Block-D2D: Blockchain-enabled Cooperative D2D-assisted Fog Computing Scheme under Imperfect CSI

Rajesh Gupta*, *Student Member, IEEE*, Tejal Rathod†, Sudeep Tanwar§, *Senior Member, IEEE*
*†‡ Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India
Email: *18ftvphde31@nirmauni.ac.in, †tejal.rathod611@gmail.com, §sudeep.tanwar@nirmauni.ac.in

2021 IEEE International Conference on Communications Workshops (ICC Workshops) | 978-1-7281-9441-7/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICCWorkshops50388.2021.9473524

***Abstract*—Fog computing (FC) supports cloud computing services at the edge of the device for more secure and reliable access and processing of the stored data. However, it is beneficial for time-sensitive applications, where the required delay is minimum, but not well suited for mission-critical applications, where the required delay is negligible. To fulfill this requirement, the authors worldwide started integrating FC with device-to-device (D2D) communication. But it was potentially affected by massive interference, which does not improve the total sum rate and secrecy capacity of the wireless channel. Motivated from these gaps, in this paper, we propose a blockchain-enabled cooperative D2D-assisted FC scheme under imperfect CSI in the presence of an eavesdropper called *Block-D2D* to enhance the total sum rate and secrecy capacity. We used non-orthogonal multiple access (NOMA) scheme for D2D pairs to improve the aforementioned characteristics. Still, the data on the device is not fully secure, which can be modified by any malicious user. This can be protected using blockchain technology, which is immutable, secure, and trusted. To improve the secrecy capacity of the network and spectral efficiency, we used a cooperative game theory. Simulation results show that the elevated performance of the NOMA-based *Block-D2D* scheme compared to the conventional OFDMA scheme in terms of sum rate, secrecy capacity, and system throughput.**

***Index Terms*—Blockchain, device-to-device communication, fog computing, NOMA.**

I. Introduction

A wireless sensor network (WSN) consists of a large number of sensor nodes that are interconnected to form a wide communication network. It possesses a small size, low cost, low power consumption, and other features. Sensors are power constrained small network devices, which do not support large computation capabilities. To achieve robust and high computing capabilities in WSNs, centralized cloud computing is a viable solution, which delivers a flexible stack of substantial computing, storage, and software services in a scalable and virtualized manner at low-cost [1]. Its provisions configure and reconfigure the servers as and when needed by the end-users. WSN is integrated with cloud computing to mitigate its shortcomings, like storage capacity (data collected by sensor nodes) and processing. Cloud computing is efficient in storage and processing capabilities but not suitable for those applications which require instantaneous results for decision making. Such applications would be autonomous vehicles, the internet of vehicles, border surveillance, etc. Instead of latency, the other major limitations of cloud computing are the single point of failure, security, and privacy, which leads to huge data loss. The latency issue has been resolved with the ultra-reliable low-latency communication (URLLC) property of fifth-generation (5G) networks, but still, other issues like security and privacy persist.

The new paradigm, such as fog computing (FC), becomes a feasible solution to cloud computing's aforementioned issues. It offers massive end-user support, fast data access and processing, a device-driven communication environment, and a heterogeneous network interface [2], [3]. To satisfy the rapidly growing need for wireless data services, the FC brings computing, storage, and intelligence capabilities near to the user by offloading the required data services and applications from the centralized cloud server. It offers high security, availability, and reliability compared to the cloud and a well adaptable solution for some mission-critical applications. The computing and storage capabilities of fog nodes (in FC) are limited, which may not handle massive connectivity and processing. This restricts its real-time implementation. So, there is a need for distributed processing, which shares the load of fog nodes efficient processing.

The device-to-device (D2D) communication is a perfect solution for the aforementioned issues in FC. It allows the nearby devices to communicate via Bluetooth or WiFi Direct by bypassing the base station between [4]. It improves bandwidth, spectrum efficiency, security, privacy, and flexibility due to its short-range communication. D2D communication minimizes the data traffic on the data servers, such as fog nodes, by extending the storage, computing, processing, and communication capabilities within the proximity range. It relies on the collaboration of nearby devices instead of sending data to the remote fog node or fog server for storage and processing. This D2D-assisted FC is perfectly suitable for all mission-critical or time-sensitive applications. Such type of communication is more affected by different types of interferences (interference from cellular user, another D2D user, and eavesdropper) and noises. Very little work has been done in this field by researchers across the globe. Many of them have taken care of resource and channel allocation but neglect the effect of interference and noise in the wireless fading channel, which is impractical [5]–[7]. A very few authors tackled the security issues but not considered the eavesdropper, which is too under the perfect channel state information (CSI), impractical in a real scenario. The existing literature of D2D-enabled FC also does not guarantee trust and transparency among the D2D nodes, which increases the security and privacy risks of data in communication.

Motivated from the aforementioned talk, in this paper, we present a blockchain-enabled cooperative D2D-assisted FC scheme called *Block-D2D* under the presence of an eavesdropper. We also assumed the channel state is imperfect, which

978-1-7281-9441-7/21/$31.00 ©2021 IEEE

means a channel realizes the fading and noise. The D2D communication is not having any fixed infrastructure, which increases eavesdroppers' involvement that overhears the communication between the D2D transmitter and D2D receiver. The traditional D2D-aided FC schemes use orthogonal frequency division multiplexing access (OFDMA), which serves one user at a time. It reduces spectrum efficacy. To increase the spectral efficiency, in this paper, we have considered the communication among D2D receiver and transmitter follows the non-orthogonal multiple access (NOMA) scheme, which serves multiple users at a time. NOMA also takes care of the intra-user interference (from D2D transmitter to D2D receiver) with their successive interference cancellation (SIC) technique. In SIC, a user correctly decodes its signal from the given signal by removing other signals interference. As NOMA increases the spectral efficiency, total sum rate, and secrecy capacity of the wireless channel, data security, privacy, trust, and transparency at the device persists.

To overcome the aforementioned issue, this paper integrates public blockchain technology with the cooperative D2D-aided FC scheme under imperfect CSI. Blockchain is a chain of blocks that grows with each transaction and is linked through cryptographic hash values. The blockchain block comprises transaction data, timestamp, nonce, and a cryptographic hash of the previous block [8]. Blockchain has many characteristics such as immutability, distribution, security, and trust, which makes it difficult for an eavesdropper to decode the message correctly [9]. Any D2D user can participate in transaction/data exchange via blockchain if it has a valid certificate issued by the registration authority. This eliminates the involvement of intruders/eavesdropper. According to the aforementioned characteristics, we believe that blockchain would be an appropriate technology to deal with mutual authentication challenges in an exceedingly FC environment for both individuals and organizations in managing and authenticating their identities [10]. The main contribution of this technology is to allow communication between heterogeneous devices. This communication is accomplished without depending on any centrally trusted devices or authority.

A. Motivation

The motivation of this study is as follows.

- The existing studies on the integration of D2D and FC were entirely focused on resource allocation, channel allocation, and security. But, they neglect the presence of eavesdroppers, which can compromise the privacy of their proposed systems. So, there is a need for a system that increases data communication security in an integrated D2D-FC enabled scheme with the active involvement of an eavesdropper.
- Researchers worldwide have used the OFDMA scheme for data offloading/downloading, which essentially serves one user at a time. It reduces spectral efficiency. Thus, a system needs to be designed with a NOMA scheme, which serves multiple requests at a time and improves the channel spectral efficiency.

B. Contributions

Motivated from the aforementioned facts (mentioned in Section I-A), following are the research contributions of this paper.

- We propose a blockchain-enabled cooperative D2D-assisted FC scheme to ameliorate the performance in terms of delay, security, privacy, spectral efficiency, trust, interference minimization, bandwidth requirement, and transparency.
- We integrate NOMA with the D2D-assisted FC system to mitigate the intra-user interference between the D2D transmitter and D2D receivers.
- A cooperative game theory has been applied to improve the total sum rate and secrecy capacity.

The remainder of this paper is organized as follows. Section II presents system model and problem formulation with channel based and blockchain-based security. Section III presents a cooperative game theoretic approach to improve sum rate and channel secrecy capacity. Section IV discussed the results and performance evaluation of the proposed *Block-D2D* scheme, and finally, Section V concludes the paper.

II. System Model and Problem Formulation

This section elaborates the system and channel modeling for blockchain-assisted cooperative D2D-enabled FC scheme under imperfect CSI. Fig. 1 shows a scenario in which both D2D users and eavesdropper coexists. D2D users can be either D2D transmitter (D_T) or D2D receiver (D_R). The eavesdropper (E) in a scenario can be any D2D user (either D_{Tx} or D_{Rx}). Consider a cellular user ($\mathcal{Z}$) and D2D user ($\mathcal{X}$) sets as $\mathcal{Z} = \{1, 2, \ldots, z, \ldots, Z\}$ and $\mathcal{X} = \{1, 2, \ldots, x, \ldots, X\}$ respectively. Any x^{th} D2D receiver D_R^x is strong or weak that decides upon its geographical location, whether it is within the cell radius (δ) or not. Any D2D transmitter D_T ($\forall D_T \in \mathcal{X}$) communicates with the D2D receiver D_R ($\forall D_R \in \mathcal{X}$) using NOMA scheme, whereas the cellular user z ($z \in \mathcal{Z}$) opts OFDMA to establish a communication with the base station/fog node over resource block (Ω). In our scenario, there exists two categories of D2D users, which are cooperative (these are those D2D users which takes part in distributing storage and processing capabilities) and non-cooperative (not helping storage and processing capabilities). The cooperative and non-cooperative D2D users are represented as $D_{T/R}^c \in \mathcal{X}$ and $D_{T/R}^{nc} \in \mathcal{X}$, respectively, where $D_{T/R}$ is any D2D transmitter of receiver. The D2D users (with D2D/edge devices) reduces the burden of fog node by performing calculations and computations locally. It also minimizes the spectrum usage (by minimizing data offloading from device to the fog node) and enhances the decision capabilities for various mission-critical applications such as autonomous vehicles, unmanned aerial vehicles, connected cars, etc. If the data is massive, then D2D devices are not capable to process it due to its limited battery and computation constraints. In such case, the data (only emergency data) need to migrate to the set of fog nodes at the fog layer (in Fig. 1) $\mathcal{N} = \{1, 2, \ldots, n, \ldots, N\}$ for further processing, otherwise, migrate it to the cloud layer.

The data can be emergency ($Data_e$) or non-emergency ($Data_{ne}$) data based on their nature. $Data_e$ can cause instant and severe damages to the people or public properties if not processed on time. Examples of $Data_e$ are breaking and control decisions for autonomous vehicles. The security of data is also utmost important against the eavesdropper E in this scenario. It can be achieved using the integration of blockchain technology, which is distributed, immutable,

trusted, and transparent in nature. It ensures security using public-private key cryptography and digital signatures.

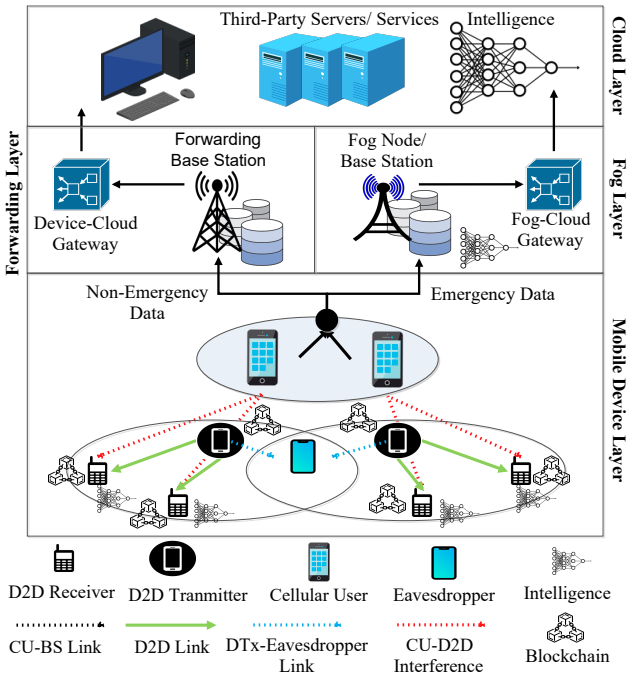

Fig. 1: *Block-D2D*: System Model.

A. Channel-based Security

As per the discussion in Section I, there are very few researches that have focused on minimizing data offloading to the fog node and efficacy of mission-critical applications to make instant decisions with cooperative D2D communication. Moreover, they have taken the channel conditions as perfect, which is unrealistic in the case of dynamic wireless communication. So, this paper considered the channel conditions as imperfect, i.e., imperfect CSI at the transmitter side (D_T^x), which encounters path loss, fading, shadowing, noise, and interference. The fading is considered as Rayleigh fading, and the interferences as cellular user $\mathcal{Z}$ to D2D D_R^x (also called cross channel interference) and intra-user interference (between D_R^x's, where $x \in \{1, 2, \ldots, i\}$, value of $i \leq$ number of D2D receivers). The channel gain (ζ) of the z^{th} cellular user to the n^{th} base station/fog node over an orthogonal uplink channel is calculated as follows.

$$\zeta_{z,n} = \sqrt{1-\vartheta}\tilde{\zeta}_{z,n} + \sqrt{\vartheta}\hat{\zeta}_{z,n} \tag{1}$$

where ϑ is the channel variance, which decides the channel is perfect of imperfect. So, the Eq. 1 represents the channel gain between CU and fog node, likewise the cooperative channel gain ζ between x^{th} D_T^x and D_R^x ($x > 0$) is calculated as follows [11].

$$\zeta_{D_T,D_R} = \left[\sqrt{1-\vartheta}\tilde{\zeta}^x_{D_T,D_R} + \sqrt{\vartheta}\hat{\zeta}^x_{D_T,D_R}\right]_{D^c_{T/R}} \tag{2}$$

In our scenario, we have considered an eavesdropper also, which is the part of D2D user only. The non-cooperative channel gain between

1) z^{th} cellular user and eavesdropper E

$$\zeta_{z,E} = \left[\sqrt{1-\vartheta}\tilde{\zeta}_{z,E} + \sqrt{\vartheta}\hat{\zeta}_{z,E}\right]_{D^{nc}_{T/R}} \tag{3}$$

2) x^{th} D2D user, i.e., D_R^x and eavesdropper E

$$\zeta_{x,E} = \left[\sqrt{1-\vartheta}\tilde{\zeta}_{x,E} + \sqrt{\vartheta}\hat{\zeta}_{x,E}\right]_{D^{nc}_{T/R}} \tag{4}$$

where $D^c_{T/R}$ and $D^{nc}_{T/R}$ represents the cooperative and non-cooperativeness of the D2D receivers/transmitters, respectively. We consider the link between cellular user and fog node is always cooperative. So, our main focus is towards the communication security between the D2D users such as D_T and D_R by mitigating or reducing intra-user interference (also called NOMA interference). It is an interference of weak D2D user towards the strong D2D user, where $|\zeta^{\varphi_s}_{D_R^x}| \geq |\zeta^{\varphi_w}_{D_R^x}|$. $\zeta^{\varphi_s}_{D_R^x}$ is the channel gain of x^{th} strong D_R and $\zeta^{\varphi_w}_{D_R^x}$ is the channel gain of x^{th} weak D_R. Any D_T send a message or data (μ) to the weak D2D user (φ), which is geographically located at the edge of network and is represented as follows [12].

$$\mu^{\varphi_w}_{D_T} = \varpi_1 + \nu^x_{D_T,\varphi_w} \tag{5}$$

$$\varpi_1 = \left(\sqrt{\xi^x_{D_T}\Upsilon_{\varphi_w}}\mathbb{M}^{\varphi_w}_{D_T} + \sqrt{\xi^x_{D_T}\Upsilon_{\varphi_s}}\mathbb{M}'^{\varphi_w}_{D_T}\right)\zeta^x_{D_T,\varphi_w} \tag{6}$$

where $\mathbb{M}^{\varphi_w}_{D_T}$ and $\mathbb{M}'^{\varphi_w}_{D_T}$ is the actual message transfer by any x^{th} D_T to the x^{th} D_R. $\zeta^x_{D_T,\varphi_w}$ is the channel gain of x^{th} weak user. $\nu^x_{D_T,\varphi_w}$ is the additive white Gaussian noise from x^{th} D_T to the weak user φ_w. Υ_{φ_w} and Υ_{φ_s} are the data message transmit powers weak and strong user respectively. The channel gain in NOMA is higher due to reduced interference as it uses SIC technique. The SINR (Φ) at the weak user is calculated as follows.

$$\Phi^{\varphi_w}_{D_T} = \frac{\xi^x_{D_T}|\zeta^x_{D_T,\varphi_w}|^2}{\left[\xi^x_{D_T}|\zeta^x_{D_T,\varphi_s}|^2 + \xi_z|\zeta^x_{z,\varphi_w}|^2\right] + \sigma^2_{D_T,\varphi_w}} \tag{7}$$

In the proposed system model, an eavesdropper E receives a signal from D2D transmitters D_T only, as the signal from z^{th} cellular user to n^{th} fog node is assumed as cooperative and trusted. So, the message received by an eavesdropper E from the x^{th} D_T is as follows [13].

$$\mu^E_{D_T} = \varpi_2 + \nu^x_{D_T,E} \tag{8}$$

$$\varpi_2 = \left(\sqrt{\xi^x_{D_T}\Upsilon_E}\mathbb{M}^E_{D_T} + \sqrt{\xi^x_{D_T}\Upsilon_E}\mathbb{M}'^E_{D_T}\right)\zeta^x_{D_T,E} \tag{9}$$

The corresponding SINR expression is evaluated as follows.

$$\Phi^E_{D_T} = \frac{\xi^x_{D_T}|\zeta^x_{D_T,E}|^2}{\left[\xi^x_{D_T}|\zeta^x_{D_T,E}|^2 + \xi_z|\zeta^x_{z,E}|^2\right] + \sigma^2_{D_T,E}} \tag{10}$$

B. Total Sum Rate

The data rates of both strong user, weak user, non-cooperative user, and eavesdropper are $\mathcal{D}_{D_T,\varphi_s}$, $\mathcal{D}_{D_T,\varphi_w}$, $\mathcal{D}_{D_T,E}$, $\mathcal{D}_{D_T,D'}$, respectively is calculated using Shannon capacity theorem as follows.

$$\mathcal{D}_{D_T,\varphi_s} = \log_2\{1+(\frac{\xi^x_{D_T}|\zeta^x_{D_T,\varphi_s}|^2}{\left[\xi^x_{D_T}|\zeta^x_{D_T,\varphi_s}|^2 + \xi_z|\zeta^x_{z,\varphi_s}|^2\right] + \sigma^2_{D_T,\varphi_s}})\} \tag{11}$$

$$\mathcal{D}_{D_T,\varphi_w} = \log_2\{1+(\frac{\xi^x_{D_T}|\zeta^x_{D_T,\varphi_w}|^2}{\left[\xi^x_{D_T}|\zeta^x_{D_T,\varphi_s}|^2 + \xi_z|\zeta^x_{z,\varphi_w}|^2\right] + \sigma^2_{D_T,\varphi_w}})\} \tag{12}$$

$$\mathcal{D}_{D_T,D'} = \log_2\{1+(\frac{\xi^x_{D_T}|\zeta^x_{D_T,D'}|^2}{\left[\xi^x_{D_T}|\zeta^x_{D_T,D'}|^2 + \xi_z|\zeta^x_{z,D'}|^2\right] + \sigma^2_{D_T,D'}})\} \tag{13}$$

$$\mathcal{D}_{D_T,E} = \log_2\{1+(\frac{\xi^x_{D_T}|\zeta^x_{D_T,E}|^2}{\left[\xi^x_{D_T}|\zeta^x_{D_T,E}|^2 + \xi_z|\zeta^x_{z,E}|^2\right] + \sigma^2_{D_T,E}})\} \tag{14}$$

The total sum rate ($\mathcal{S}_T$) of any D_T is calculated as follows.

$$\mathcal{S}_T = \mathcal{D}_{D_T,\varphi_s} + \mathcal{D}_{D_T,\varphi_w} + \mathcal{D}_{D_T,D'} + \mathcal{D}_{D_T,E} \tag{15}$$

This shows that the improvement in total sum rate (or data rate) of the system with NOMA and its SIC technique.

C. Total Secrecy Capacity

The channel secrecy capacity ($\mathbb{C}$) of D_T against any non-cooperative D2D user (D') and eavesdropper E is represented as follows.

$$\mathbb{C}_{D_T,D} = [\mathcal{S}_T - \mathcal{S}_{D_T,D'}]^+ \tag{16}$$

$$\mathbb{C}_{D_T,E} = [\mathcal{S}_T - \mathcal{S}_{D_T,E}]^+ \tag{17}$$

The total secrecy capacity is evaluated as follows.

$$\mathbb{C}_{D_T,Tot} = [\mathcal{S}_{D_T,E} + \theta \sum_{\{D_T,D_R\}\neq D'}^{X} \mathcal{S}_{D_T,E}] \tag{18}$$

where $\mathbb{C}_{D_T,Tot}$ is the total channel secrecy capacity of D_T. θ is represents the non-cooperative indicator, $\theta = 1$ represents cooperative D2D user.

D. Blockchain-based Security

The above discussion takes care of imperfect channel conditions against the non-cooperative D2D user and eavesdropper E. For cooperative data processing, the data should be distributed among the trusted D2D users. But, the data exchange between D_T and D_R for cooperative and distributed processing is not fully protected due to trust issues of non-cooperative D2D users as well as channel interference. The solution to the aforementioned issues is the integration of blockchain technology (β), which ensures trust, transparency, and protection against any kind of data modification. It is a chain of immutable blocks, which store metadata as well as transactions. The hash of the current block (η_C) is calculated using the hash of the previous block (η_P) and the block data (B_{Data}). The hash function (one-way function) is represented as follows [14].

$$\eta : \{\varkappa\} \rightarrow \{0,1\}^k, \forall \varkappa \in \mathbb{M}_{D_T,D_R} \tag{19}$$

$$\eta(\varkappa) = \varkappa' \tag{20}$$

s.t.

$$\eta(\varkappa') \neq \varkappa \tag{21}$$

$$\eta(\varkappa_1) \neq \eta(\varkappa_2),\ \varkappa_1 \neq \varkappa_2 \tag{22}$$

where $\varkappa$ is a message to the transmitted that belongs to the set of messages $\mathbb{M}$. $\varkappa'$ is the hash value of any message $\varkappa$ transmitted over wireless channel from D_T to D_R. So, the hash of the current block is calculated as follows.

$$\eta_C = \{\eta_P \oplus TimestampT_0 \oplus f \oplus Nonce_0\} \tag{23}$$

A node (D_R) receives a message $\varkappa$ from D_T, but it needs to be validated to establish the trust, whether the message $\varkappa$ received from cooperative user ($D^c_{T/R}$), non-cooperative user ($D^{nc}_{T/R}$), or eavesdropper (E) [15].

$$\mathbb{V}_\beta : \mathcal{X} \times \mathcal{T} \rightarrow \{True, False\} \tag{24}$$

$$(x, \mathcal{T}_j) \rightarrow \mathbb{V}_\beta(x, \mathcal{T}_j) \tag{25}$$

If the result of $\mathbb{V}_\beta(x, \mathcal{T}_j)$ is *True*, then the transaction from x^{th} D_T is considered to be valid, then it is forwarded to all the participants/members (all D_R) by adding it to the blockchain β.

$$\mathcal{T}_j.append(\mathcal{T}) \tag{26}$$

Blockchain is distributed, each D_R and D_T have a copy of the entire ledger with them. Each participant of the blockchain is having a wallet. If the transaction is not valid, i.e., $\mathbb{V}_\beta(x, \mathcal{T}_j)$ is *False*, then a fixed is to be deducted from the participant's wallet as a penalty and mark that particular participant as non-cooperative. The decidability on the selection of blockchain β member is based on the certificate issued by the registration authority R_A. Fig. 2 shows the flow of the entire process from participant registration to the transaction publish. Blockchain has a smart contract, which takes a decision the storing of D2D participant's D_T transaction $\mathcal{T}_j$ into the block of a blockchain β. A participant first creates a transaction and sends it to the blockchain β. Before storing transaction into the blockchain, it first met the conditions of smart contract $\mathcal{SC}$. A $\mathcal{SC}$ verify the participant's certificate issued by the registration authority R_A. It then checks the status of the certificate, whether it is 0 (not given permission) or 1 (given permission). If it is 1, then store the transaction into the blockchain β, otherwise, deny the request and ask to get a certificate from R_A. A $\mathcal{SC}$ eliminates the need for trusted third-party systems which establishes the trust between D_T and D_R.

The ultimate goal of the proposed scheme is to maximize

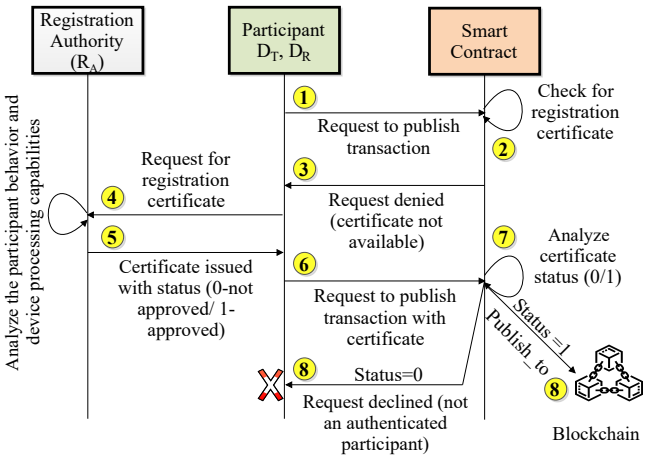

Fig. 2: Flow of the proposed scheme from participant registration to the transaction publish.

the total sum rate and secrecy capacity of the communication channel between D_T and D_R. The communication should be protected against the eavesdropper as well as the non-cooperative D2D user using the SIC technique of NOMA.

Algorithm 1 shows the blockchain-based secrecy-ensured message transfer between D_T and D_R.

Algorithm 1 Blockchain-based secrecy-ensured message transfer between D_T and D_R.

Input: $D_T \rightarrow$ Total number of D2D transmitters and $D_R \rightarrow$ Total number of D2D receivers.

Output: Secrecy-ensured data transfer between D_T and D_R.

Step 1: The SIC technique of NOMA helps to mitigate the intra-user interference.

Step 2: NOMA allocated different power coefficients to the D2D users, i.e., D_R based on the strong and weak classification.

Step 3: Both Step 1 and Step 2 assures the correct delivery of message to the D_R, but cannot protect information from eavesdroppers (passive listeners).

Step 4: A blockchain β ensures high secrecy even against the eavesdropper also.

Step 5: A blockchain $\mathcal{SC}$ verifies the transaction storage request is from the valid user or not.

Step 6: A $\mathcal{SC}$ verification process is shown in Fig. 2.

Step 7: The proposed system ensures high security by combining interference mitigation and blockchain.

III. Cooperative Game Formulation

The cooperative game is used to create a D2D pair between transmitter and receiver, i.e., D_T and D_R, based on the following parameters

- Distance γ of D_R from D_T. Based on distance the D2D users has been classified as strong (φ_s) or weak (φ_w).
- Status of certificate issued by the R_A, i.e., status $\in \{0,1\}$. Status=1 means a valid certificate has been issues to the participant for transaction processing and storage, otherwise not.

Then, the utility function to create a D_T and D_R pair is as follows.

$$\mho = \lambda(D_T^x, D_R^x) < \delta_{max} + \textit{status(certificate)} \quad (27)$$

where $\mho$ is a utility function between x^{th} D_T^x and D_r^x. λ is a function that calculates the distance between D_T and D_R. δ_{max} specifies the max radius δ of the cell. The game parameters of the proposed scheme are as follows.

- *Player*: D2D devices/users (D_T and D_R) int the network
- *Payoff*: Creation of D_T and D_R pair for data exchange.
- *Resource*: Actual message.
- *Strategy*: The working of proposed algorithm.

In this game formulation, the D2D user pair forms Y disjoint coalitions (where two coalitions are mutually exclusive) to enhance the sum rate and secrecy capacity of the wireless channel.

$$\mathcal{H} \in \{\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_y, \ldots, \mathcal{H}_Y\}, \quad (28)$$

$$\mathcal{H}_y \cap \mathcal{H}'_y = \phi \quad (29)$$

$$\cup_{y=1}^{X} \mathcal{H}_y = \mathcal{X} \quad (30)$$

The D2D users can change their coalitions in order to improve the data rates. This coalition shifting is also called as switching. It converges towards the maximal solution.

IV. Results and Discussion

This section shows the evaluation results and performance evaluation of the proposed *Block-D2D* scheme. The results are evaluated based on both network (NOMA integration into the proposed scheme) and blockchain parameters. The subsequent subsections show the detailed description of the evaluation of *Block-D2D* based on the aforementioned parameters.

TABLE I: Parameters for simulation

Parameters	Values
Cell Layout	Circular
Cell Area	300mx300m
Radius (δ)	30m
Number of CUs ((Z))	4 –5
Number of D2D pairs ($\mathcal{X}$)	4 –10
Bandwidth (B)	30MHz
Number of DTx	2
Maximum transmit power of DTx (Υ_x)	20dBm
Maximum transmit power of CU (Υ_z)	35dBm
Estimation error variance (ϑ)	0.1
Path Loss Exponent	4

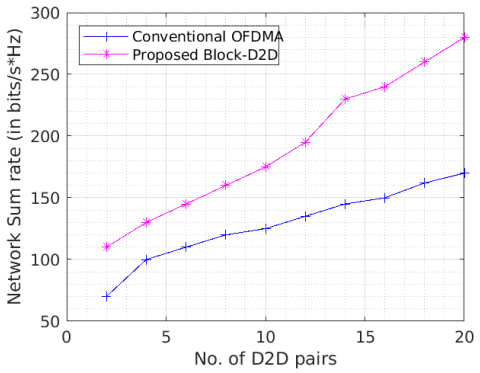

Fig. 3: Achieved sum rate of *Block-D2D* with respect to OFDMA scheme.

A. Network-based Evaluation

The proposed *Block-D2D* scheme is accessed against the OFDMA scheme and Table I shows the parameters considered for the simulation.

Fig. 3 represents the comparison of the total sum rate of the proposed *Block-D2D* with respect to the conventional OFDMA scheme. The x-axis of the graph represents the number of cellular users and D2D pairs. It is inferred from the graph that the total sum rate of *Block-D2D* improves with the increase in the number of cellular users and D2D pairs, which is due to disjoint coalition and switching, whereas the sum rate of the conventional OFDMA scheme decreases with an increase in cellular users and D2D pairs, which causes excessive noise and interference.

Fig. 4 represents the comparison of achieved secrecy capacities of the proposed *Block-D2D* and the conventional OFDMA scheme. It is inferred from the graph that the total secrecy capacity of *Block-D2D* improves drastically with the increase in the number of cellular users and D2D pairs. It is due to the SIC technique of NOMA as well as blockchain technology.

B. Blockchain-based Evaluation

Fig. 5 shows the throughput comparison of existing non-blockchain and the proposed *Block-D2D* scheme in the presence of eavesdropper or malicious user. We observe that the increase in the number of D2D users in the traditional non-blockchain-based systems decreases the average throughput of

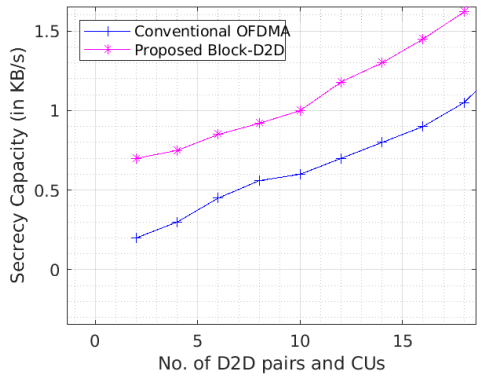

Fig. 4: Achieved secrecy capacity of *Block-D2D* with respect to OFDMA scheme.

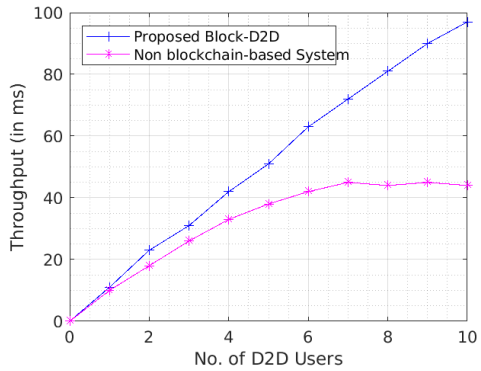

Fig. 5: Throughput comparison of *Block-D2D* and non blockchain-based systems in the presence of eavesdropper.

the system due to the decoding of $(n-1)$ users signals to decode its signal correctly. This does not affect the throughput of the proposed *Block-D2D* scheme.. The smart contract of the proposed *Block-D2D* scheme is compiled and executed over Remix integrated development environment and get the byte code. It then deployed in the Remix testing environment to test, debug, and publish the smart contract. Fig. 6 shows the smart contract functions with their parameters executed over Remix using solidity language.

V. Conclusion

In this paper, we proposed a novel Blockchain-based D2D-aided FC system to facilitate services to mission-critical applications. The proposed system improves both the sum rate and channel secrecy capacity of the network by minimizing the processing delay and the effect of interference and noise. To achieve a high sum rate and secrecy capacity, we introduce the SIC technique NOMA for D2D pairs. This not only minimizes the interference but also minimizes the effect of an eavesdropper. Further, to increase the spectral efficiency and secrecy rate, we formulated a coalition game. The simulated results show that the proposed system is superior compared the traditional OFDMA technique with the increasing number of D2D pairs and CUs in terms of sum rate, channel secrecy capacity, and processing delay. In the future, we will take into account the co-channel interface to further enhance the sum rate and secrecy capacity of the wireless communication channel.

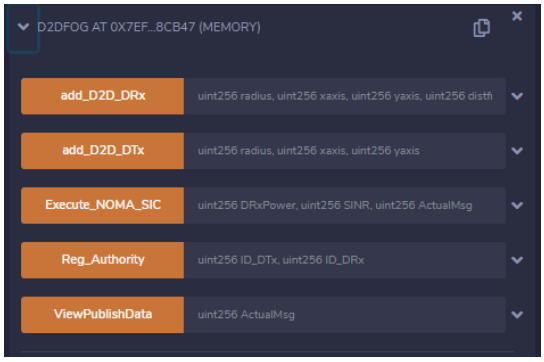

Fig. 6: Interface of the proposed *Block-D2D* scheme deployment and testing of the smart contract over Remix IDE.

Acknowledgment

This work is supported by Visvesvaraya Ph.D. Scheme for Electronics and IT by Department of Electronics and Information Technology (DeiTY), Ministry of Communications and Information Technology, Government of India <MEITY-PHD-2828>.

References

[1] A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi, and M. A. Hossain, "A survey on sensor-cloud: architecture, applications, and approaches," *International Journal of Distributed Sensor Networks*, vol. 9, no. 2, p. 917923, 2013.

[2] V. Moysiadis, P. Sarigiannidis, and I. Moscholios, "Towards distributed data management in fog computing," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[3] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges," *Computers and Electrical Engineering*, vol. 72, pp. 1 – 13, 2018.

[4] Y. Zhang, E. Pan, L. Song, W. Saad, Z. Dawy, and Z. Han, "Social network aware device-to-device communication in wireless networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 1, pp. 177–190, 2014.

[5] Y. Lan, X. Wang, D. Wang, Z. Liu, and Y. Zhang, "Task caching, offloading, and resource allocation in d2d-aided fog computing networks," *IEEE Access*, vol. 7, pp. 104876–104891, 2019.

[6] C. Yi, S. Huang, and J. Cai, "Joint resource allocation for device-to-device communication assisted fog computing," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2019.

[7] P. Gope, J. Lee, R. Hsu, and T. Q. S. Quek, "Anonymous communications for secure device-to-device-aided fog computing: Architecture, challenges, and solutions," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 10–16, 2019.

[8] P. Singh, A. Nayyar, A. Kaur, and U. Ghosh, "Blockchain and fog based architecture for internet of everything in smart cities," *Future Internet*, vol. 12, no. 4, p. 61, 2020.

[9] Y. L. X. Y. Z. S.-H.-J. K. Zhiliang Deng, Yongjun Ren, "Blockchain-based trusted electronic records preservation in cloud storage," *Computers, Materials & Continua*, vol. 58, no. 1, pp. 135–151, 2019.

[10] Y. Gao, M. Wu, Y. Xiao, P. Yang, B. Fu, and D. Wang, "Blockchain enabled distributed cooperative d2d communications," in *2019 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6, 2019.

[11] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, and J. J. P. C. Rodrigues, "Tactile internet for smart communities in 5g: An insight for noma-based solutions," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 3104–3112, 2019.

[12] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, and M. Guizani, "Cr-noma based interference mitigation scheme for 5g femtocells users," in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2018.

[13] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, and M. Guizani, "Cross layer noma interference mitigation for femtocell users in 5g environment," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 4721–4733, 2019.

[14] V. Gayoso Martínez, L. Hernández-Álvarez, and L. Hernandez Encinas, "Analysis of the cryptographic tools for blockchain and bitcoin," *Mathematics*, vol. 8, p. 131, 01 2020.

[15] Coperneec, "How to represent a blockchain through a mathematical model?." https://canopee-group.com/wp-content/uploads/2020/05/Blockchain-Coperneec.pdf. Accessed: April 2020.