TÜBİTAK

Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2022) 30: 2165 – 2178
© TÜBİTAK
doi:10.55730/1300-0632.3931

Two-layered blockchain-based admission control for secure UAV networks

Müge EREL-ÖZÇEVİK[*]
Department of Software Engineering, Manisa Celal Bayar University, Manisa, Turkey

Received: 13.12.2021 • **Accepted/Published Online:** 02.06.2022 • **Final Version:** 28.09.2022

Abstract: The frequent replacement requirement of UAVs for recharging outputs an extreme number of messaging for admission control of end-users. There are many studies that try to optimize the network capacity in an energy-efficient manner. However, they do not consider the security of data and control channels, which is the urgent requirement of 5G. Blockchain handles secure systems. However, the high numbered transactions in blockchain may cause bottlenecks while considering computational delay and throughput of end-user. In UAVs, a high percentage of battery is consumed for computational tasks instead of communication tasks. Therefore, to handle security by considering the computational needs, this paper proposes a novel two-layered blockchain-based admission control in UAV networks. It has two layers named as side-chain for UAVs and off-chain for end-users building in a decentralized manner. In the former one, the data bearer of end-users is protected by the side-chain of each transaction which is signed by admitted end-users and UAVs. Here, each transaction includes a unique transaction id, nonce value, IMSI of the user, RNTI of UAV, signed data, and hash value. In the latter one, the off-chain is built by signing admission contracts between users in a decentralized manner and the Merkle tree is constructed for the off-chain where the root hash is only stored in a side-chain. Then, the number of transactions that should be validated is extremely decreased. Moreover, PoS is used for the validation of transactions where the validator is selected randomly instead of the competition requirement as in PoW. A novel blockchain-based admission control algorithm isolates readmission control of end-users to 5G core-side during UAV replacement. According to performance evaluation, the proposed approach serves end-users by 64.2% better QoS than the conventional one during UAV replacement. Moreover, it keeps edge delay in acceptable range by using Merkle tree and PoS.

Key words: UAV networks, blockchain, 5G, admission control, Merkle tree

1. Introduction

Recently, unmanned aerial vehicles (UAV) networks have been used in many special cases such as sport events, natural disasters, and parades. Thanks to its adaptive altitude, it enables several applications which meet the high demand of 5th generation (5G) users [1]. The replacement characteristic for recharging of UAV also maintains the endurance of network [2]. There are many challenges in UAV networks such as coordination of drones, collision avoidance, completeness seeking and the replacement problem due to limited battery etc. [3]. Wireless sensor network (WSN) is known to be an energy-efficient way to longer the network lifetime with low powered data aggregation [4]. However, the case studies for UAV networks carries high traffic intense while compared WSN. Therefore, the replacement requirement of UAV for recharging becomes frequently [5, 6].

In the literature, there are many studies that try to solve aforementioned challenge by enhancing network capacity and decreasing the UAV replacements in an energy-efficient way. In [7], a trajectory control problem is formalized to maximize the capacity of UAV network in a single cell. In [8], it is indicated that each drone

[*] Correspondence: muge.ozcevik@cbu.edu.tr

is self-organized by executing distributed decision making. In [9], the flight strategy is performed by proposed distributed delay optimization algorithm. In [10, 11], there is joint optimization for trajectory planning and resource allocation problem.

However, these studies do not consider the security of data and control channels. The integration of many contents in 5G such as enhanced mobile broadband (eMBB), ultrareliable low latency communication (URLLC), and massive machine type communication (mMTC) result several challenges for security, privacy, data integrity etc. [12]. The security of data transmission is an urgent requirement of 5G networks. The protecting privacy of user equipment (UE) has become more challenging issue due to broadcasting in wireless channel. To overcome security challenge, blockchain can be implemented in many areas in 5G [13]. It builds a secure system without any centralized authority. It decreases the cost of secure system implementation by increasing the number of transactions while comparing conventional database systems. Here, the number of transactions in a block can be one or more. Generally, each transactions includes unique transaction id, nonce value, the hash value of previous block, the data signed by the peers etc. The validation of blocks is performed by checking the hash values in a blockchain. In the study [14], BlockWare is proposed as a wireless blockchain which tries to meet 5G applications. The blockchain construction and block validations are computed on the core side of 5G network where the edge computation does not considered. Moreover, in the paper [15], the spectrum sharing is under consideration by blockchain assisted 5G network. Here, centralized authority challenge is tried to be overcome by blockchain as a service platform. Again, network functions are securely used by blockchain controlled core side of 5G network. There is another study that proposes blockchain enabled authentication to remove unnecessary procedures between heterogeneous cells in 5G [16]. In [17], the smart contract between mobile operator and end-user is controlled by distributed blockchain. Here, spectrum sharing is the main data in blockchain assisted contracts. In these studies, the proof of work (PoW) is used for the validation of temporary blocks. Nevertheless, these studies do not consider the computational load of such validation procedure and do not give implementation details of edge side 5G networks in UAVs by handling low operational and capital expenditures (OPEX/CAPEX) as 5G requirement.

While considering implementation of blockchain on UAV networks, the high number of transactions outputs from end-users may cause a bottleneck challenge while considering the delay and throughput in transaction validation. Because, the transaction blocks may be build faster than processing of transactions. In [18], there is an analysis for UAV networks in terms of communication and computational cost. Accordingly, the battery is mostly consumed for computational tasks. Therefore, the PoW for transactions may cause unacceptable computational delay in UAVs in case of using highly secure hashing algorithms [19, 20]. PoW is a competitive approach that requires high computational power. For example, Bitcoin uses PoW to generate unique block identifier. Winner is selected according to be first validator who finds a unique value of a block that outputs; for example, finding a combination that outputs the first four digit zero in hashed data. It is significant to be first validator in order to transform its energy power to coin. However, there is no need to produce a coin in UAV admission control. It is closed architecture. Therefore, less computational work is required for transaction validation in a blockchain. On the other hand, proof of stake (PoS) where Ethereum currently uses is built on randomly selected validators instead of competing to find unique identifier. It highly decreases the processing time for temporary block validation and it also overcomes competing challenge of PoW [21–23].

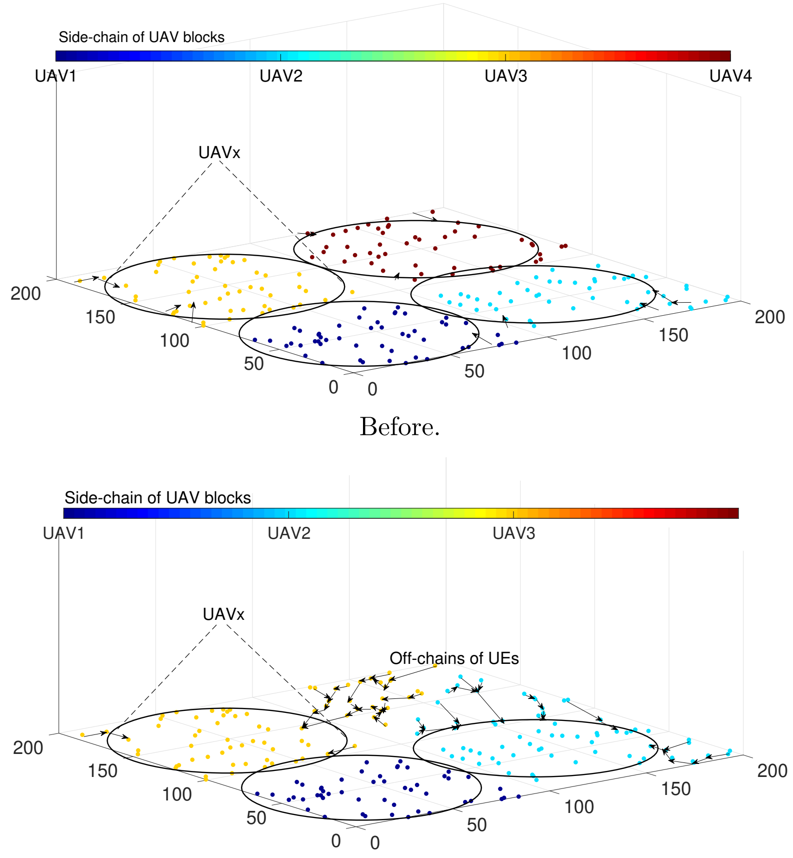
There are also some studies that focus on security in UAV networks in the literature. In [24], the security in 5G enabled drone communication is considered into such subareas: the privacy of blockchain, data, and trajectory of drones. Here, asymmetric encryption algorithm is proposed to handle security of data while building blockchain of drones. To overcome lack of admission control in 5G based UAV stations, another study claims that drones can be served as a service to increase the coverage area and handle the computational requirement of blockchain based applications in 5G [25]. It is supported by fog and edge computing in the core side of 5G network. However, they do not consider the landing case of UAV due to limited battery life time and readmission procedure should be isolated to end-users in an efficient way. Conventionally, by landing notification of UAV due to battery limitation, the admitted user should be readmitted to remained UAVs. During readmission phase the quality of service (QoS) of end-user has extremely damaged due to extreme number of messaging in admission control procedure. Instead of frequently readmission signaling during UAV replacement, off-chain is proposed to serve end-user by remained UAVs. For the proof of authentication in limited powered systems, Merkle tree is proposed to be used [26, 27]. This data structure outputs high data integrity and low performance overhead [**?**]. It is also a proof system for structured domains [28]. The implementation of such data structure for low complex validation in blockchain based UAV network is open issue. In the light of these, this paper proposes a novel two-layered blockchain to meet secure UAV networks with Merkle tree authentication in off-chain. Here, there is no readmission procedure which creates huge amount of control signalling data. Because off-chain transactions are not stored in two-layered blockchain, new admission procedure of user is isolated to core-side in secure way. As a result, the whole contributions of two-layered blockchain based admission control are given below:

- A novel blockchain architecture is proposed into two-layered named as ”side-chain” of UAVs and ”off-chain” of end-users.
- The transactions are hashed and validated by using different data structures as List and Merkle tree.
- Layer 1: Side-chain of UAVs
  - UAVs builds side-chain to protect data privacy of each end-user who is admitted to itself.
  - Each transactions of end-user are only stored for layer 1.
- Layer 2: Off-chain of end-users
  - The end-user who is admitted to landing UAV signs a novel admission contract by executing asymmetric encryption algorithm in decentralized manner.
  - The aggregation of such contracts builds a novel off-chain of end-users to admit remained UAV.
  - The chain is built by using Merkle tree; and therefore, the root hash is only stored in side-chain of UAVs.
  - A novel decentralized admission control algorithm is implemented cost-efficiently according to OPEX/CAPEX thanks to not storing any transaction block in off-chain until a new UAV replaced in a side-chain.
  - It isolates admission control of end-users to UAV network.

The rest of paper is organized as follows: In Section 2, the proposed network architecture is detailed in terms of both considering two layers of proposed blockchain in UAV networks. In Section 3, the proposed system model is given by handling communication diagram for UAVs and their serving end-users with a novel admission control algorithm. In Section 4, the performance evaluation of proposed system is given. As a result, the paper is summarized by giving the conclusion and the future work in Section 5.

2. Network architecture

The proposed network architecture for blockchain based UAVs is given in Figure 1. There are M UEs and N UAVs in a topology. For example, there are 4 UAVs that serve whole topology where the UEs are randomly distributed in the figure. Before the landing of UAV due to limited battery as shown in Figure 1a, each UE starts random access and radio resource control setup procedure to admit UAV and to allocate a resource block with a radio bearer [29]. In 5G, UE has three different states named as new radio (NR) RRC_CONNECTED, NR RRC_INACTIVE and NR RRC_IDLE. Initially, UE is in RRC_IDLE and after the connection with UAV is established the state of UE changes as either RRC_CONNECTED or RRC_INACTIVE [30]. If there is no data for UE and there are only mobility monitoring and paging signalling, this state is called RRC_INACTIVE. In other case, if there is data for UE in uplink/downlink manner, it is in RRC_CONNECTED state. Here, the admission control procedure creates a secret radio bearer between UE and UAV, and then, UE is in RRC_CONNECTED state. This radio bearer is unique by using radio network temporary identifier (RNTI) of UAV and international mobile subscriber identity (IMSI) of UE. The mobility of UE is controlled by core side equipments in 5G NR. Therefore, only RRC_CONNECTED state of UE is considered by UAV acting as a NR.



Before.

After.

Figure 1. A blockchain based UAV network architecture before and after UAV landing.

While executing admission control of UEs, the data of UEs are protected via list based blockchain. Here, each radio bearer assignment between UE and UAV is stored by a transaction in a block. It includes unique transaction id, nonce value, IMSI of UE, RNTI of UAV, data signed by UE and UAV, previous hash value of a block, and hash of whole block.

In Figure 1b, the admission of UEs is shown in the case of UAV landing. During replacement of UAV, UEs build off-chain in decentralized manner until reaching a root UE who is already admitted to a UAV that still able to serve end-user over side-chain of blockchain. This action is taken with landing notification of UAV sending to UEs who are admitted to itself. Namely, each UE is reconnected to network thanks to off-chain of UEs before closing the connection with landing UAV. The data structure of blockchain is also exemplified in Section 3. In a hierarchical tree, it is proposed to have two layers named as side-chain of UAVs and off-chain of UEs. In layer 1, each UAVs are a part of side-chain; whereas in layer 2, UEs build off-chain of UAVs. Each transaction (hashed data) of UEs is stored via UAVs' blockchain in layer 1 of Merkle tree. The charging of UEs can be also executed over such stored transactions without any need of off-chain storage. Therefore, the replacement of UAVs is performed seamlessly to UE thanks to two-layered blockchain architecture. Moreover, the transactions in off-chains are not recorded into blockchain which would decrease the cost on algorithm while considering transaction validation performed in UAVs and relay UE. This procedure is isolated to UAV backbone and it decreases the control signalling of UEs while readmission to network. Here, the blockchain construction adds extra delay on traffic flow of end-user which is under acceptable range. The details of proposed method are given in following section.

3. Proposed system model

In this section, there are three subsections to determine the details of proposed two-layered blockchain based admission control in UAV networks. Firstly, the communication diagram of UAV and UEs is given, then the data structure of blockchain layers is exemplified; and finally, the proposed admission control algorithm is given.

3.1. Communication diagram

In Figure 2, the communication diagram of blockchain based UAV networks is given. By landing notification of UAV due to battery limitation, admitted UE pairs start to build an off-chain by signing admission contract between each other. They use private keys to sign this contract in order to use a channel over UE. Here, one is in producer role, whereas the other one is in consumer role in terms of channel usage. This transaction is hashed/encrypted by SHA-256 algorithm [19]. These data can be decrypted by using public keys in both UAVs and relay UEs which has a role as Merkle root. As shown in Figure 2, UE_1 admitted to UE_2 and this transaction is added to off-chain of UEs. Afterwards, UE_2 and UE_3 signs a contract; and now, UE_2 becomes as consumer whereas UE_3 becomes producer in terms of allocated channel usage. This transaction is also hashed and added to off-chain of UEs. This chain is ended until reaching a UE who is in producer role and has already allocated channel from remained UAV. Then, the off-chain goes up one layer and ended by Merkle root. Namely, it reaches side-chain of UAV blocks. Here, the UE who is active radio bearer between remained UAV acts as a producer in a blockchain and builds the transactions in layer 1 by using Merkle tree hashing mechanism. The side-chain of UAVs is rebuilt in terms of routing strategy. However, there is no strict change in this chain before and after UAV replacement. Here, a transaction of landing UAV is dropped from side-chain and off-chains of UEs are added to side-chain via relay UE who is Merkle root of off-chain.

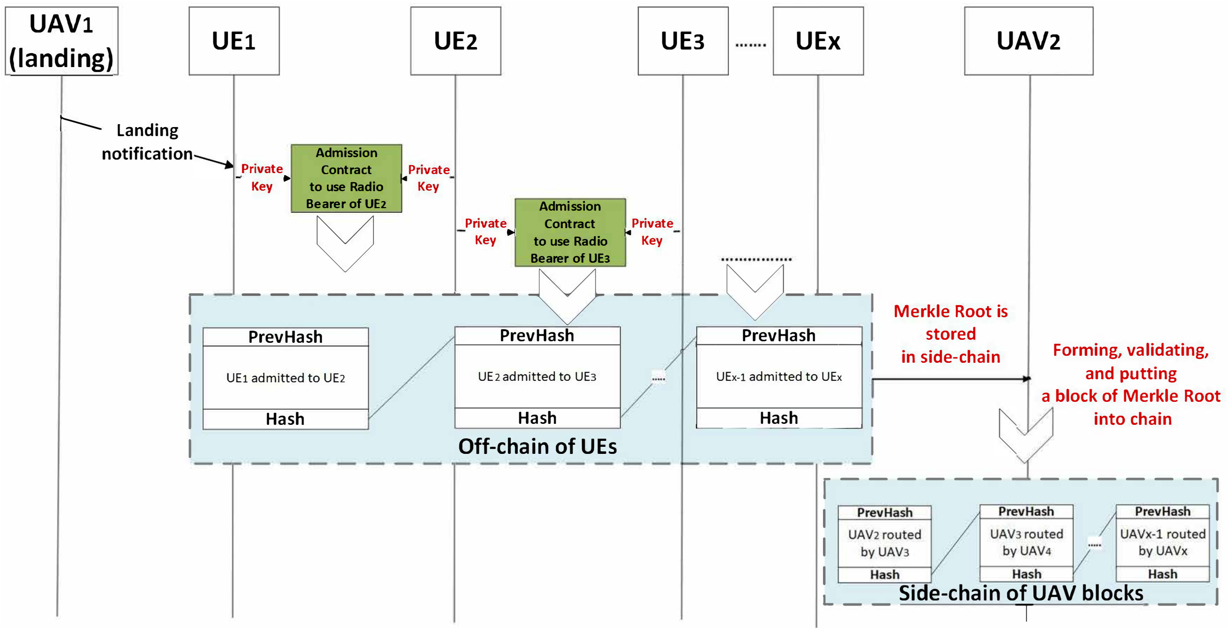
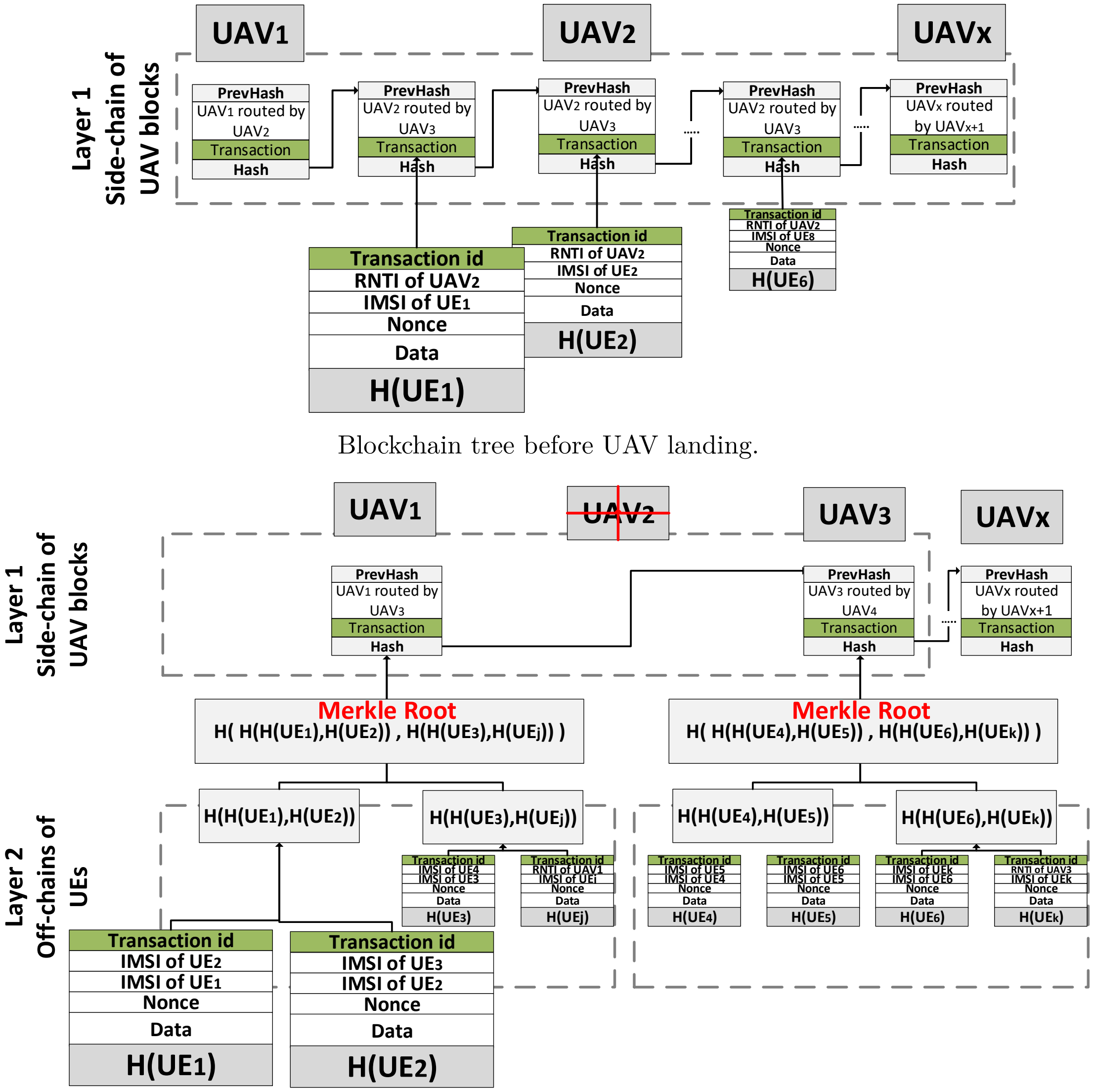


Figure 2. Communication diagram of blockchain based UAV networks.

3.2. Data structures of blockchain

In Figure 3, the data structures used in the construction of blockchain are exemplified. Before and after UAV landing are given in Figures 3a and 3b, respectively. Before, each UE is admitted to UAV and their data is securely routed over list based blockchain which is named as side-chain. For example there are 6 UEs admitted to UAV_2. Each transaction of UE includes transaction id, id of producer (RNTI of UAV), id of consumer (IMSI of UE), nonce value, data of UE and hash value of whole transaction (H(UE)). Here, the producer of each UEs are UAV_2. Each block in a side-chain shows the smart contract between UE and UAV in admission control. It includes the hash value of previous block and forwarding rule. It takes transaction as a data and creates a hash value of whole block.

As seen in Figure 3b, after UAV landing, off-chain between UEs is constructed by Merkle tree. To decrease processing cost on relay UE who has active radio bearer from remained UAV, Merkle tree is preferred to built an off-chain where the only the hash of Merkle root is stored in side-chain of UAVs. For example, 6 UEs of UAV_2 admit to closest UE until founding a relay UE that has active radio bearer in remained UAV. UE_1 admits to UE_2 in distributed manner. In a transaction, the producer id becomes IMSI of UE_2 and the consumer id becomes IMSI of UE_1. The hash of whole transaction (H(UE_1)) is shared as left subtree in Merkle tree. In the second transaction where UE_2 is admitted to UE_3, the hash of whole transaction H(UE_2) is shared for left subtree in Merkle tree. The transactions of UE_3 and relay UE (UE_j) are shared as right sub tree of Merkle tree. The root is calculated by relay UE_j. By using active radio bearer of relay UE, whole data in the off-chain is routed by UAV_3 (it was being routed by UAV_2 before landing). The second Merkle tree is also constructed for UE_4, UE_5, UE_6, and a relay UE_k who is admitted to UAV_3. Thanks to the tree construction in decentralized manner, both the security of data is handled and the cost of validation is also minimized by only storing hash value of the Merkle root. This data structure is going to be evaluated in terms of delay and the number of transactions to be executed for the validation in section 4.



Blockchain tree before UAV landing.

Blockchain tree after UAV landing.

Figure 3. The construction of blockchain tree before and after UAV landing.

3.3. Proposed blockchain based admission control algorithm

The proposed blockchain based admission control algorithm is shown in Algorithm 1. It shows executable functions running in decentralized manner in either UAVs or UEs. The admission control functions for UAVs and UEs are given between lines 1–8 and lines 9–24, respectively. In the first one, the UAV checks battery status continuously. If the batter is low as defined in line 3, it sends landing notification to admitted UEs. Therefore, UEs start to build off-chain to not loss connection through the internet. This message triggers UE as shown in line 11. If a UE is in consumer role, it admits to nearest UE in order to use this UE as a relay. They signs an admission contract by using private keys as shown in lines 13 and 15. If UE is in producer role, it is responsible to add the previous transactions to off-chain until it is being a consumer. The off-chain is built in decentralized manner by executing producer and consumer roles, respectively. It ends until reaching a UE who has already allocated radio bearer from remained UAV as defined in line 17. Namely, this UE is Merkle root and acts as a

Algorithm 1 Blockchain based admission control algorithm.

```
Require: UAVs' battery status
Ensure: Reconstruction of blockchain
 1: function Admission Control(UAV)                          ▷ Each UAV runs it in decentralized manner
 2:     while true do
 3:         if Battery is low then
 4:             Send landing notification to admitted UEs.
 5:             Delivery public keys of admitted UEs to previous UAV in side-chain.
 6:             Break
 7:         if Is there any landing/newcomer UAV in side-chain then
 8:             Reconsider routing path in side-chain.
 9: function Admission Control(UE)                           ▷ Each UE runs it in decentralized manner
10:     while true do
11:         if Landing notification from admitted UAV then
12:             if UE is in consumer role then
13:                 Sign an Admission Contract by a nearest UE by using private key.
14:             if UE is in producer role then
15:                 Sign an Admission Contract by a nearest UE by using private key.
16:                 Add transaction to off-chain.
17:                 if UE has already allocated readio bearer from remained UAV then    ▷ Merkle root role of relay UE
18:                     End off-chain and validate transactions in off-chain to add it as own child in Merkle tree.
19:                     Sends the block of transactions to UAV in side-chain.
20:                 if There is newcomer UAV to side-chain then
21:                     Reject off-chain from childhood.
22:         if There is a newcomer UAV in side-chain then
23:             Allocate radio bearer block from UAV.
24:             Built new transactions over UAV side-chain.
```

relay in a system. It ends off-chain and validates transactions in off-chain to add it as own child in Merkle tree as in line 18. It routed the block of transactions to side-chain; and then, the data of UEs being in off-chain are now routed over this UAV as shown line 19.

After landing cases and Merkle tree reconstruction, a new UAV can be placed to serve the topology. In that case, remained UAVs checks line 7; whereas, UE checks line 20. The routing path is reconsidering in side-chain of UAVs and the off-chain is rejected from childhood of Merkle root. Meanwhile, newcomer UAV allocates radio bearer to UEs in off-chain and the transactions are now routed over side-chain as before.

For the validations in this algorithm, the PoS is preferred. There would be the high number of transactions outputs from UEs in both off-chain and side-chain, PoW most probably increases the processing delay for the validation of transactions. Therefore, QoS of UE may decrease to unacceptable levels. While considering the cost effect of the proposed admission control algorithm on battery usage, it can be ignored in UAVs; because UAV spends the vast majority of energy for flight control instead of control and data signalling. The controlling channels and the security algorithms for forming and validation of chains do not cause a significant energy expenditure. By considering the huge amount of battery is used for computational tasks in UAV instead of communications task, the delay would become high if PoW is used for block validation [18]. With PoS validation, the validator is randomly selected according to its offering instead of contention requirement as in PoW to find unique identifier for each transaction [21–23]. According to the literature, the blockchain can be executed in low powered devices [20]. These proposed algorithms are performed in decentralized manner.

Using Merkle tree extremely decreases the number of transaction to be executed in validation. Thanks to using this data structure instead of list based chain in off-chain, the number of transaction that should be validated is extremely decreases that would keep the delay for validation process under acceptable level. In a worst case the form and validation of transactions takes O(M) where M is the number of user in a topology. Therefore, the cost analysis directly depends on the number of UAV (N). The total cost can be summarized as $O(M \cdot N)$. The delay analysis of extra cost caused by construction of blockchain is also given in following section.

4. Performance evaluation

In the performance evaluation, the blockchain is implemented by using Python based hashing algorithms. Afterwards, such real results are simulated by using MATLAB 2019b environment to handle delay analysis of UAV networks. The test-bed environment is run over 2.3 GHz Dual-Core Intel Core i5 based controller with 8Gb RAM. Initially, it is assumed that there is one transaction per UE in the topology. The number of UE is increased from 1 to 1000 per UAV, where the number of UAV is 10. The evaluation scenarios and performance parameters are summarized in Table . There exists four different evaluation scenarios named as off-chain, side-chain evaluations, depth of Merkle tree effect and landing simulation of UAV.

Table . The evaluation scenarios and parameters for performance evaluation.

Evaluation parameters	**Value**
Number of UE	1–1000
Number of UAV	10
Depth of Merkle tree	2–6
Landing probability of UAV	0.1–0.9

Evaluation scenario	**Results**	**Details**
Off-chain evaluation	Figure 4	Edge Delay(seconds) is considered according to increased number of UE as many as possible in off-chain.
Side-chain evaluation	Figure 5	Delay of blockchain (seconds) is observed by executing blockchain construction as the number of UE is increased in a side-chain where there is no off-chain.
Depth of Merkle tree effect	Figures 6 and 7	As the depth of Merkle Tree is increased, the number of transaction in a blockchain that needs to be validated is considered.
Landing simulation of UAV	Figure 8	Comparison of blockchain based admission control is evaluated on MATLAB 2019b with conventional case in terms of delay (second)

4.1. Off-chain evaluation

In Figure 4, off-chain is only considered part of blockchain to analyze the length of off-chain where the hash value of root is only stored in blockchain by using Merkle tree. Due to physical distance limitation between wireless nodes (UE), there is path loss on signal and the signal attenuation becomes high as the length of chain is increased. In this evaluation, the length of off-chain is increased as much as possible. According to technical reports, increasing the number of UE in an off-chain after 64 is not realistic [31, 32]. Therefore, the edge delay is evaluated in y-axis where the number of UE in off-chain is increased from 4 to 64. Namely, x-axis also shows the depth of Merkle tree from 2 to 6. The results are run in 10 times and the confidence interval is determined as 0.95. Then, this graph proves that the propagation delay is under acceptable range while the number of UE in the off-chain is increased as many as possible.

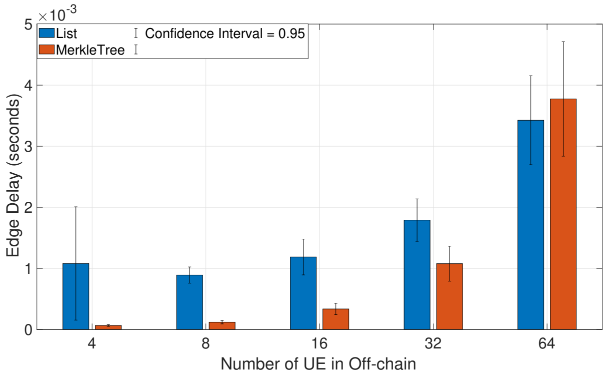


Figure 4. Edge delay in case of using different data structures in off-chain.

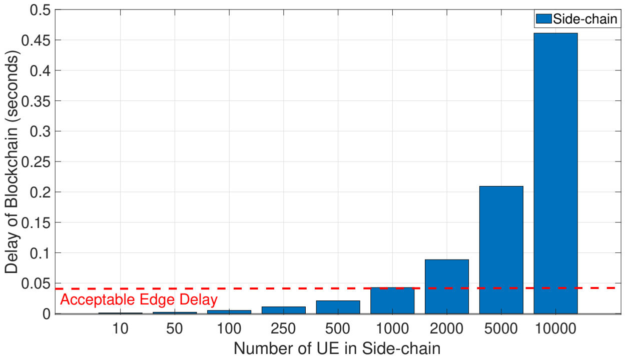


Figure 5. The total delay of blockchain when there is only side-chain.

According to that, as the number of UE is increased the edge delay becomes worse for both data structures which are list and Merkle tree. Until the number of UE in an off-chain is 32, Merkle tree outputs 1 ms less edge delay than using list based chain, because there is also processing time for validation of transactions for each step in list-based chain; whereas, there is only one validation in Merkle root in tree based chain. However, when the number of UE is 64, i.e. the depth of Merkle tree is 6; it results unacceptable edge delay than list-based construction because of extreme increase on recursive callings. It is significant to emphasize that the length of off-chain probably would be under 16 level, where the depth is under 4. While considering the physical distances between UEs and finally reaching a relay UE, the probability of having the length higher than 16 is low and nearly impossible. Therefore, the Merkle tree is preferred to build off-chain.

4.2. Side-chain evaluation

In Figure 5, the side-chain of blockchain is under consideration where there is only one layer in blockchain. Each radio bearer details of UE storing in a transaction is stored in a side-chain. Here, the number of transactions is exactly same with the number of UEs in one layered blockchain. Therefore, the result in this figure shows the total delay of blockchain. It proves that the length of side-chain can be increased up to 1000 by considering the blockchain delay effect on QoS of UE in conventional approach. As the total number of UE is increased form 2000 to 10000, the delay becomes unacceptable levels; whereas, it serves end-user with an acceptable edge delay (under a few msecs) until there is 1000 UEs in a side-chain. Thanks to using two-layered blockchain, the length of side-chain can be kept under 1000 with 10 long Merkle tree validation in off-chain per UAV in a topology.

4.3. Depth of Merkle tree effect

In Figure 6, the number of transaction which is stored in the proposed two-layered blockchain is given in y-axis where the landing probability of UAVs vary from 0.1 to 0.9 in a topology. When there is 1000 UE in a topology, the effects of building off-chain via Merkle tree and the depth of it are also given in this figure. For example, when the probability is 0.1 which means there is only one landing UAV at the same time, the off-chain decreases the number of transactions up to 906 by using Merkle tree where the depth is 4. Here, there is 10% less proof of work in proposed approach which directly decreases the processing delay in a blockchain. When the probability of landing is 0.5, the proposed admission control algorithm builds many more off-chain than lower probabilities. This reduces the less requirement on proof of work in a system. According to the results, there is nearly 50% less proof of work in the proposed approach. This gain can reach 85% when the landing probability is 0.9. However, 0.9 is not realistic in a real test-bed environment and it is acceptable as theoretic output. Therefore, the maximum gain is determined as 50% when the landing probability is 0.5. The whole cases for different number of UE in a topology are resulted in Figure 7. As the number of transaction increases, the number of proof processing for each transaction also increases which negatively affects the QoS of end-users. This effect is tried to be decreased by the depth of Merkle tree.

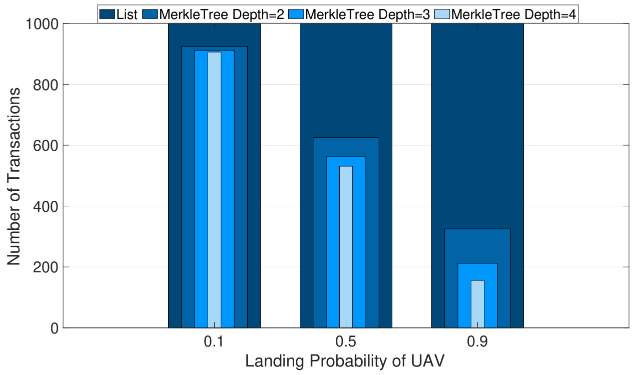


Figure 6. Number of transactions in blockchain when the number of UE is 1000.

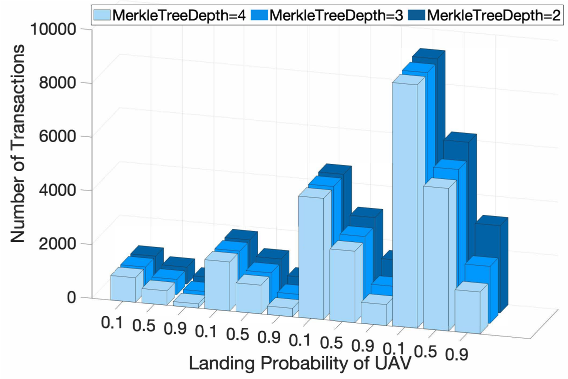


Figure 7. Number of transactions in blockchain for proof of work.

4.4. Landing simulation of UAV

In Figure 8, y-axis shows the total delay of blockchain whereas x-axis gives the simulation time per UE in UAV network. Here, the proposed admission control in UAV network is compared by the conventional one. The conventional approach is defined such that there is no blockchain implementation between UEs and UAVs, and the UE tries to readmitted to remained UAVs in landing case. The proposed one builds off-chain in distributed manner between UEs and adds them in blockchain of UAVs to securely route data of UE. Therefore, there is no need readmission process which brings extra overload with huge control signalling between UAVs and UEs; namely, the proposed two-layered blockchain based admission control isolates this procedure to UAV chain until a UAV is replaced due to battery change. During simulation, there are four phases for both approaches named as before UAV landing (0–30 ms), notification (30–40 ms), landing (40–50 ms), after a UAV replacement (after 50 ms). Before UAV landing, the proposed approach builds a side-chain between UAVs and each UE is added by a transaction to side-chain. Therefore, there is extra processing delay per UE in UAV. By running Python based codes in off-chain evaluation, it is shown that the results are under acceptable range when there is 1000 UE in a topology. The conventional one serves end-user better QoS during this phase. In case of landing notification sending from UAV due to the battery is low, there is extra control signalling to readmit UE to other UAVs in the conventional approach. This is observed as worsening on QoS of UE. In the proposed one, the off-chains are built in distributed manner; and therefore, there is also extra control signalling between UEs while signing admission contract. In landing phase, the UEs are served over two-layered blockchain in proposed admission control algorithm, and it results a few degradation on delay of UE which is higher value than acceptable range. However, there is extremely high increase on delay in conventional one due to blocking the connection from previous UAV and readmitting to remained UAVs. The delay can be reached up to 0.14 s which also resulted from the extreme queuing delay during readmission (Here, the queue sizes of UAVs and UEs are assumed as infinite. There would be packet drops if the queuing size is limited). This damage on delay is fading away in after UAV replacement phase and it can only be under acceptable edge delay after 64 ms in simulation time for conventional approach. In the proposed one, the delay of UEs has less degradation thanks to the isolated admission control of UE by two-layered blockchain. As a result, the proposed one serves end-user by 64.2% better QoS than conventional one and isolates the side-chain from such controlling procedures.

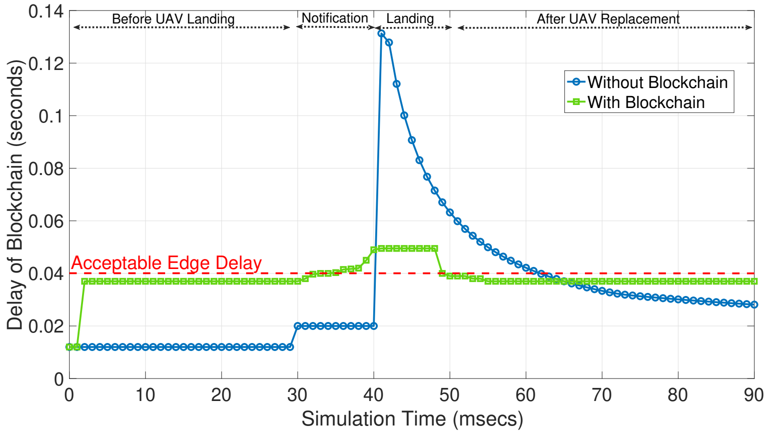


Figure 8. The total delay of blockchain comparison for conventional and proposed approach during a simulation.

5. Conclusion and future Work

In UAV based 5G networks, there is lack of studies that consider the security of communication. The different contents of 5G result several challenges for security which is urgent requirement in wireless channels of UAV. There are several blockchain implementations in 5G networks; but they do not consider the computational load and implementation details on UAV networks. The landing probability of UAV due to limited battery should be also considered to initiate the readmission procedure on end-user. In order to isolate this procedure to end-user, a novel two-layered blockchain is proposed for admission control in secure UAV networks.

In the proposed blockchain, each admission control procedure in radio resource control, allocating radio bearer is stored as a transaction. Each transaction includes unique transaction id, nonce value, IMSI of user, RNTI of UAV, data signed by user and UAV with a blockchain smart contract, previous hash value and hash value of whole block. The proposed blockchain has two layers named as side-chain of UAVs and off-chain of end-users. In the former one, the data privacy of end-users is protected by the side-chain of each transactions which are signed by admitted users of UAVs. In the latter one, the off-chain is built by signing admission contracts between end-user pairs in decentralized manner. Thanks to Merkle tree where the root hash is only stored in side-chin, it is proven by PoS where the validator is randomly selected and the number of transactions in off-chain that would be validated is extremely decreased. Therefore, the admission control of end-users is isolated to the core side of 5G during UAV replacement without any storage of transactions in blockchain. A novel blockchain based admission control algorithm is proposed and implemented cost-efficiently according to OPEX/CAPEX. According to the performance evaluation, the proposed approach serves end-user by 64.2% better QoS than conventional one during UAV replacement. Moreover, the extra computational delay for validation of transactions in UAVs is in acceptable range thanks to using different data structures in blockchain.

As a future work, the two-layered blockchain will be implemented in authentication mechanisms in network functions of 5G core side. Here, dynamic orchestration of network equipment will be performed by distributed software-defined networks (SDN) where the service providers use the physical infrastructure as a service.

References

[1] Mozaffari M, Saad W, Bennis M, Nam YH, Debbah M. A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems. IEEE Communications Surveys Tutorials 2019; 21 (3): 2334–2360. doi:10.1109/COMST.2019.2902862

[2] Ozcevik Y, Canberk B. Energy Aware Endurance Framework for Mission Critical Aerial Networks. Ad Hoc Networks 2019; 96: 101992. doi:10.1016/j.adhoc.2019.101992

[3] Macktoobian M, Gillet D, Kneib JP. Astrobotics: Swarm Robotics for Astrophysical Studies. IEEE Robotics Automation Magazine 2021; 28 (3): 92–101. doi:10.1109/MRA.2020.3044911

[4] Shen T, Ochiai H. A UAV-enabled Wireless Powered Sensor Network based on NOMA and Cooperative Relaying with Altitude Optimization. IEEE Open Journal of the Communications Society 2021; 2: 21–34. doi:10.1109/OJCOMS.2020.3042257

[5] Zhang Y, Mou Z, Gao F, Xing L, Jiang J et. al. Hierarchical Deep Reinforcement Learning for Backscattering Data Collection with Multiple UAVs. IEEE Internet of Things Journal 2021; 8 (5): 3786–3800. doi:10.1109/JIOT.2020.3024666

[6] Bozkaya E, Foerster KT, Schmid S, Canberk B. Airnet: Energy-Aware Deployment and Scheduling of Aerial Networks. IEEE Transactions on Vehicular Technology 2020; 69 (10): 12252–12263. doi:10.1109/TVT.2020.3019918

[7] Zhang S, Zhang H, Di B, Song L. Cellular UAV-to-X Communications: Design and Optimization for Multi-UAV Networks. IEEE Transactions on Wireless Communications 2019; 18 (2): 1346–1359. doi:10.1109/TWC.2019.2892131

[8] St-Onge D, Kaufmann M, Panerati J, Ramtoula B, Cao Y et al. Planetary Exploration with Robot Teams: Implementing Higher Autonomy with Swarm Intelligence. IEEE Robotics Automation Magazine 2020; 27 (2): 159–168. doi:10.1109/MRA.2019.2940413

[9] Li L, Wang M, Xue K, Cheng Q, Wang D et al. Delay Optimization in Multi-UAV Edge Caching Networks: A Robust Mean Field Game. IEEE Transactions on Vehicular Technology 2021; 70 (1): 808–819. doi:10.1109/TVT.2020.3045509

[10] Liu M, Wang Y, Chen Y, Jia H. Joint Stochastic Computational Resource and UAV Trajectory for Wireless-Powered Space-Air-Ground IoRT Networks. IEEE Access 2020; 8: 193728–193743. doi:10.1109/ACCESS.2020.3033615

[11] Ozcevik Y, Bozkaya E, Akkoc M, Erol MR, Canberk B. GA-based Energy Aware Path Planning Framework for Aerial Network Assistance. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems 2021; 8 (26). doi:10.4108/eai.13-4-2021.169186

[12] Tahir M, Habaebi MH, Dabbagh M, Mughees A, Ahad A et al. A Review on Application of Blockchain in 5G and Beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities. IEEE Access 2020; 8: 115876–115904. doi:10.1109/ACCESS.2020.3003020

[13] Wongthongtham P, Marrable D, Abu-Salih B, Liu X, Morrison G. Blockchain-enabled Peer-to-Peer Energy Trading. Computers & Electrical Engineering 2021; 94: 107299. doi:10.1016/j.compeleceng.2021.107299

[14] Li X, Russell P, Mladin C, Wang C. Blockchain-enabled Applications in Next-Generation Wireless Systems: Challenges and Opportunities. IEEE Wireless Communications 2021; 28 (2): 86–95. doi:10.1109/MWC.001.2000455

[15] Weerasinghe N, Hewa T, Liyanage M, Kanhere SS, Ylianttila M. A Novel Blockchain-as-a-Service Platform for Local 5G Operators. IEEE Open Journal of the Communications Society 2021; 2: 575–601. doi:10.1109/OJCOMS.2021.3066284

[16] Yazdinejad A, Parizi RM, Dehghantanha A, Choo KKR. Blockchain-enabled Authentication Handover with Efficient Privacy Protection in SDN-based 5G Networks. IEEE Transactions on Network Science and Engineering 2021; 8: 1120–1132.

[17] Gorla P, Chamola V, Hassija V, Ansari N. Blockchain based Framework for Modeling and Evaluating 5G Spectrum Sharing. IEEE Network 2021; 35 (2): 229–235. doi:10.1109/MNET.011.2000469

[18] Thammawichai M, Baliyarasimhuni SP, Kerrigan EC, Sousa JB. Optimizing Communication and Computation for Multi-UAV Information Gathering Applications. IEEE Transactions on Aerospace and Electronic Systems 2018; 54 (2): 601–615. doi:10.1109/TAES.2017.2761139

[19] Martino R, Cilardo A. SHA-2 Acceleration Meeting the Needs of Emerging Applications: A Comparative Survey. IEEE Access 2020; 8: 28415–28436. doi:10.1109/ACCESS.2020.2972265

[20] Tran TH, Pham HL, Phan TD, Nakashima Y. BCA: A 530-mw Multicore Blockchain Accelerator for Power-Constrained Devices in Securing Decentralized Networks. IEEE Transactions on Circuits and Systems I: Regular Papers 2021; 68 (10): 4245–4258. doi:10.1109/TCSI.2021.3102618

[21] Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT et al. Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. IEEE Access 2019; 7: 85727–85745. doi:10.1109/ACCESS.2019.2925010

[22] Li X, Xu J, Fan X, Wang Y, Zhang Z. Puncturable Signatures and Applications in Proof-of-Stake Blockchain Protocols. IEEE Transactions on Information Forensics and Security 2020; 15: 3872–3885. doi:10.1109/TIFS.2020.3001738

[23] Zaghloul E, Li T, Mutka MW, Ren J. Bitcoin and Blockchain: Security and Privacy. IEEE Internet of Things Journal 2020; 7 (10): 10288–10313. doi:10.1109/JIOT.2020.3004273

[24] Wu Y, Dai HN, Wang H, Choo KKR. Blockchain-based Privacy Preservation for 5G-Enabled Drone Communications. IEEE Network 2021; 35 (1): 50–56. doi:10.1109/MNET.011.2000166

[25] Aloqaily M, Bouachir O, Boukerche A, Ridhawi IA. Design Guidelines for Blockchain-Assisted 5G-UAV Networks. IEEE Network 2021; 35 (1): 64–71, 2021.

[26] Li H, Lu R, Zhou L, Yang B, Shen X. An Efficient Merkle-Tree based Authentication Scheme for Smart Grid. IEEE Systems Journal 2014; 8 (2): 655–663. doi:10.1109/JSYST.2013.2271537

[27] Sun Z, Liu Y, Wang J, Mei F, Deng W et al. Non-cooperative Game of Throughput and Hash Length for Adaptive Merkle Tree in Mobile Wireless Networks. IEEE Transactions on Vehicular Technology 2019; 68 (5): 4625–4650. doi:10.1109/TVT.2019.2899647

[28] Bruschi F, Rana V, Pagani A, Sciuto D. Tunneling Trust into the Blockchain: A Berkle based Proof System for Structured Documents. IEEE Access 2021; 9: 103758-103771. doi:10.1109/ACCESS.2020.3028498

[29] 3GPP TS 38.321. 5G-NR; Medium Access Control (MAC) Protocol Specification (Version 15.6.0 Release 15); 2019.

[30] 3GPP TS 38.331. 5G; NR; Radio Resource Control (RRC); Protocol Specification (Version 15.3.0 Release 15); 2018.

[31] 3GPP TR 38.901. 5G; Study on Channel Model for Frequencies from 0.5 to 100 GHz (Version 15.0.0 Release 15); 2018.

[32] Diaz VV, Marcano Aviles D. A Path Loss Simulator for the 3GPP 5G Channel Models. In: 2018 IEEE XXV International Conference on Electronics, Electrical Engineering and Computing (INTERCON); 2018. pp. 1–4. doi:10.1109/INTERCON.2018.8526374