Received XX Month, XXXX; revised XX Month, XXXX; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version 11 January, 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.011100

Blockchain-assisted Dynamic Resource Pool Selection for D2D Roaming Scenarios

Seung-Hoon Park[1], Tahira Mahboob [1,2] *(Member, IEEE)*, Syed Tariq Shah[3], Mahmoud A. Shawky [4], Minseok Choi [5] *(Member, IEEE)*, and Min Young Chung [1] *(Member, IEEE)*

[1]Department of Electrical and Computer Engineering, Sungkyunkwan University, Republic of Korea
[2]Department of Computer and Software Engineering, Information Technology University of the Punjab, Pakistan
[3]School of Computer Science and Engineering, University of Essex, CO4 3SQ Colchester, UK
[4]James Watt School of Engineering, University of Glasgow, Scotland, G12 8QQ, UK
[5]Department of Electronic Engineering, Kyung Hee University, Yongin 17104, Republic of Korea

Corresponding Author: Min Young Chung (email: mychung@skku.edu), Co-corresponding Author: Tahira Mahboob (tahira.mahboob@itu.edu.pk) and Syed Tariq Shah(syed.shah@essex.ac.uk)

ABSTRACT Device–to–device (D2D) communications are based on direct signaling and data transmission within wireless devices. Furthermore, it facilitates mission-critical services for public safety (PS), vehicle–to–vehicle (V2V) or drones. These D2D applications need nationwide coverage across multiple operators. The existing roaming system, however, does not provide sufficient trust for D2D roaming scenarios since the direct link between devices is difficult to monitor in the core network side. Therefore, a novel framework to support D2D roaming is proposed inspired by blockchain–based trust systems. The framework consists of an authentication for D2D user equipment (UE) access, authorization to configure D2D service, and resource pool selection. Also, a dynamic D2D resource pool selection enabled by D2D class awareness is supported. Analytical results show that the proposed dynamic resource pool selection scheme improves capacity in the form of decoding performance.

INDEX TERMS Blockchain, Device–to–device (D2D), Proximity Service (ProSe), Roaming

I. Introduction

The proximity service (ProSe) has been worked in the Third-generation Partnership Project (3GPP) [1], [2]. ProSe supports industrial and governmental applications such as PS, V2V, drones, robots, Internet–of–Things (IoT), location–based services, or local social networking. The applications depend on device-to-device (D2D) communication [3]–[7], which enables direct communications between user equipment (UE). The 3GPP manages the standardization of D2D operations including user equipment (UE) discovery [8], [9], D2D link management, and resource management. The 3GPP defines different type of D2D communication, such as unicast or multicast, on top of the physical layer broadcasting link [10].

Likewise, any communication system, D2D link at layer 2 is a top of signaling and data transmission at layer 1. In 3GPP, D2D signaling is transmitted via scheduling assignment (SA) message, and D2D data message is transmitted via resources allocated across time and frequency. The UE selects resources for transmission of SA and data messages from a D2D resource pool which is a periodic resource structure. For the convenience of D2D service management, a D2D service is assigned to a specific D2D resource pool which is configured according to service requirements. In addition, different scheduling policy may be applied to each D2D pool for UEs being identically scheduled inside of the specific pool, but differently across different pools.

The existing roaming system in mobile communications depends on its trust to monitoring functionality at the packet gateway. Meanwhile the traditional roaming depends on monitoring and controlling of the session at the core network. Since the packet gateway is located inside the core network, a method of monitoring direct D2D communication links is not feasible considering the lack of such capability at base station (BS) or UE under the visiting operator. If we would like to avoid delay of checking the D2D trust relationship at the core network, the radio access network (RAN) should directly manage the D2D trust at the ProSe server (which manages D2D communications of the RAN according to the 3GPP specification).

Blockchain systems are known as the trust machine especially for decentralized architecture. It means that home operator can delegate to the mobile device suitable configurations, such as, UE–specific service class or profile, for the UEs when it moves to a visiting operator network. The delegated mobile device can store the information for the security process with the visiting network's ProSe server and verify that the information was already approved by the home network. Considering this, features of a blockchain–assisted roaming system are investigated and applied for the authentication, authorization and trusted computing perspectives. The proposed details of how to enable the trusted D2D roaming system is the first to the best of our knowledge. The performance may be affected by the existing D2D communication system, as well as the benefits from the proposed roaming system. The simulation results show the benefit of trusted roaming in terms of the throughput and delay.

The remainder of this paper is structured as follows: Section II provides overall descriptions on the D2D communications and blockchain systems; technical issues for D2D roaming are discussed in Section III and a blockchain-assisted D2D roaming framework is proposed in Section IV; Section V investigates the feasibility of a proposed dynamic D2D resource pool selection in terms of the performance from a variety of conditions, and lastly, the conclusion is presented.

II. Preliminaries

A. Overall system structure of D2D communications

D2D UEs are configured in different ways in accordance with the location of the UE as shown in Fig. 1. If a UE (as UE 1) is located in-coverage of the BS, the UE is configured by the BS for a D2D resource pool and a resource pattern for data transmission. If another UE (as UE 4) is not attached to any BS and defined as an out-of-coverage UE, the UE is operated in the pre-configured resource pool. The pre-configured resource pool is set by the vendor before delivering the UE machine to the operator. For both types of UE, sensing is performed to select control resource to transmit a SA message. For the sake of simplicity, implicit mapping between a SA resource pattern and a data resource pattern are assumed. It means that selection of a SA resource pattern leads to the selection of the related data resource pattern. Therefore, avoiding high congested SA resource is helpful to get less interference from the selected data resource. Whichever resource pattern is assigned, UE waits a next opportunity to transmit SA and data signals when the congestion level from the sensing result is higher than the configured threshold level.

A transmission UE (TX UE) transmits a SA message through the control channel. The SA message contains a number of resouce blocks (RBs), a resource allocation pattern, a modulation and coding scheme (MCS), and a destination identifier (ID). The destination ID is used for the TX UE to designate the target UE or a target group of UEs. A reception UE (RX UE) matched to the destination ID identifies also the resources to be listen from the received SA message.

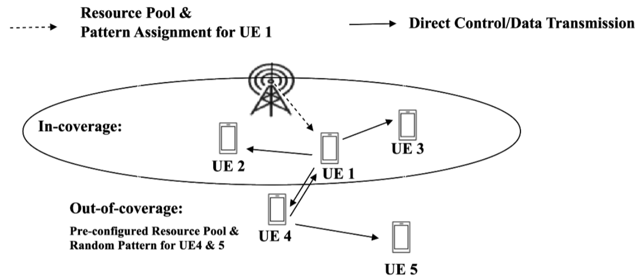


FIGURE 1: D2D UE types and resource configuration cases.

For less signal collision, the TX UE chooses the set of RBs that are not chosen by the other TX UEs. In general, sensing–based SA resource selection is performed to achieve the low collision rate and high signal–to–noise–and–interference (SINR) level. The overall packet error rate (PER) is suppressed under the target PER level owing to the sensing scheme. A TX UE selects radio resources, called a resource pattern for transmission (RPT), and indicates this RPT information to the neighboring UEs through SA signaling. Since there is no direct negotiation, a selected RPT of multiple TX UEs may be collided. The collision may degrade the performances because of a higher interference of the signal from the collided TX UEs.

In reality, coordination for collision avoidance between operators are difficult since one network operator does not cover the whole mobile user subscription in a nation. In addition, there may be a situation that UEs subscribed to one operator and other UEs subscribed to another operator should communicate in the same D2D channel, in cases of emergency responders, V2V, drones, or etc. Roaming is a federation service to allow a subscriber in the home operator to access a visiting network. The visiting network decides to attach the UE based on the contract between the home and visiting operators. The similar scheme may be applied to D2D cases; however, it is hard to say that the same approach still works under the D2D-specific issues. A key issue is how to provide the suitable D2D service according to the specific D2D channel or user profiles, in the precise and trusted way. In general, the conventional roaming service has only a couple of roaming profile and policy, due to the complexity of controlling, charging, and billing issues within operators. Therefore, this chapter focuses to achieve the dynamic resource selection tailoring to the user demands. Hereafter, three technical topics (i.e., authentication and authorization, trusted computing, and D2D resource assignment) are investigated in terms of the D2D roaming case. It is noted that pre-configured resource pool is out–

of–scope of this paper, since out–of–coverage UEs are not involved in the roaming scenario.

B. A brief description of blockchain and smart contracts

A blockchain (or a distributed ledger) is essentially a linked-list type data structure that is constructed by following certain rules. The invention of blockchain is as an underlying technology of the Bitcoin system [11] which enables peer-to-peer electronic cash transfer. It is, however, beyond just a data structure and enables a variety of new services especially on handling multi–party transactions. Since the blockchain stores historical and immutable records which are open to public, or at least a consortium, it is useful to verify the ownership of a data in a transparent way achieved by the visibility and traceability. The second innovation following Bitcoin is a smart contract which was defined conceptually in 1994 [12], and implemented after 30 years by Ethereum [13] in 2015. Compared to a message–based transaction in Bitcoin, Ethereum utilizes computing instructions made of operation codes in virtual machines. Operation codes can be compiled from high–level programming languages, giving a high degree of freedom to code any algorithm. It opens a second wave of mass adoption of blockchain technologies.

In this paper, it is noted that read/write instructions for configuring ProSe server located at the core network of each operator, is executed via smart contract. We briefly discuss how a smart contract is deployed and executed in a blockchain system. A smart contract is written in a specific high–level language and compiled into an operation code, referred to as opcode. An opcode is deployed in a memory area as an instruction and communicated via an application binary interface (ABI). The opcode is regarded as trusted since the opcode is written in the blockchain, and open to public to be verified by anyone (by code-level hash matching [14]). A blockchain client can trigger a programming function of the smart contract via ABI which is exposed by the deployed opcode. Each deployed opcode has an address and can be called by address. In general, ABI is formatted in javascript object notation (JSON) for web front–end implementation. Once a function of the smart contract is triggered, the opcode tries to execute the function and change the state according to the computing result. To make sure of the integrity of the state change, blockchain system relies on the consensus mechanism that multiple nodes execute the triggered function of the opcode concurrently and follow the computing results of majority decision.

After the Bitcoin software was released in 2009, numerous blockchain systems and blockchain–inspired studies followed. Blockchain technology has been mainly applied within financial systems [15]. Other areas, such as, decentralized web services including but not limited to, decentralized name service [16], decentralized storage [17], decentralized cloud resource scheduling [18], decentralized internet [19], and decentralized IoT system [20], have also been investigated.

Recently, from 2022 to 2024, more diverse works have been for blockchain system improvements [21], data caching [22] and data sharing [23], security [24] [25] [26], transport networking [27] [28]. With regard to the topic of resource allocation, which is related to this paper's concern, there were two papers for a resource allocation between cellular and D2D networks [29] and another resource allocation between remote device and relaying device [30]. Unfortunately, there is no prior work for D2D roaming case due to the technical challenges. Also, D2D applications have resided on the single operator, such as, public safety networks, where a government is apt to delegate the whole authority to a specific and verified operator. Upcoming industries such as automotive vehicle, drones–based logistics, and intelligent swarm robot need public investments as well as the D2D roaming within operators for national coverage and overcoming subscriber silos. In the following sections, technical issues on D2D roaming will be investigated.

III. Technical Issues on D2D Roaming

A. Authentication and Authorization

The first technical topic comes from how to authenticate the roaming UE and authorize proper services (represented by ProSe ID) in the different operator's network. There would be two possible options: the first is interworking, and the second is token-based. Option 1 performs authentication and authorization between ProSe functions of each operator. It needs a subscriber verification process between two operators. A visiting network sends a verification request to the home network upon receiving the global identifier of a roaming UE – international mobile subscriber identity (IMSI). Home subscriber server (HSS) handles the verification request and returns the confirmation to the visiting network. If this is a conventional roaming case, UE' s charging report is collected from the visiting network and bandwidth usage is counted at the home network (since the session termination is performed at P–GW of the home network). In the end, a settlement process is performed for billing and payment according to their roaming agreement.

Option2 performs authentication and authorization between a ProSe function and a roaming UE. It is similar to token–based authorization (i.e., single–sign–on) on the web. The roaming UE is storing the issued token from the home network. The token consists of IMSI, ProSe ID, SA priority, Data priority, verifier signature, issuing date, validation period, etc. It is noted that the token is recorded to the verifiable storage and UE should manage transactions with its private keys. UE can verify the ownership of the token by sending the digital signature of itself. In any case of first and second options, the ProSe function in the roaming network should be trusted by the home network as well as the roaming UE.

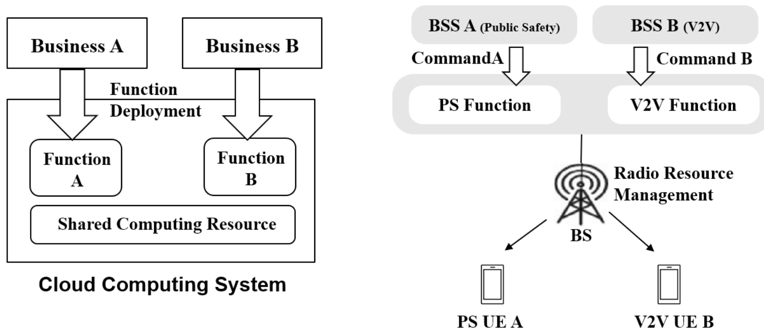


FIGURE 2: Cloud computing system.

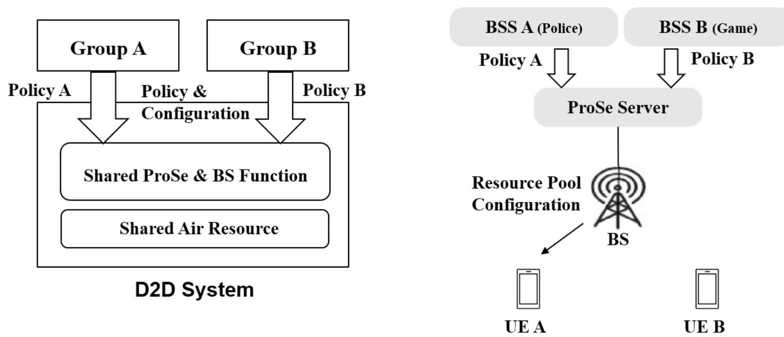


FIGURE 3: D2D communications system.

B. Trusted Computation

Trust in cloud computing is achieved in general by providing monitoring tools to customers. The monitoring tools manage (metrics, events, logs, traces) M.E.L.T. in real-time. Customers can trust the cloud service by checking the transient metrics. In general, a neutral 3rd party is involved in monitoring and service level agreements (SLA) verifications. SLA is a legal contract which may incur legal service cost. In addition, monitoring is available only to the visible sources of the system. Therefore, conventional service level agreement (SLA) verification supports neither the dynamic contract nor the hidden operations inside the system.

In the case of the D2D scenario, UE may have multiple group associations, and details of the SLA for each group may be different. In addition, direct link monitoring by the home network is difficult in roaming cases. To overcome these constraints, a trust relation at the function level should be achieved. The differences between cloud computing and D2D communication are shown in Figs. 2 and 3. In cloud systems, a function may be deployed and monitored by a customer. In D2D systems, a function is shared by multiple customers but managed differently by customer-specific policy and configurations per each policy. The main reason of policy-based function sharing comes from the widely distributed aspect of D2D control functions, compared to the centralized cloud computing. In general, two approaches can be studied in the D2D context as following:

1) Intent–based D2D service

An intent-based D2D service is useful to customers by automating management. The automated management system receives an intent from the customer and uses the intent to manage the D2D service by monitoring quality-of-service (QoS) and checking SLA violations. Once the system gets intents from a customer, it is interpreted to concrete policies for network operation. The policy may consist of UE ID, UE group ID, discovery flavor, communication flavor, QoS priority class, UE service coverage and etc. The ProSe server understands the policy and translates it into the actual configurations for discovery and communication in the allowed UE service coverage. The discovery configuration may handle discovery signature, and discovery broadcasting period, and discovery listening period. The communication configuration may handle D2D resource pool, control message, data message, etc.

The ProSe server can report about the configuration log to the home network of the roaming UE, but the report does not include the communication performance. There is, in fact, no practical method to monitor D2D performance indicators without embedding monitoring modules into BS or UE. UE has a low device capability as well as a chance of abusing to monitor with bias as a served entity. Dedicated resources in a BS for monitoring and reporting continuously may degrade the performance of the BS.

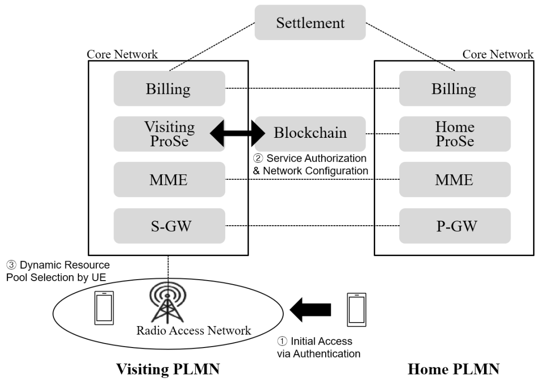


FIGURE 4: Overall Architecture and 3 Steps of Blockchain-assisted D2D Roaming.

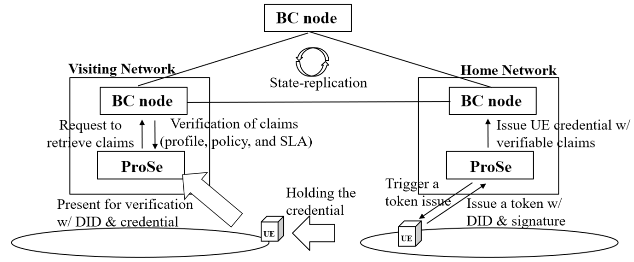


FIGURE 5: Initial Access Procedure in the D2D Roaming Framework.

2) Function sharing in cloud computing and D2D communication systems

When there is a limit to monitor what is going on inside the system from the outside observer, delegating controllability of the serving function itself to the system will be effective. Therefore, it is a fair way for multi-party to share the same function. The features of the shared function are open, neutral, transparent, and verifiable. Customers may remotely deliver and deploy their own function on the cloud infrastructure. The cloud provider places isolated resources for workloads of the remote customer. As shown in Fig. 2, different business services (e.g. PS and V2V) managed by different business support system (BSS) are served by different functions on the server system. In contrast, considering the D2D case, policy-based configuration and conflict resolution is important since the radio resources are utilized physically and there is no way for the function to handle radio resources like dedicated computing resources. Therefore, single ProSe function is preferred over multiple ProSe functions, but the single ProSe function should be neutral among multi-party. In Fig. 3, different service groups (e.g. police and gaming) access air resources according to the indicated service policy including how much portion is assigned to each service group.

IV. The Proposed Blockchain-assisted D2D Roaming Framework

This section investigates how to realize the discussed topics above based on a blockchain-based neutral and trust system. The blockchain technologies are emerging from back-end systems to decentralized applications [31]–[33]. As discussed, the conventional SLA framework in cloud computing will not work properly for D2D communications from agility and privacy perspectives. Therefore, all aspects of authentication, authorization, configuration, function sharing, and tracing will be designed inspired by the blockchain system. Figure 4 shows the overall considered architecture to support D2D roaming assisted by the blockchain system. It contains key entities (i.e., mobility management entity (MME), gateways, billing, and settlement) for conventional roaming as well as new entities (i.e., ProSe, blockchain) for D2D roaming. The proposed D2D roaming system model covers stepwise 3 procedures as shown also in Fig. 4; initial access to the visiting network, service-aware network configuration, and D2D resource pool selection. First, an authentication procedure is needed to decide whether to allow the roaming UE into the visiting network. Second, the visiting network verifies the requested service authorization and the relevant claims including service profile and policy for differentiating the requested service type. Third, the UE, which is configured by the acquired service policy, selects dynamically a suitable resource pool according to the matching with the demanded D2D channel of the UE.

A. Identity and Access Management (IAM) for Initial Access

In a single domain, a user is identified by its identity, which is a collection of verifiable claims to prove consistency in a specific time period. Contrary to the conventional IAM depending Identity Provider (IdP), verifiable claims to represent the identity are recorded on the blockchain. The blockchain node (BC node) provides the identifier and cryptographic base (i.e., PKI - Public Key Infrastructure) to store, present and prove the verifiable claims.

A D2D UE which resides in the home network requests to issue verifiable claims such as user profile, D2D service profile, and SLA contract relevant to the D2D roaming as shown in Fig. 5. The UE is regarded as holding issued claims since only the UE can handle the claims by using its own private key. When the UE moves from home to visiting network, the visiting network gets the UE identifier and retrieves the user and D2D service profile, as the form of verifiable claims, from the blockchain. The roaming agreement details the QoS and charging policies, and SLA. In this paper, the D2D access class is a key QoS parameter which is a differentiator to access a D2D resource pool.

B. Service-aware Network Configuration

In the proposed procedure as shown in Fig. 6, decentralized Identifiers (DID) from world wide web consortium

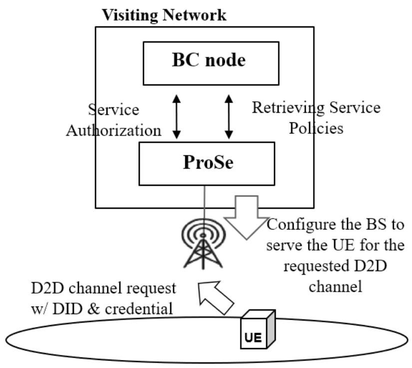


FIGURE 6: D2D Service Provision via Trusted Computing.

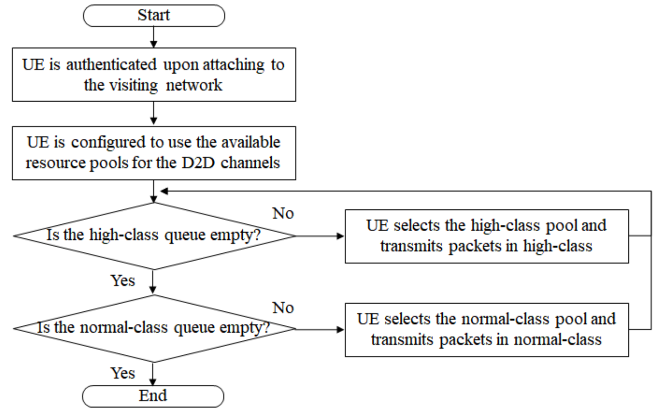


FIGURE 7: A flow chart of the proposed dynamic pool selection.

(W3C) standards developing organizations (SDO) is used to authenticate and authorize the roaming UEs. The roaming UE stores the wallet and requests a decentralized identifier (DID) verification procedure upon attaching to the visiting network. Since there is no session establishment procedure in the core network for the D2D roaming, the verification should be done at the ProSe server via the BS. Therefore, the BS delivers the request message including the DID and credential from the UE to the ProSe server so that the ProSe server verifies the roaming UE by checking with the blockchain. The ProSe server can resolve the authorization service endpoint of the blockchain by parsing the request message. Then it retrieves the relevant profiles of the roaming UE for initiating services. In the end, the return message comes back to the roaming UE with DID-recorded event logs.

This scheme gives the flexibility to selectively disclose the claims to request of the specific D2D channel. During the procedure, the ProSe server and the BS configure the operation parameters for the requested D2D channel. The ProSe server generates and indicates the D2D discovery signature or SA index to the roaming UE. The BS assigns the roaming UE to the specific D2D resource pool where all the relevant D2D UEs talk and listen to the specific D2D channel. Messaging events and configuration logs are stored in the system and may submit them to the home network for charging and settlement procedures.

C. D2D Resource Pool Selection

The BS may adjust the quantity of D2D resources by pool configurations. There are two types of pools according to D2D channel classes - high-class pool taking 80% of resources and normal-class pool taking remaining 20%. In the static pool selection case, the roaming UEs are served in the normal-class pool, as the BS treats them blindly without knowing the proper class of the demanding D2D channel. The cause of not knowing may be the settling time to establish the roaming agreement, cost burden for the legal contract or the privacy issue.

On the other hand, in the dynamic pool selection case as shown in Fig. 7, the roaming UEs reveal their demand and authority to access the specific D2D channel. The roaming UE acquires the allowed SA identifier for entering the class and is configured to send D2D packets in the suitable resource pool accordingly. That is, the roaming UE that would like to talk with members in high-class, sends SA and data messages in the configured SA and data resource pools for high-class UEs. Monitoring bandwidth usage in a D2D scenario is not feasible because D2D communications are in broadcast manner and even the BS may not count the usage exactly. In that sense, rather, the history of modifying D2D resource pool configurations is recorded as logs to the blockchain.

V. Numerical Analysis of Dynamic Pool Selection

The parameters utilized for the numerical analysis are stated in Table 3. Here, we leverage the exponential pathloss model with an exponent α, the Rayleigh fading with a mean of 1, and the transmit power$P_tx[W]$is considered. Also, the receiving UE (RX UE) receives the transmitted signal from the transmitting (TX UE k) with the received power $h_k d_k^{(-\alpha)}[W]$, where the random variable h_k follows an exponential distribution with a mean of 1. When assuming there is no sensing-scheme and considering the same arrival rate, only the intensity matters to the congestion level. The intensity (in terms of power) will be same across multiple D2D resource pools in case that UEs randomly select a pool. It changes, however, according to the density of UEs in the pool, if UEs have a condition to select a specific pool, e.g., the roaming UE can select only a pool for normal-class. The selection condition affects in a form of an arrival rate λ_l to the interference term from UE l. Therefore, decoding probability, $P_{r_{dec}}(d_k)$, can be expressed as:

$$Pr_{dec}(d_k) = Pr(\gamma_k > \gamma_{thr}) = Pr\left(\frac{P_{tx} h_k d_k^{-\alpha}}{\sum_{j=1}^{N_f} \sum_{l\in\Phi}^{l\neq k} \delta_j P_t \lambda_l h_l d_l^{-\alpha}} > \gamma_{thr}\right), \quad (1)$$

which is written as the following equation:

$$Pr_{dec}(d_k) = Pr\left(h_k > d_k^{\alpha}\gamma_{thr}\sum_{j=1}^{N_f}\sum_{l\in\Phi}^{l\neq k}\delta_j\lambda_l h_l d_l^{-\alpha}\right) = 1 - Pr\left(h_k \leq d_k^{\alpha}\gamma_{thr}\sum_{j=1}^{N_f}\sum_{l\in\Phi}^{l\neq k}\delta_j\lambda_l h_l d_l^{-\alpha}\right) \quad (2)$$

Since cumulative distribution function of $h_k(Pr(h_k \leq b))$ follows $1 - e^{-b}$ [34], Equation 2 can be written, as follows:

$$Pr_{dec}(d_k) = E\left[\exp\left(-d_k^{\alpha}\gamma_{thr}\sum_{j=1}^{N_f}\sum_{l\in\Phi}^{l\neq k}\delta_j\lambda_l h_l d_l^{-\alpha}\right)\right] \quad (3)$$

where δ_j, h_l and d_l are independent random variables. Equation 3 therefore is written as the following equation: [35]:

$$Pr_{dec}(d_k) = E\left[\prod_{j=1}^{N_f}\left(\prod_{l\in\Phi}^{l\neq k} E_{h_l}[\exp(-d_k^{\alpha}\gamma_{thr}\lambda_l h_l d_l^{-\alpha}) \mid d_l]\right)^{\delta_j}\right] \quad (4)$$

Since we expect h_l follows an exponential distribution with mean 1 (i.e., $E[X] = 1/\lambda$ where $F(x;\lambda) = \{ \begin{smallmatrix} 1-e^{-\lambda x} & x\geq 0 \\ 0 & x<0 \end{smallmatrix}$), equation4 can be restructured as the following equation:

$$Pr_{dec}(d_k) = E\left[\prod_{j=1}^{N_f}\left(\prod_{l\in\Phi}^{l\neq k}\frac{1}{1 + d_k^{\alpha}\gamma_{thr}\lambda_l d_l^{-\alpha}}\right)^{\delta_j}\right] \quad (5)$$

By considering the Poisson point process [36] and assuming that change of the arrival rate due to the specific selection condition is identical across participating UEs in an average sense, Equation 5 can then be approximated as the following equation:

$$Pr_{dec}(d_k) \cong \prod_{j=1}^{N_f}\left[\exp\left(-\tilde{\lambda}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} M(x_l, y_l)dx_l dy_l\right)\right]^{\delta_j} \quad (6)$$

where the following equation is plugged:

$$M(x_l, y_l) = 1 - \frac{1}{1 + d_k^{\alpha}\gamma_{thr}(x_l^2 + y_l^2)^{-\alpha/2}} \quad (7)$$

$$\tilde{\lambda} = E_{\lambda_l}\left[\frac{\lambda}{\lambda_l}\right] \quad (8)$$

TABLE 1: Different cases of pool selection policy for analysis

Type	80 %	20 %
Static 1	Non-roaming UEs	Roaming UEs
Static 2	Non-roaming UEs and Roaming UEs	
Dynamic	Non-roaming UEs and High-class roaming UEs	Normal-class roaming UEs

By plugging, we can find the decoding probability of UE k as the following equation:

$$Pr_{dec}(d_k) \cong \exp\left(-\frac{2\pi^2\cdot\tilde{\lambda}\cdot d_k^2\cdot\gamma_{thr}^{2/\alpha}}{\alpha\cdot\sin(2\pi/\alpha)}\right) \quad (9)$$

$$= \exp\left(-K\cdot\tilde{\lambda}\right) \quad (10)$$

where the following equation applies:

$$K = \frac{2\pi^2\cdot d_k^2\cdot\gamma_{thr}^{2/\alpha}}{\alpha\cdot\sin(2\pi/\alpha)} \quad (11)$$

According to the derived equation, decoding probability in different cases of D2D resource pool selection policy is studied. The equation of decoding probability means that density of signals and interferences are caused by the arrival rate of each, and SINR is also impacted by the difference of each arrival rate. When experienced SINR is over the threshold, decoding is successful. So we can infer that change of D2D resource pool affects the arrival rate of the UEs in the specific resource pool as well as the decoding probability of the resource pool. Under the broadcast system, in average sense, the overall decoding probability of participating UEs in the resource pool is same regardless of the type of UEs – high or normal class. Total resources are divided into two pools; one is the high-class pool and the other is the normal-class pool. The ratio of two pools is 80% to 20%, as shown in Table 4. First static case as a conventional scheme, i.e., static 1, assumes that all roaming UEs are configured to select only normal-class pool for any type of traffic. In second static case, i.e., static 2, we assume that all roaming UEs select only the high-class pool for any type of traffic, but is not allowed to select the normal-class pool. For the last case, i.e., dynamic, we assume that roaming UEs having high-class traffic selects the high-class pool and other roaming UEs with normal-class traffic resides in the normal-class pool.

To verify the proposed scheme, the simulation results are obtained and compared with the numerical result. The simulator is coded using C++ tool and leverages it's libraries. These mainly consist of radio generation part to obtain signals and interferences, and traffic generation within the network.[1] Table 2 shows simulation parameters which are tuned to fit to the numerical analysis case. The simulation model assumes that sensing-based resource selection is applied for SA resource selection and explicit RPT collision avoidance

[1] Here, the value of k is set to 0.3

TABLE 2: Parameters for simulation.

Parameter	Value
Cell layout	Grid: Hexagonal, Cellsites: 19, sector/site:3, Wrap Around Opt5: Urban macro (1732m inter-site distance (ISD)) (all UEs outdoor)
UE drop	D2D links under 50 m [37]
Carrier frequency	2.4 [GHz]
UE TX power	20 [dBm]
Path loss model	ITU-R P.1411 D2D channel model Probability of LOS:NLOS=5:5
Shadowing	Log-normal distribution with 4 [dB]
Small scale fading	30 km/h velocity
Noise figure	7 [dB]
Implementation loss	8 [dB]
Frame structure	44 RBs & 40 subframes

TABLE 3: Parameters for Numerical Analysis.

Parameter	**Value**
d_k	Distance between TX UE and RX UE
$P_{r_{dec}}(d_k)$	Probability UE received SA message from UEk
γ_r	SINR value of a RX UE
γ_{thr}	Minimum SINR for decoding SA message
Pathloss model	Exponential pathloss model
Fading	Raylegh fading with mean 1
$P_{tx}[W]$	Transmit power

is applied for data resource selection. UE deployment area is 500 m x 500 m, the D2D link range is set randomly in [0.1, 50] m, the number of D2D links is set to [1, 81] (depending on the high-class and normal class ratio), the RX UE sensitivity is set to -76 dBm, with consensus scheduling method, and carrier sensing threshold is set to 9dB. The simulation is run for 5 sec. for up to 200 iterations. In Fig. 8, two curves from numerical analysis and simulation fits tightly. It is noted that the decoding probability from the simulation is calculated from throughput results in the sense of capacity theorem (a.k.a. Shannon–Hartley theorem). It means that the calculated PER (Packet Error Rate) is different from the actual one since the PER is regulated to keep it under the target PER, owing to the sensing-based SA resource selection. It has, however, a side-effect that packet delay increases as waiting time goes until UE takes an opportunity to transmit. A total packet delay comprises of a queueing delay and a transmission delay, but the last is negligible. Figure 9a shows the trend of increasing delay according to varying loading ratios. On the other hands, Figure 9b shows that the actual PER is well suppressed near to the target PER which is set to 0.01 in general. The decoding probability is calculated in different loading ratios between non-roaming (Ln) and roaming (Lr) UEs, varying from 9:1 to 1:9. Higher loading in the normal-class pool, worse to the decoding probability of the roaming UEs in the static pool selection case. On the other hand, in the dynamic pool selection case, high-class UEs among the roaming UEs select high-class pool and do not suffer from the higher congestion. For the sake of simplicity, the representative value K of a deployment condition is assumed to be set as 0.01, 0.02, and 0.03. In Fig. 10a, the decoding probability of the roaming UEs at the normal-class pool decreases as the loading of the normal-class pool goes higher. The decoding probability in the dynamic selection case, however, gets higher than that in the static selection case, when the value K is same.

TABLE 4: Different cases of pool selection policy for analysis

Type	**80 %**	**20 %**
Static 1	Non-roaming UEs	Roaming UEs
Static 2	Non-roaming UEs and Roaming UEs	
Dynamic	Non-roaming UEs and High-class roaming UEs	Normal-class roaming UEs

In the dynamic pool selection case, UEs demanding high-class D2D channels select the high-class pool. The class-aware selection makes more balanced load distribution as shown at the Fig. 10c compared to the Fig. 10b. Since the congested situation at the normal-class pool is so harsh, there is no doubt that the static pool selection shows a poor decoding performance. The fair comparison is possible by adding another static high-class pool selection where roaming UEs is configured to always select the high-class pool. Figure 10d shows that dynamic pool selection is still superior to the static high-class pool selection which called as second static pool selection.

VI. Conclusion

A D2D roaming means that a specific D2D channel and service continues seamlessly on the national coverage. Existing roaming in telecom may not be fully feasible for D2D

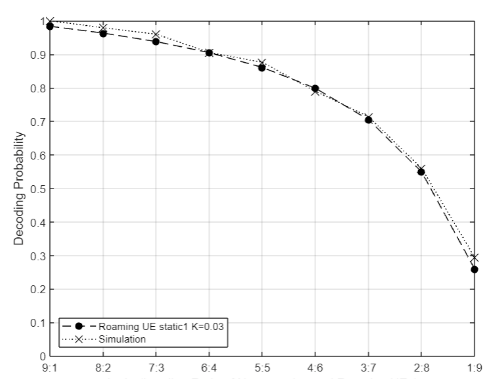
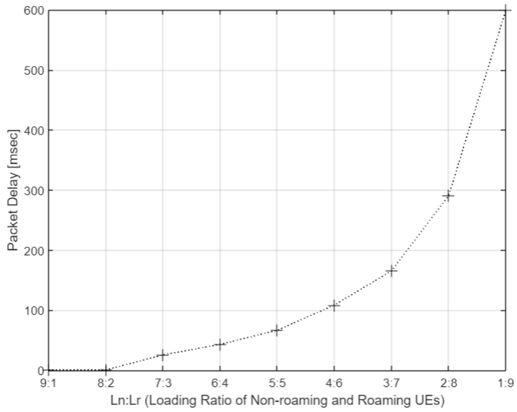
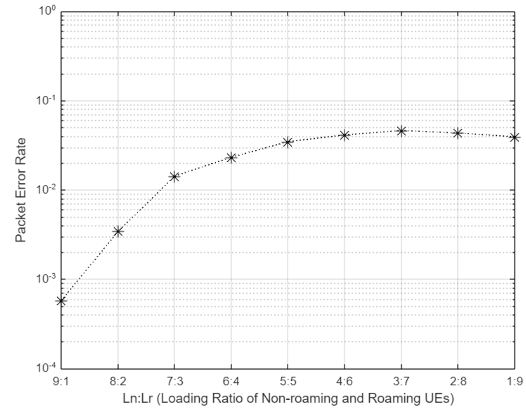


FIGURE 8: Decoding probability of roaming UEs.

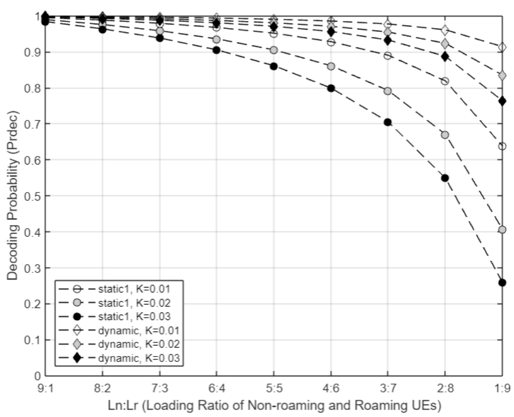


(a) Total packet delay.

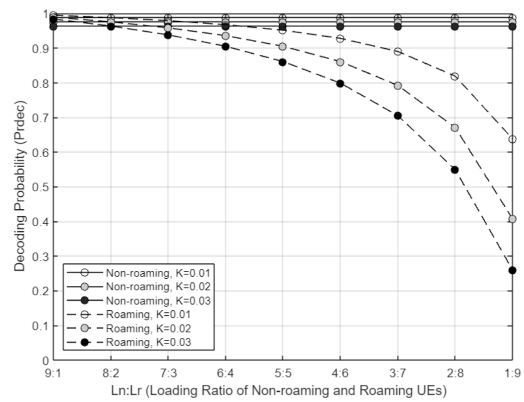


(b) Actual PER.

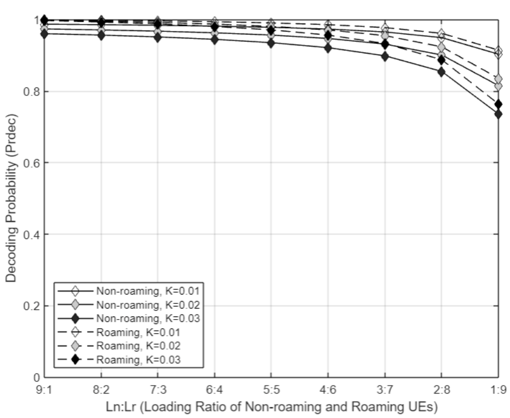
FIGURE 9: Delay and PER from simulation results.



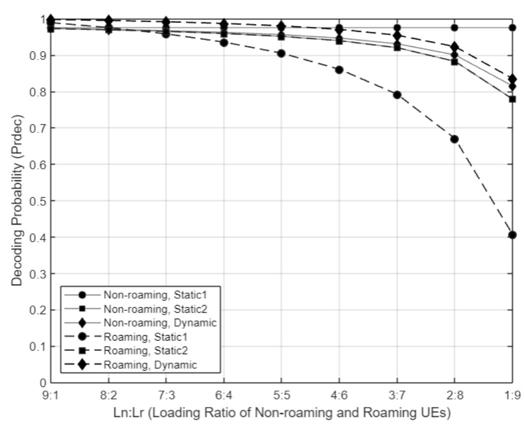
(a) Roaming UEs in static and dynamic pool selection cases.



(b) Non-roaming and roaming UEs in cases of static pool selection.



(c) Result of non-roaming and roaming UEs in cases of dynamic pool selection.



(d) Result of non-roaming and roaming UEs in static and dynamic pool selection cases.

FIGURE 10: Decoding probability from analytics results (at K=0.02).

scenarios since the conventional roaming agreement within operators is designed for internet protocol (IP) sessions which are established at core network. Upcoming D2D use-cases demand a fine granular service policy and a dynamic resource assignment according to the policy. It requires that RAN should manage those dynamic service types and flexible resource allocation. Since the security process between central points is replaced by the decentralized security process between the visiting network and the UE, the burden to verify the identity and authorize for service is lessen and the delay until the D2D resource allocation is reduced as well. The proposed D2D roaming framework supports three technical requirements, including IAM, trusted computing, and D2D resource pool selection, assisted by the blockchain system. The blockchain-assisted D2D roaming framework and a numerical analysis present the benefit from the dynamic D2D resource pool selection. The DID-based authorization and service–aware network configuration enable the roaming UE's suitable resource pool selection on the service demand dynamically. The freedom of resource selection avoids congestion due to the inefficient resource utilization. It shows the higher decoding performance in a simple scenario and is expected to be more beneficial in the complicated scenario in D2D roaming.

REFERENCES

[1] X. Lin, J. G. Andrews, A. Ghosh, R. Ratasuk, An overview of 3GPP device-to-device proximity services, IEEE Communications Magazine, April 2014, vol. 52, no.: 4, pp. 40-48.

[2] J. Liu; N. Kato; J. Ma; and N. Kadowaki, Device-to-Device Communication in LTE-Advanced Networks: A Survey, IEEE Commun Surv. and Tuts., vol. 17, no. 4, pp. 1923–1940, 2015.

[3] S.-Y. Lien; C.-C. Chien; F.-M. Tseng; T.-C.n Ho, 3GPP device-to-device communications for beyond 4G cellular networks, IEEE Commun. Mag., vol. 54, no. 3, pp. 29 - 35, 2016.

[4] X. Xu, H. Wang, H. Feng, C. Xing, Analysis of device-to-device communications with exclusion regions underlaying 5G networks, Trans. Emerg. Telecommun., 2015, vol. 26, no. 1, pp. 93–101, 2015.

[5] G. Fodor, E. Dahlman, G. Mildh, S. Parkvall, N. Reider, G. Miklós, Z. Turányi, Design aspects of network assisted device-to-device communications, IEEE Commun. Mag., vol. 50, no. 3, pp. 170–177, 2012.

[6] L. Lei, Z. Zhong, C. Lin, X. Shen, Operator controlled device-to-device communications in LTE-advanced networks, IEEE Wirel. Communs., vol. 19, no. 3, pp. 96–104, 2012.

[7] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, S. Li, G. Feng, Device-to-device communications in cellular networks, IEEE Commun. Mag., vol. 56, no. 4, pp. 49–55, 2016.

[8] F. Baccelli, N. Khude, R. Laroia, J. Li, T. Richardson, S. Shakkottai, S. Tavildar, X. Wu, On the design of device-to-device autonomous discovery, in: 2012 IEEE Proceedings of Fourth International Conference on Communication Systems and Networks (COMSNETS), pp. 1–9, 2012.

[9] Haiqiao Wu; Xiang Gao; Shaoyi Xu; Dapeng Oliver Wu; Peng Gong, Proximate Device Discovery for D2D Communication in LTE Advanced: Challenges and Approaches, IEEE Wireless Commun., , vol. 27, no. 4, pp. 140–147, 2020.

[10] S.-Yu Lien, C.-C. Chien, G. S.-Tsz Liu, H.-L. Tsai, R. Li, Y. J. Wang, Enhanced LTE Device-to-Device Proximity Services, IEEE Commun. Mag., vol. 54, no. 12, pp. 174 - 182, 2016.

[11] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, 2008 Available: https://bitcoin.org/bitcoin.pdf.

[12] N. Szabo, Smart contracts: building blocks for digital markets, 2018. Available: URL http://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf

[13] V. Buterin, Ethereum: A next-generation cryptocurrency and decentralized application platform, Bitcoin Magazine, 23, 2014. Available: https://bitcoinmagazine. com/articles/ethereum-next-generation-cryptocurrency-decentralized-application-platform-1390528211/.

[14] S. Šimunić; D. Bernaca; K. Lenac, Verifiable Computing Applications in Blockchain, IEEE Access, vol. 9, pp. 156729 – 156745.

[15] H. Amler, L. Eckey, S. Faust, M. Kaiser, P. Sandner, B. Schlosser, Defi-ning defi: Challenges & pathway, in: 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pp. 181–184, 2021.

[16] B. Benshoof, A. Rosen, A. G. Bourgeois, R. W. Harrison, Distributed decentralized domain name service, in: 2016 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), pp. 1279–1287, 2016.

[17] Q. Zheng, Y. Li, P. Chen, X. Dong, An innovative IPFS-based storage model for blockchain, in: 2018 IEEE/WIC/ACM international conference on web intelligence (WI), pp. 704-708, 2018.

[18] H. Zhu, Y. Wang, X. Hei, W. Ji, L. Zhang, A blockchain-based decentralized cloud resource scheduling architecture, in: 2018 IEEE International Conference on Networking and Network Applications (NaNA), pp. 324–329, 2018.

[19] M. F. Galmés, A. Cabellos-Aparicio, Decentralised Internet Infrastructure: Securing Inter-Domain Routing (demo), in: IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 10–13, 2021.

[20] J. C. Song, M. A. Demir, J. J.Prevost , and P. Rad. Blockchain design for trusted decentralized IoT networks. In IEEE 2018 13th Annual Conference on System of Systems Engineering (SoSE), pp. 169-174, 2018.

[21] R. H. Kim; H. Noh; H. Song; G. S. Park. Quick Block Transport System for Scalable Hyperledger Fabric Blockchain Over D2D–Assisted 5G Networks, IEEE Trans.s on Net. and Serv. Manag., vol, 19, no. 2, 2022.

[22] S. Guzey, G. K.-Kurt, Anas Mhaish, E. Ozdemir, N.Tavakkoli, Secure Device-to-Device Caching With Blockchain, IEEE Internet of Things Journal, vol. 9, no. 20, 2022.

[23] Y. Peng, T. Cui, B. Shen, F. Lin, X. Huang, and Q. Chen, Blockchain-assisted D2D Data Sharing in Fog Computing, IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), 2022.

[24] S. V. Jansi Rani; Iacovos I. Ioannou; P. Nagaradjane, C. Christophorou, V. Vassiliou; H. Yarramsetti, S. Shridhar, L. Mukund Balaji, A. Pitsillides, A Novel Deep Hierarchical Machine Learning Approach for Identification of Known and Unknown Multiple Security Attacks in a D2D Communications Network, IEEE Access, vol. 11, 2023.

[25] R. Hasan; Md. A. Amin; S. Dobir Hossain; Md. I. Abdullah, Blockchain-Based Key Sharing Mechanism for IoT Device-to-Device (D2D) Secure Communications, 2023 IEEE International Conference on Telecommunications and Photonics (ICTP), 2023.

[26] S. T. Siddiqui, Integrating IoT and Blockchain-Enabled Device-to-Device Communication to Improve Privacy in Intelligent Quarantine Environments, 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 2023.

[27] A.Tankovic, T. Markesic; E. Kaljic, Blockchain-based Protocol for Active Tracing of IP Traffic in 5G/6G Networks, 2024 23rd International Symposium (INFOTEH), 2024.

[28] D. Das,U. Ghosh, N.Evans; S. Shetty, Blockchain-Enabled Secure Device-to-Device Communication in Software-Defined Networking, 2024 IEEE International Conference on Communications Workshops (ICC Workshops), 2024.

[29] Y. Li, Z. Guo, T. Yang, L. Jiang, M. Li, Satisfied Matching-Embedded Social Internet of Things for Content Preference-Aware Resource Allocation in D2D Underlaying Cellular Networks, IEEE Internet of Things Journal, vol. 9, no. 11, 2023.

[30] G. Khekare, S. Gambhir, I. S. Abdulrahman, C. M.Sai Kumar, V. Tripathi, D2D Network: Implementation of Blockchain Based Equitable Cognitive Resource Sharing System, 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2023.

[31] J. Xu, S. Wang, A. Zhou, F. Yang, Edgence: A blockchain-enabled edge-computing platform for intelligent IoT-based dApps, China Commun. 17(4), 2020, 78-87.

[32] D. Miller. Blockchain and the internet of things in the industrial sector.IT Professional, vol. 20, no. 3, pp. 15 – 18, 2018.

[33] X. Li, P. Russell, C. Mladin, C.Wang, Blockchain-enabled applications in next-generation wireless systems: Challenges and opportunities, IEEE Wirel. Commun., vol. 28, no. 2, pp. 86-95, 2021.
[34] J. G. Andrews, F. Baccelli, R. K. Ganti. A tractable approach to coverage and rate in cellular networks, IEEE Trans. Commun. vol. 59, no. 11, pp. 3122-3134, 2021.
[35] A. Papoulis, S. U. Pillai, Probability, random variables and stochastic processes, 4th edition, McGraw-Hill, 2002.
[36] D. Stoyan, W. S. Kendall, S. N. Chiu, J. Mecke, Stochastic geometry and its applications, John Wiley & Sons., 1996.
[37] 3GPP, 3GPP TR 36.843 V12.0.1 TSG RAN Study on LTE D2D proximity services; radio aspects, Third Generation Partnership Project, 2014. URL https://www.3gpp.org/dynareport/36843.htm