^2 + C_2 \bullet p_1\right) + \beta_1 \ln 2\right) \tag{15}$$

Then, using the logarithmic change of the variable $\overline{p}_1 = \ln(p_1)$, we can convert the $G_1(p_1)$ to the log-sum-exp function denoted by $\overline{p}_1$, as follows:

$$G_1(\overline{p}_1) \approx \frac{1}{\ln 2}\left(\alpha_1 \ln(A_2 \bullet p_2) - \alpha_1 \ln\left(\delta^2 + C_2 \bullet e^{\overline{p}_1}\right) + \beta_1 \ln 2\right) \tag{16}$$

$G_1(\overline{p}_1)$ is non-convex since $\overline{p}_1 = \ln(p_1)$ is strictly convex. When the third term in (10) is replaced by (16), we assume that the objective function is denoted as $\overline{C}$.

On the other hand, when $\overline{p}_1 = \ln(p_1)$, we can convert the second term in (10) to $-\log_2\left(1+\dfrac{e^{\overline{p}_1}B_1}{\delta^2 + D_1}\right)$, which is also non-convex function and the fourth term has no variable p_1. Hence, the difficulty to convert the original problem to be a convex problem is how we convert the first term in (10) to a non-convex function.

The first term in (10) can be expressed as by adding the auxiliary variable η:

$$\begin{aligned} &\max_{p_1} \quad \overline{C} \\ &s.t \\ &\quad \text{C1}: p_1 \geq \frac{\left(2^{\beta}-1\right)\left(\delta^2 + p_2 \bullet C_1\right)\left(\delta^2 + D_1\right)}{A_1 \bullet \left(\delta^2 + D_1\right) - 2^{\beta} \bullet B_1 \bullet \left(\delta^2 + p_2 \bullet C_1\right)} \\ &\quad \text{C2}: 0 \leq p_1 \leq P_1^{\max} \\ &\quad \text{C3}: \log_2\left(1+\frac{p_1 A_1}{\delta^2 + p_2 C_1}\right) \geq \eta, (\eta \geq 0) \end{aligned} \tag{17}$$

where the C3 constraint is a non-convex constraint, which also can be expressed as $p_1 - \dfrac{\delta^2 + p_2 C_1}{A_1}\left(2^{\eta}-1\right) \leq 0$. We denote it as $F(p_1,\eta) = p_1 - \dfrac{\delta^2 + p_2 C_1}{A_1}\left(2^{\eta}-1\right)$, which is a non-convex function because its Hesse matrix is a negative semidefinite one,

i.e., $\nabla^2 F(p_1,\eta) \le 0$. Therefore, we deal with it SCA algorithm.

The first-order Taylor expression of $f(\eta)=\left(2^{\eta}-1\right)$ at ξ is:

$$\begin{aligned} f_1(\eta,\xi) &\triangleq f(\xi)+\nabla f(\xi)(\eta-\xi) \\ &= 2^{\xi}\left(1+\ln 2 \bullet (\eta-\xi)\right)\text{-}1 \end{aligned} \tag{18}$$

We can easily get $f_1(\eta,\xi)-f(\xi)\le 0$ because of $\nabla^2 f(\eta)\ge 0$, $F_1(p_1,\eta)=p_1-\frac{\delta^2+p_2C_1}{A_1}\bullet\left[2^{\xi}\left(1+\ln 2\bullet(\eta-\xi)\right)\text{-}1\right]$ is the convex upper bound of $F(p_1,\eta)$. On the other hand, it can be verified that $F_1(p_1,\eta)$ hold the following equation when $p_1=\xi$:

$$\begin{aligned} F(p_1,\eta) &= F_1(p_1,\eta,\xi) \\ \nabla F(p_1,\eta) &= \nabla F_1(p_1,\eta,\xi) \end{aligned} \tag{19}$$

Thus, in the $l-th$ recursion, the C3 constraint in (17) can be replaced by the following convex constraint condition:

$$p_1-\frac{\delta^2+p_2C_1}{A_1}\bullet\left[2^{\xi^{(l)}}\left(1+\ln 2\bullet\left(\eta-\xi^{(l)}\right)\right)\text{-}1\right]\le 0 \tag{20}$$

where $\xi^{(l)}=p_1^{(l-1)}$ and $p_1^{(l-1)}$ is represented as the local optimal solution of the transmission power for the cellular user in the $(l-1)-th$ recursive. Thus, the suboptimization problem (17) can be rewritten as:

$$\begin{aligned} &\max_{p_1} \ \overline{C} \\ &s.t \\ &\text{C1}: \exp(\tilde{p}_1)\ge \exp\left(\frac{\left(2^{\beta}-1\right)\left(\delta^2+p_2\bullet C_1\right)\left(\delta^2+D_1\right)}{A_1\bullet\left(\delta^2+D_1\right)-2^{\beta}\bullet B_1\bullet\left(\delta^2+p_2\bullet C_1\right)}\right) \\ &\text{C2}: 0\le \exp(\tilde{p}_1)\le P_1^{\max} \\ &\text{C3}: \exp(\tilde{p}_1)-\frac{\delta^2+p_2C_1}{A_1}\bullet\left[2^{\xi^{(l)}}\left(1+\ln 2\bullet\left(\eta-\xi^{(l)}\right)\right)\text{-}1\right]\le 0 \end{aligned} \tag{21}$$

Hence, the optimization problem in (21) is a convex program, which can be efficiently solved by the standard convex solver, e.g., CVX. **Table 1** gives the algorithm to solve the power optimization problem in (21) after the original optimization problem in (8) being handled by the relaxation and the SCA algorithm.

Table 1. Power optimization algorithm for the cellular user (21)

Initialization: Set $l=0$, $\mathbf{P}_2=P_2^{\max}$, δ, $\alpha_1^{(0)}=0$, $\beta_1^{(0)}=0$ select the first point $\left(\mathbf{P}_1^{(0)}\right)$
Step 1: While (1),
Step 2: Solve the problem (18), get the optimal solution $\left(\mathbf{P}_1^{*}\right)$,
Step 3: $l=l+1$,
Step 4: set $\left(\mathbf{P}_1^{(l)}=\mathbf{P}_1^{*}\right)$, calculate $\alpha_1^{(l)}$ and $\beta_1^{(l)}$ using (14) given in **Lemma 1**;
Step 5: Until $\overline{C}_n^{(l)}-\overline{C}_n^{(l-1)}\le\delta$, stop.
Output: the optimal solution $\left(\mathbf{P}_1^{*}\right)$, the optimal value $\overline{C}_n^{*}$.

3.3 Power Optimization for the D2D transmitter node

We discuss how to get the local optimal solution of transmission power for the cellular user in the above subsection. Now we will substitute the obtained suboptimal p_1 from the above subsection into (10). Next we will only optimize the transmission power of the D2D transmitter node when it is assumed that the transmission power for the cellular user is fixed. Similarly, we use the same method discussed in the above subsection to optimize the D2D transmission power. Hence, it will not be explained in detail here.

We can see that the fourth term in (10) is a non-convex function and the second term has no the variable p_2. Based on the **Lemma1**, we can relax the first term (10) to be stated in (22), where α_2, β_2 are the lower-bound coefficients:

$$G_2\left(\overline{p}_2\right) \approx \frac{1}{\ln 2}\left(\alpha_2 \ln\left(A_1 \bullet p_1\right) - \alpha_2 \ln\left(\delta^2 + C_1 \bullet e^{\overline{p}_2}\right) + \beta_2 \ln 2\right) \tag{22}$$

When the first term in (10) is replaced by (22), we denote the objective function as $\overline{\overline{C}}$. Then, by adding the auxiliary variables t, the third term in (10) can be expressed as:

$$\log_2\left(1 + \frac{p_2 A_2}{\delta^2 + p_1 C_2}\right) \geq t, \left(t \geq 0\right) \tag{23}$$

We denote $F_2\left(p_2, t\right) = p_2 - \frac{\delta^2 + p_1 C_2}{A_2}\left(2^t - 1\right)$, which is a non-convex function because its Hesse matrix a negative semidefinite one, i.e., $\nabla^2 F_2\left(p_2, t\right) \leq 0$. Similarity, we also can get $F_3\left(p_2, t\right) = p_2 - \frac{\delta^2 + p_1 C_2}{A_2} \bullet \left[2^{\zeta}\left(1 + \ln 2 \bullet \left(t - \zeta\right)\right) \text{-} 1\right]$ is the convex upper bound of $F_2\left(p_2, t\right)$.

On the other hand, it can be verified that $F_2\left(p_2, t\right)$ hold the following equation when $p_2 = t$:

$$\begin{aligned} F_2\left(p_2, t\right) &= F_3\left(p_2, t, \zeta\right) \\ \nabla F_2\left(p_2, t\right) &= \nabla F_3\left(p_2, t, \zeta\right) \end{aligned} \tag{24}$$

Thus, in the $l-th$ recursion, (23) can be replaced by the following convex constraint condition:

$$p_2 - \frac{\delta^2 + p_1 C_2}{A_2} \bullet \left[2^{\zeta^{(l)}}\left(1 + \ln 2 \bullet \left(t - \zeta^{(l)}\right)\right) \text{-} 1\right] \leq 0 \tag{25}$$

where $\zeta^{(l)} = p_2^{(l-1)}$, $p_2^{(l-1)}$ is represented as the local optimal solution of the transmission power for the D2D transmitter in the $\left(l-1\right)-th$ recursive. Hence, the suboptimizaiton problem can be expressed as:

$$\begin{aligned} &\max_{p_2} \ \overline{\overline{C}} \\ &s.t \\ &\quad \mathrm{C1}: 0 \leq \exp\left(\overline{p}_2\right) \leq P_2^{\max} \\ &\quad \mathrm{C2}: \exp\left(\overline{p}_2\right) - \frac{\delta^2 + p_1 C_2}{A_2} \bullet \left[2^{\zeta^{(l)}}\left(1 + \ln 2 \bullet \left(t - \zeta^{(l)}\right)\right) \text{-} 1\right] \leq 0 \end{aligned} \tag{26}$$

Similarity, the optimization problem in (26) is a convex program, which also can be

solved by the standard convex solver, e.g., CVX. Because the algorithm is similar to the one to optimize the transmission power for the cellular user shown in **Table 1**, here we omit the specific procedure.

3.4 Joint Power Optimization Algorithm

From the above subsections, the original optimization problem (8) is divided two convex optimization subproblems to be solved after being handled by the relaxation and the SCA algorithm. Now in this subsection, the joint iterative transmission power optimization algorithm for both the cellular user and D2D transmitter node is proposed as follows:

Table 2. Joint power optimization algorithm (8)

Initialization: Set $l=0$, $p_2^{temp}=P_2^{\max}$, β, δ, $\alpha_1^{(0)}=0$, $\beta_1^{(0)}=0$, $\alpha_2^{(0)}=0$, $\beta_2^{(0)}=0$.
While(1)
Step 1: Set $p_2=P_2^{temp}$, solve the problem (21) with SCA algorithm shown in the **Table 1**, get the optimal solution p_1^*, denoted as p_1^{tenp}.
Step 2: Set $p_1=p_1^{tenp}$, solve the problem (26) with SCA algorithm , get the optimal solution p_2^*, denoted as p_2^{temp}.
Step 3: $l=l+1$,
Step 4: set $\left(p_1^{(l)}=p_1^*, p_2^{(l)}=p_2^*\right)$.
Step 5: Until $C^{(l)}-C^{(l-1)}\le\delta$, stop. Otherwise, to the Step1.
Output: the optimal solution $\left(p_1^*, p_2^*\right)$, the optimal value C^*.

Property 1 (Convergence)： The proposed joint transmission power optimization algorithm converges to the equilibrium ergodic secrecy rate.

Proof Sketch: Now, we briefly analyze the convergence of the joint transmission power optimization algorithm in **Table 2**. The parameters $\xi^{(l)}$ and $\zeta^{(l)}$ in the optimization problems (21) and (26) respectively satisfy (20) and (25) when they are updated. Therefore, the set of feasible solutions in $n-th$ recursive is a subset of the feasible solutions in the $(n+1)-th$ recursive. Consequently, the optimal target values in the $(n+1)-th$ recursive are at least less than the optimal ones in the $n-th$ recursive. In other words, the optimal values got by the optimization problems in (21) and (26) are non-decreasing. On the other hand, the ergodic secrecy rate of this hybrid network must have the upper bounds with the given transmission power. Based on the above analysis, the joint transmission power optimization algorithm in **Table 2** is convergent.

4. Simulation Results

We present simulation results to prove the overall system performance under the proposed scheme. A simplified cellular network model is considered with the radius R=500m. Eve is in the cell subject to uniform distribution. We assumed that all the channels are the path loss model[26] $h_{ij}=d_{ij}^{-k/2}e^{j\varphi}$. Simulation parameters are given in **Table 3**.

Table 3. Simulation Parameters

Parameter	Setting
radius of the cellular network R	500m
transmission antennas number of the full-duplex base station N_t	6
reception antennas number of the full-duplex base station N_r	4
transmission antenna number of the cellular user N_c	1
transmission antenna number of the D2D pair N_d	1
transmission antenna number of Eve N_e	1
path-loss exponent κ	3
artificial noise power of the full-duplex base station	40dBm
maximum transmission power of the cellular user	20dBm
maximum transmission power of the D2D transmitter node	20dBm
location of the full-duplex base station	$(0,0)$
location of the cellular user	$(100,0)$
location of the D2D transmitter node	$(400,0)$
location of the D2D destination node	$(450,0)$
secrecy rate threshold of the cellular user β	0.5bits/s/Hz
every cyclic discrimination threshold δ	0.01bits/s/Hz

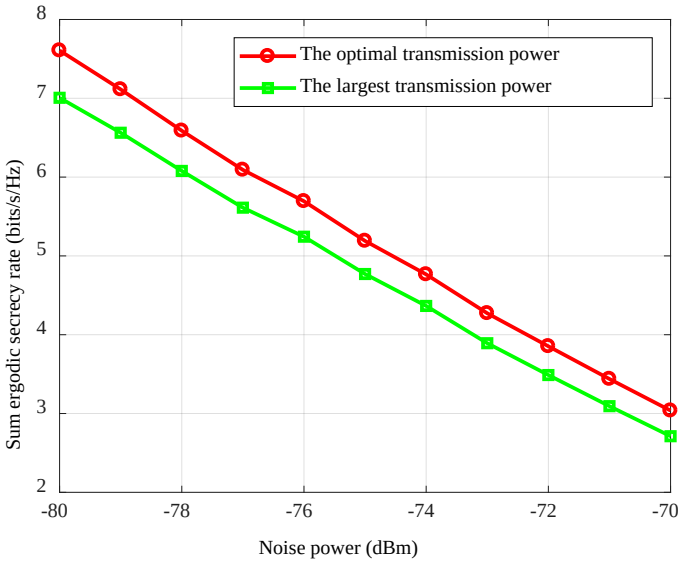

Fig. 2. Sum ergodic secrecy rate with noise power

Fig. 2 demonstrates the sum ergodic secrecy rate of different kinds of users with the proposed joint transmission power optimization algorithm under the different noise power, where the sum secrecy rate with their largest transmission power is also presented for comparison. As observed, it can see that the sum secrecy rate with the proposed algorithm is larger than that with the largest transmission power. In this paper, it is assumed that the

eavesdropper has the powerful multi-user decidability, which could subtract the interference induced by the information-bearing signals from the cellular user and D2D transmitter node. Hence, the interference induced by the hybrid links reused the same resource will not degrade the eavesdropper's channel capacity.

What is more, as mentioned above in subsection 2.2, their security performances directly depends on their transmission power. Especially, improving the transmission power of the cellular user will improve itself secrecy rate obviously. However, it will degrade the ergodic secrecy rate of the D2D transmitter node. It will be in the same situation when the transmission power of the D2D transmitter node is improved. Therefore, the scheme with their largest transmission power may be not the optimal one from the perspective of the secrecy performance for this hybrid network. Thus, we should carefully design their transmission power to maximize the sum secrecy rate for this hybrid network. Compared with the largest transmission power, it could improve the overall secrecy performance with the optimal transmission power obtained by the proposed algorithm.

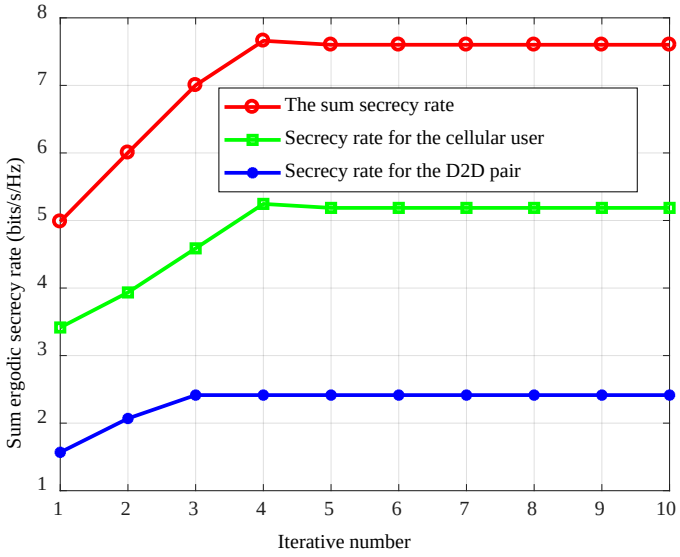

Fig. 3. Sum secrecy rate under iterative numbers

Fig. 3 shows the secrecy rate with the iterative number increasing when the noise power is -80dBm. As shown in **Fig. 3**, all secrecy rates converge to a stable value fast with the iterative number increasing. We can see that all the security rates have been stable when the iterative number is 4. Hence, we can conservatively conclude that the proposed scheme is effective and efficient.

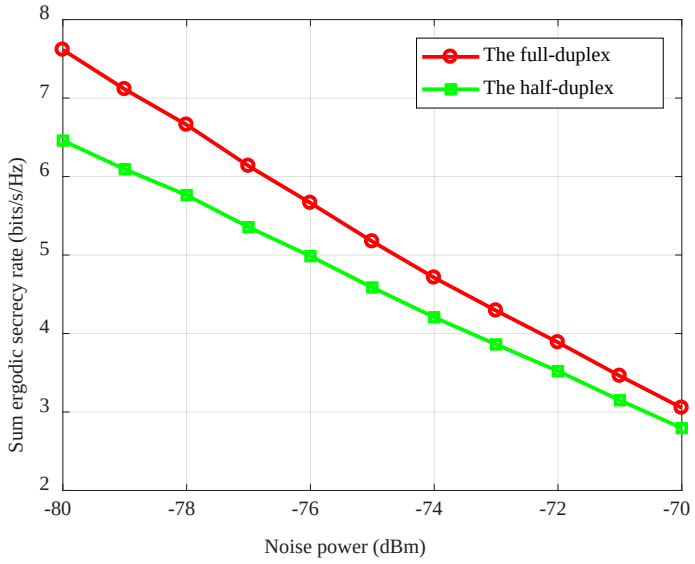

Fig. 4. Sum ergodic secrecy rate with different noise powers compared with the half-duplex scheme

The sum ergodic secrecy rate for this hybrid network is presented in **Fig. 4** under the different noise power compared with the traditional half-duplex scheme. The artificial noise designed within the null space of the joint channel from the full-duplex base station is injected into the downlink information-bearing signals while receiving uplink signals, resulting in only degrading the the channel capacity for the eavesdropper. As expected, the sum ergodic secrecy rate with the full-duplex base station is larger compared with the half-duplex scheme. In other word, the proposed secure transmission scheme based on the artificial noise under the full-duplex base station could improve its performance compared with the traditional half-duplex scheme.

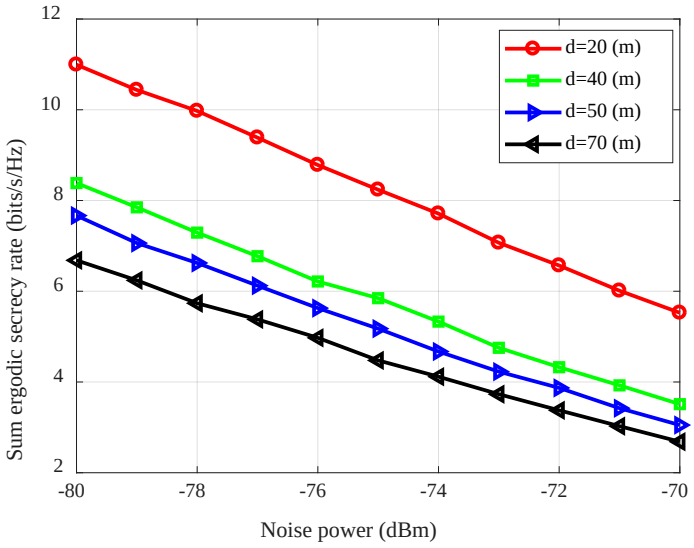

Fig. 5. Sum ergodic secrecy rate with different distance between D2D pair under different noise powers

Furthermore, we exploit the impact of the distance between D2D pairs on the overall security performance. From **Fig. 5**, we can see that the sum ergodic secrecy rate of this hybrid network will be smaller with the distance between the D2D pair increasing. This is because the channel fading between the D2D pair will be more serious, the smaller the channel capacity with a larger distance between the D2D pair, resulting in a smaller sum ergodic secrecy rate.

5. Conclusion

A secure transmission scheme based on the artificial noise for D2D-enabled cellular networks was exploited in this paper. The full-duplex base station transmits the artificial noise to achieve secure communication for both the cellular user and D2D transmitter node when it receives signals of the cellular uplink. To maximize the overall secrecy rate for the hybrid work, a secure power allocation scheme is presented. However, the original optimization problem is non-convex. To solve it, we utilize the proper relaxation and the successive convex approximation algorithm to change the original optimization problem into a convex program problem. Finally, simulation results are conducted to evaluate the effectiveness of the proposed scheme. In the further work, we should fully study the full-duplex transmission gain to guarantee the secure communication in other scenarios.

References

[1] Fodor G, Roger S, Rajatheva N, et al., "An Overview of Device-to-Device Communications Technology Components in METIS," *IEEE Access*, vol.4, pp. 3288-3299, 2016. Article (CrossRef Link).

[2] K. Doppler, M. Rinne, C. Wijting, et al., "Device to-device communication as an underlay to LTE-Advanced networks," *IEEE Communication Magazine*, vol.47, no.12, pp. 42-49, 2009. Article (CrossRef Link).

[3] G. Fodor, E. Dahlman, G. Mildh, et al., "Design aspects of network assisted device-to-device communications," *IEEE Communication Magazine*, vol.50, no.3, pp.170-77, 2012. Article (CrossRef Link).

[4] B. Li, Z. Fei, Z. Chu, Y. Zhang, "Secure Transmission for Heterogeneous Cellular Networks with Wireless Information and Power Transfer," *IEEE Systems Journal*, vol.12, no.4, pp. 3755-3766, 2018. Article (CrossRef Link).

[5] B. Li, Z. Fei, Z. Chu, et al., "Robust Chance-Constrained Secure Transmission for Cognitive Satellite-Terrestrial Networks," *IEEE Transactions on Vehicular Technology*, vol.67, no.5, pp.4208-4219, 2018. Article (CrossRef Link).

[6] B. Li, Z. Fei, X. Xu, et al., "Resource Allocations for Secure Cognitive Satellite Terrestrial Networks," *IEEE Wireless Communications Letters*, vol.7, no.1, pp.78-81, 2018. Article (CrossRef Link).

[7] B. Li, X. Qi, K. Huang, Z. Fei, F Zhou, R. Hu, "Security-Reliability Tradeoff Analysis for Cooperative NOMA in Cognitive Radio Networks," *IEEE Transactions on Communications*, vol.67, no.1, pp.83-96, 2019. Article (CrossRef Link).

[8] Y. Chen, X. Ji, K. Huang, et al., “Opportunistic access control for enhancing security in D2D-enabled cellular networks," *SCIENCE CHINA Information Sciences*, vol. 61, no. 4, 042304:1-12, April. 2018. Article (CrossRef Link).

[9] Z. Chu, F. Zhou, P. Xiao, Z. Zhu, et al., “Resource Allocation for Secure Wireless Powered Integrated Multicast and Unicast Services With Full Duplex Self-Energy Recycling,” *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 620-636, Jan. 2019. Article (CrossRef Link).

[10] M. Alam, Y. Du, J. Rodriguez, et al., “Secure Device-to-Device Communication in LTE-A,” *IEEE Communications Magazine*, vol.52, no.4, pp. 66-73, 2014. Article (CrossRef Link).

[11] D. Zhu, A. Swindlehurst, S. Fakoorian, et al., “Device-to-device communications: the physical layer security advantage,” in *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence*, 1606-1610, 2014. Article (CrossRef Link).

[12] H. Zhang, T. Wang, L. Song, et al., “Radio resource allocation for physical-layer security in D2D underlay communications,” in *Proc. of IEEE International Conference on Communications (ICC), Sydney, NSW*, 2319-2324, 2014. Article (CrossRef Link).

[13] J. Yue, C. Ma, Y. Hui, et al., “Secrecy-Based Access Control for Device-to-Device Communication Underlaying Cellular Networks,” *IEEE Communications Letters*, vol.17, no.11, pp.2068-2071, 2013. Article (CrossRef Link).

[14] J. Yue, C. Ma, H. Yu, et al., “Secrecy-based Channel Assignment for Device-to-Device Communication: An Auction Approach,” in *Proc. of IEEE International Conference on Wireless Communications & Signal Processing (WCSP), Hangzhou, China*, 1-6, 2013. Article (CrossRef Link).

[15] Y. Chen, X. Ji, K. Huang, et al., “Artificial noise-assisted physical layer security in D2D-enabled cellular networks,” *EURASIP Journal on Wireless Communications and Networking*, 178, 2017. Article (CrossRef Link).

[16] B. Day, A. Margetts, D. Bliss, and P. Schniter, “Full-duplex bidirectional MIMO: Achievable rates under limited dynamic range,” *IEEE Transactions on Signal Processing*, vol.60, no.7, pp. 3702-3713, 2012. Article (CrossRef Link).

[17] W. Cheng, X. Zhang, and H. Zhang, “Optimal dynamic power control for full-duplex bidirectional-channel based wireless networks,” in *Proc. of IEEE 32nd INFOCOM, Turin, Italy*, 3120-3128, 2013. Article (CrossRef Link).

[18] W. Afifi, M. Abdel-Rahman, M. Krunz, et al., “Full-Duplex or Half-Duplex: A Bayesian Game for Wireless Networks with Heterogeneous Self-Interference Cancellation Capabilities,” *IEEE Transactions on Mobile Computing*, vol.17, no.5, pp.1076-1089, 2018. Article (CrossRef Link).

[19] V. Nguyen, H. Nguyen, O. Dobre, “A New Design Paradigm for Secure Full-Duplex Multiuser Systems,” *IEEE Journal on Selected Areas in Communications*, vol.36, no.7, pp. 1480-1498, 2018. Article (CrossRef Link).

[20] X. Ji, X. Kang, K. Huang, et al., "The full-duplex artificial noise scheme for security of a cellular system," *China Communications*, vol.12, no. Supplement, pp. 150-156, 2015. Article (CrossRef Link).

[21] M. Li, Y. Guo, K. Huang, et al., "Secure power and subcarrier auction in uplink full-duplex cellular networks," *China Communications*, vol.12, Supplement, pp. 157-165, 2015. Article (CrossRef Link).

[22] G. Chen, Y. Gong, P. Xiao, et al., "Physical layer network security in the full-duplex relay system," *IEEE Transactions on Information Forensics and Security*, vol.10, no.3, pp. 574-583, 2015. Article (CrossRef Link).

[23] S. Goel, I. Negr, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol.7, no.6, pp. 2180-2189, 2008. Article (CrossRef Link).

[24] A. Beck, A. Ben-Tal, and L. Tetruashvili, "Application of the sequential parametric convex approximation method with application to nonconvex truss topology design problems," *Journal of Global Optimizaiton*, vol.47, no.1, pp. 29-51, 2010.

[25] W. Cheng, X. Zhang, H. Zhang, "Optimal Dynamic Power Control for Full-Duplex Bidirectional-Channel Based Wireless Networks," in *Proc. of IEEE INFOCOM 2013, Turin, Italy*, 3120-3128, 2013. Article (CrossRef Link).

[26] L. Dong, Z. Han, A. Petropulu and H. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays," *IEEE Transactions on Signal Processing*, vol.58, no.3, pp. 1875-1888, 2010. Article (CrossRef Link).

Chen Yajun received the B.E. degree in UESTC University. He then received the M.S. and Ph.D degrees in National Digital Switching System Engineering & Technological R&D Center (NDSC), Zhengzhou, China. He has been a faculty member of NDSC since 2017. His research interests include physical layer security, wireless location and resource management in 5G networks.

Yi Ming received the B.E. degree in PLA Information Engineering University, Zhengzhou, China. He then received the M.S. and Ph.D degrees in NDSC. He has been a faculty member of NDSC since 2012. His research interests include physical layer security, channel coding.

Zhou Zhong received his Ph.D. degree in NDSC, Zhengzhou, China. Currently, he is a lecturer at NDSC. His research interests include wireless communication and physical layer security.

Ma Keming received the B.E. degree in PLA Information Engineering University, Zhengzhou, China. He then received the M.S. degree in NDSC. He has been a faculty member of NDSC since 2014. His research interests include wireless location.

Kaizhi Huang received her B.E. degree in digital communication and M.S. degree in communication and information system from Information Engineering University, Zhengzhou, China, and Ph.D. degrees in communication and information system from Tsinghua University, Beijing, China, in 1995, 1998 and 2003 respectively. She has been a faculty member of NDSC since 1998, where she is currently a professor and director of the Laboratory of Mobile Communication Networks.

Xinsheng Ji received the B.E. degree in Fudan University, Shanghai, China, in 1984, and received the M.S. degrees in PLA Information Engineering University, Zhengzhou, China, in 1991. He has been a faculty member of NDSC since 1988, where he is currently a professor and the chief engineer of NDSC. He has been a member of the Network and Communication (NaC) specialist group for China 863 High Technology Program and a senior member of China Institute of Communication. He was awarded as an outstanding expert of state in 2015. His major research interests include wireless communication network, security and signal processing.