A Blockchain-based Framework for Drone-Mounted Base Stations in Tactile Internet Environment

Vikas Hassija[1], Vikas Saxena[1], and Vinay Chamola[2]
[1]Department of Computer Science and Engineering, JIIT, Noida Campus, India
[2]Department of Computer Science and Information Systems, BITS Pilani, Pilani Campus, India

***Abstract*—5G, blockchain, and drones are potentially revolutionizing future technologies. 5G promises to provide a tactile internet environment to the users. Tactile internet is characterized by ultra-low latency, with high reliability, security, and availability. Few attempts have been made in academia and industry to use drones-mounted small cell base stations. Such flying base stations can be used in disaster areas, emergencies, or in rural areas. The major challenge in deploying such flying base stations is data security. Drones being resource-constrained devices cannot be overloaded with heavy security algorithms. Moreover, the decision of user association, drone movement, and bandwidth allocation are major bottlenecks in deploying such networks. In this paper, we propose a blockchain-based security framework for drone-mounted base stations in the tactile internet environment. Furthermore, a game-theoretic model is proposed as a smart contract to decide on the dynamic bandwidth allocation to different users based on bandwidth availability and cost. Numerical results show that the proposed model helps in better user experience in terms of bandwidth allocation in low network areas.**

***Index Terms*—5G, Tactile internet, bandwidth allocation, Blockchain, low latency, security, reliability**

I. Introduction

The exponential increase in the number of mobile devices and consequently computation-intensive mobile applications such as video streaming, face recognition, etc. presents a major challenge for mobile network providers. The 5G network promises a tactile internet environment with features of low latency, security, privacy, and reliability. Various attempts have been made in recent years in the industry as well as research to use drone-mounted small base stations to provide high and flexible network coverage [1]. Drone base stations are considered to be highly efficient for 5G related services [2]. Drones can dynamically move to different locations, at different altitudes and can transmit different power to fulfill the network demands in different areas at different times [3]. Various algorithms can be applied to dynamically and automatically move the drone-mounted base stations in different areas. Such base stations can have multiple use cases, such as disaster management, emergency, rural area development, and supporting high network demands in case of some events or gatherings. Drones can be utilized both as a fully functional base station or as a remote radio head. Few recent works have also proposed the use of drone-mounted base stations for integrated access and backhaul operations. Such drones can simultaneously perform both the above-discussed functions.

Although there are various benefits of using drone-mounted base stations for 5G, it also comes with a number of associated security challenges. Drones are highly resource-constrained devices, and installation of heavy-weight security and authentication algorithms on drones would not always be feasible. Such algorithms might act as an overhead and might end up reducing the overall efficiency and flight time of the drone, thereby making it impractical to use in real-life scenarios. Also, a lot of communication would be required among the drone-mounted base stations and the normal base stations to decide on the strategic positions of drones and user association. Such communication would be further prone to attacks such as eavesdropping or man-in-the-middle attacks. The attackers might attempt to capture such information and might try to use the bandwidth provided by the drone-mounted base stations for some illegal or ulterior motives [4], [5], [6].

To prevent the possibility of such security threats, and to use such frameworks in real-life scenarios, blockchain is a highly promising security solution [7]. Blockchain is being repeatedly discussed and considered in the research and industry for securing

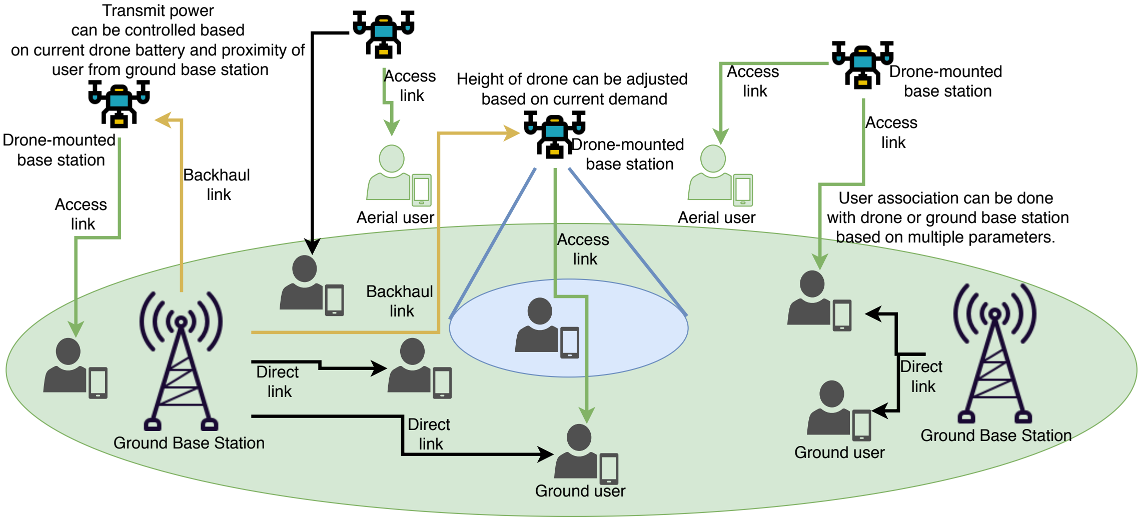


Fig. 1: A scenario depicting the use and benefits of the drone-mounted base stations.

various drone-related applications. Blockchain is a distributed network of permissioned or permissionless nodes that can securely interact with each other directly, without the use of any centralized third party. Various smart contracts can also be deployed on the blockchain network to ensure autonomous decision making and prevent any disputes or disagreements among the nodes in the network. Using blockchain, all the data and information exchanges in wireless communication will be recorded in a tamper-proof open ledger using cryptographic security algorithms [8]. Furthermore, various strategic and game theory-based smart contracts can also be designed to take immediate and important decisions such as a shift in bandwidth allocation, changing the drone speed or height, changing the transmit power level, changing user association, or other major decisions.

The major contributions of this work are summarized as follows:

- A permissioned blockchain-based P2P network of authorized drone-mounted small cell stations and cellular base stations is created.
- A game theory-based smart contract is deployed on the blockchain network to automatically take the strategic decisions related to user association, transmit power level, drone speed, and altitude, etc.
- The smart contract is flexible enough to add any number of parameters or conditions to make proper decisions as and when required.
- Numerical results show that the proposed model helps in better user experience in terms of bandwidth allocation in low network areas.

II. Proposed System Model and Blockchain Preliminaries

Blockchain is a widely used peer-to-peer distributed ledger technology. This technology was initially used only for banking transactions to make them secure, fast, and cheap. Gradually, the technology became widespread and is currently being used in almost all domains, including healthcare, transport, data offloading, education, and wireless communication. In the background, the blockchain technology is empowered with various cryptographic security algorithms such as SHA 256 and ECDSA. In this section, we will discuss the system model of the blockchain-based network of drone-mounted small cell base stations. The basic steps required to set up the blockchain network are also discussed along with the system model.

A. *Digital Identity*

The blockchain network under consideration would be a peer-to-peer network of drone-mounted small cell base stations and ground-based cellular base stations. Considering the controlled and limited number of nodes required in the network, it is proposed to keep it as a private blockchain network. We use the ethereum framework to simulate and verify the working of the proposed blockchain network. Each node entering the network would require a digital identity that will be used for all future communication. Based on the required authentication and permissions, new nodes can any

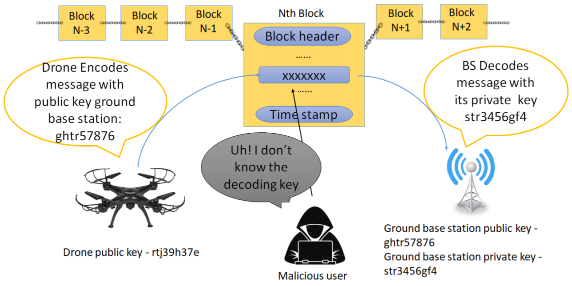

Block N-3
Block N-2
Block N-1
Nth Block
Block header
......
xxxxxxx
......
Time stamp
Block N+1
Block N+2
Drone Encodes message with public key ground base station: ghtr57876
BS Decodes message with its private key str3456gf4
Uh! I don't know the decoding key
Drone public key - rtj39h37e
Malicious user
Ground base station public key - ghtr57876
Ground base station private key - str3456gf4

Fig. 2: Avoiding data thefts using cryptographic features of blockchain.

time enter or leave the network. We use the Elliptic Curve Digital Signature Algorithm (ECDSA) for the process of key generation. Each node has its own set of public and private keys. The public key is used to encrypt the transactions to prevent issues related to confidentiality and integrity. The private key is used to digitally sign the transactions to prevent the issues related to authentication and non-repudiation.

B. *Consensus Algorithm*

The consensus is a technical term used to signify an agreement among the nodes in the peer-to-peer network. In a centralized architecture, the central authority or the central server acts as a trust generator and helps in reaching an agreement among the participating entities [9], [10]. In a distributed network, there is no presence of any central authority, and therefore various consensus algorithms are used to reach to the point of trust in the distributed environment. The basic consensus algorithm used in bitcoin is the proof-of-work (POW) algorithm [11]. In this algorithm, any node that has a specific amount of storage and computation power can act as an authority to verify the upcoming transactions and to add them to the main chain. Such an algorithm cannot work in the private network setting, as any arbitrary node cannot be allowed to perform the task of verification and block addition. The proof-of-authority (POA) consensus algorithm given by the ethereum foundation is used in this work to reach the point of consensus among the participating nodes [12], [13].

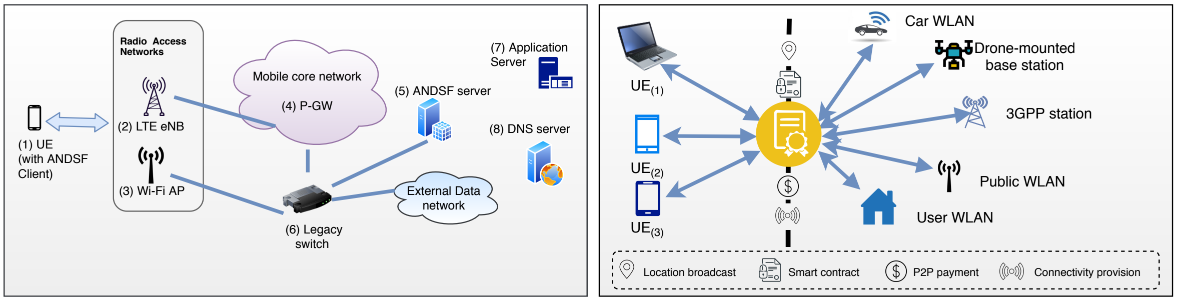
III. Network Model for Drone-Mounted Small Cell Base Stations

The network model under consideration allows the authorized cellular service providers with ground-based cellular base stations and private network providers with drone-mounted small cell base stations to be part of the network. The intuitive idea behind the framework is to use the drone-mounted small cell stations to provide network coverage to the users of different authorized cellular service providers in remote areas, disaster areas, or areas having some temporary and unexpected network demand in case of some public events. The feasibility of establishing a full-fledged ground-based base station is very low in the above-mentioned scenarios. Generally, in such scenarios, the users have to suffer from very low or no network coverage and this further results in loss of customer trust and revenue for the cellular service providers. The big cellular service providers would like to provide the best possible service to their customers at as little cost as possible. In such a scenario, the use of private drone-mounted small cell base stations is a highly promising solution.

Let the set of ground-based cellular base stations be denoted by $\mathcal{X} = \{\mathcal{X}_1, \mathcal{X}_2, ..., \mathcal{X}_m\}$ and the set of private drone-mounted small cell base stations be denoted by $\mathcal{Y} = \{\mathcal{Y}_1, \mathcal{Y}_2, ..., \mathcal{Y}_n\}$. Here m and n are the number of cellular service providers and drone-mounted small cell base stations. Let us consider the situation of a public event being organized in a rural area. The network demand in such a situation will surely be high, and the availability of network resources with the cellular service providers would be low. There can be users associated with different cellular service providers from $\{\mathcal{X}_1, \mathcal{X}_2, ..., \mathcal{X}_m\}$ in the area under consideration. The cellular service providers may opt to hire or rent a private drone-mounted small cell base station from $\{\mathcal{Y}_1, \mathcal{Y}_2, ..., \mathcal{Y}_n\}$ to provide services to its users that are temporarily present in the rural area. In such cases, the different cellular providers may opt to choose the same or different drone-based cell station based on different criteria of cost, required bandwidth, time complexity, pending bandwidth with drone-based cell station and many other factors.

A. *Smart Contract Design*

The smart contract is a very important component of a distributed blockchain-based network. The smart contract makes the network intelligent and self-executable based on the transactions committed by different users. Based on the design of the smart contract, automatic decisions can be taken and executed in the network. The cellular service providers need not worry about the decision of



(a)

(b)

Fig. 3: Comparison of current and blockchain-enabled cellular models.

using the existing drone-based small cell station or deploying a new small cell base station. The service providers just need to set their parameters and constraints in the smart contract. Based on the conditions in the smart contract, the decisions will be taken automatically by the network. The design of the smart contract can be as complicated as required and can cater to as many requirements as needed. The smart contract can also be programmed to automatically control the user association and transmit the power level of a base station based on different conditions. In this paper, we limit the use of smart contracts to automatically take the decision of deploying a new drone-based small cell station in a rural area based on the cost and bandwidth parameter. The cellular service providers need to provide the best possible bandwidth to their associated users and, at the same time, want to minimize their cost. Let $\mathcal{X}_a$ and $\mathcal{X}_v$ be two cellular service providers that want to provide network service to their users in a rural area. Let $\mathcal{Y}_c$ and $\mathcal{Y}_d$ be two drone-based small cell private base stations that can assist $\mathcal{X}_a$ and $\mathcal{X}_v$ to fulfill their requirements at a certain cost for certain data rates. Let there be $\mathcal{M}$ number of users in the area under consideration, and the users associated with $\mathcal{X}_a$ and $\mathcal{X}_v$ be $\mathcal{K}$ and $\mathcal{M} - \mathcal{K}$ respectively.

The drone-based small cell private base stations, i.e., $\mathcal{Y}_c$ and $\mathcal{Y}_d$ have their own limitations in terms of bandwidth they can provide, a number of users they can cater to and the minimum cost they would be charging. These private base stations also need to enhance their revenue by providing service to cellular service providers. To fulfill the constraints of both the service provider and the consumer, an auction-based model is designed in the smart contract to choose the set of best possible service providers (drone-mounted small cell base stations) and consumers (cellular service providers). In the next section, we discuss the auctioning model to choose the service provider.

B. Auctioning model to choose service provider

Initially, both the service providers and the consumers can set their requirements in the network. The requirements here are in terms of the cost charged by service providers and the bandwidth that the service providers commit to provide. The cellular service providers also set their minimum demand in terms of bandwidth requirements and the cost they are willing to pay. The costs for providing network coverage as given by drone-mounted small cell base stations are stored in an array $\alpha = \{\alpha_1, \alpha_2, ..., \alpha_m\}$. Similarly, the bandwidth that the drone-mounted cell stations can provide to the users are stored in an array $\beta = \{\beta_1, \beta_2, ..., \beta_m\}$. The cellular service provider, or in this case, the consumer also mentions its own minimum requirements in terms of cost and bandwidth. These values are stored in variables Θ and Γ, respectively. The consumer can also set certain weights to the cost and time parameters in variables φ and ω, respectively.

To perform a fair auctioning, it is imperative to check that the demand of the consumer is fair and not unrealistic. To do so, we need first to calculate the median of the values of cost and bandwidth provided by drone-mounted base stations as follows.

$$i = (j + 1)/2 \tag{1}$$

Here, j represents the total number of service providers participating in the auction, and i is the index of the median value. Similarly, we can calculate the median of the bandwidth. It is required to bring the values of cost and bandwidth provided by the cellular service provider very close to the median value calculated above. We go on increasing the minimum cost by the cellular service provider by a fixed value of τ until the difference between the median value and Θ becomes near to zero.

$$\Theta = \Theta + \tau \tag{2}$$

until,

$$\alpha_i - \Theta \approx 0 \tag{3}$$

The same is done for time or bandwidth requirement as follows.

$$\Gamma = \Gamma - \mu \tag{4}$$

until,

$$\beta_i - \Gamma \approx 0 \tag{5}$$

Here, μ is the fixed value that reduces the bandwidth requirement given by cellular service provider to bring it close to median of bandwidth values provided by drone-mounted small cell base stations.

IV. Assigning Drone-mounted Base Stations to Service Providers

Now, based on the values of φ and ω, the smart contract can decide as to which drone-mounted base station to be used for which service provider. The values of φ and ω are chosen based on the following constraint.

$$\varphi + \omega = 1 \tag{6}$$

In this scenario, there are two major conditions that influence the decision taken by the smart contract. In this section, we discuss these conditions.

1) ***Weight of bandwidth is greater than the weight of cost***
Based on the values of φ and ω, the objective function can be defined as a maximization or minimization problem. In the first case,

$$\varphi \geq \omega \tag{7}$$

In such a case, the objective function Ψ can be defined as follows.

$$Maximize : \Psi\left(\Psi_c, \Psi_d\right) \tag{8}$$

Here, c and d are the two competing drone-mounted base stations. The value of Ψ can be calculated as follows.

$$\Psi_i = \varphi * \alpha_i + \omega * \beta_i \tag{9}$$

2) ***Weight of bandwidth is less than weight of cost***
In this case, the objective function will become the minimization problem as follows.

$$Minimize : \Psi\left(\Psi_c, \Psi_d\right) \tag{10}$$

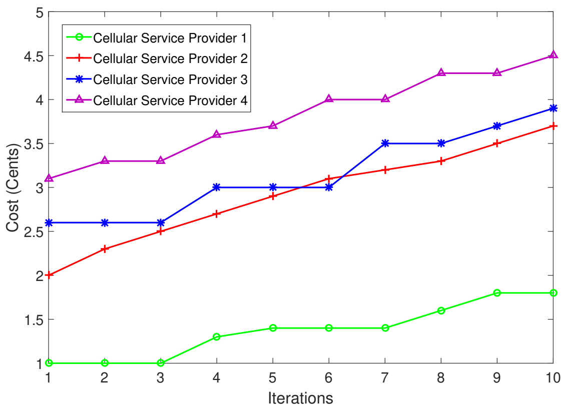


Fig. 4: Change in cost requirement of the cellular service provider over iterations.

Based on the above discussed auctioning process, we try to calculate the changes in cost and bandwidth requirement of 4 cellular service providers. These results are discussed in the next section.

V. Numerical Analysis

To perform the simulation, we consider an auction scenario where a number of cellular service providers perform an auction to choose the best private drone-mounted small cell base station. The demand of the cellular service providers in terms of cost and bandwidth requirements are considered to be in the range of $[100, 250]$ cents for $[10, 20]$ Mb data per second. The drone-mounted small cell base stations have different demands ranging from $[150 - 500]$ cents for $[5 - 15]$ Mb data per second.

Figure. 4 shows the change in the cost proposed by the cellular service providers to the private drone-mounted small cell base stations for providing network coverage. We can see from the graph that initially, the cellular service providers were providing very low cost for the services. Gradually over iterations, due to the proposed model, the cost increases until it reaches closer to the median of the costs given by private network providers. This increases the overall revenue and welfare of private service providers. This feature also makes the dealing between the two parties fair and prevents the big cellular service providers from becoming dominant. A similar change in bandwidth demand by the cellular service provider is shown in Fig. 5. The bandwidth demand goes on decreasing over iterations until it reaches close to the median of the bandwidth provided by the private service providers.

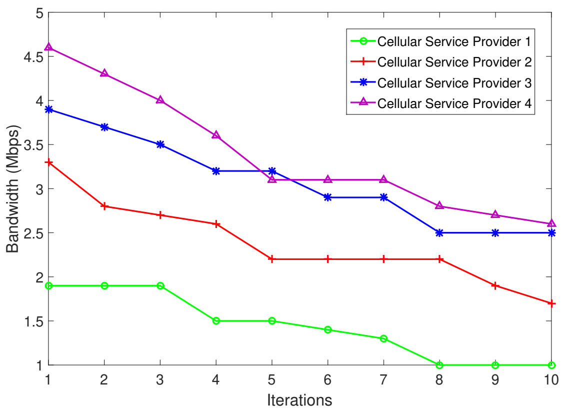


Fig. 5: Change in bandwidth requirement of the cellular service provider over iterations.

VI. Conclusion

In this paper, we have proposed a small blockchain-based framework for allowing secure usage of private drone-mounted small cell base stations to increase the network coverage. Such flying base stations can be used in various use cases such as disaster, public events, rural areas, etc. The use of blockchain provides a security layer for securing the inner communication between resource-constrained unmanned aerial vehicles. A basic smart contract is also deployed to make automatic decisions and pricing strategies over the network. The contract can be made more realistic, and more decisions can be automated in the further part of this work. The numerical results show the enhancement in the welfare of both the parties involved in the network.

VII. Acknowledgement

This work is supported by DST-SERB (Science and Engineering Research Board (SERB)) funding under Project Grant File no. ECR/2018/001479.

References

[1] A. Fouda, A. S. Ibrahim, I. Guvenc, and M. Ghosh, "Uav-based in-band integrated access and backhaul for 5g communications," in *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2018, pp. 1–5.

[2] V. Hassija, V. Saxena, and V. Chamola, "A mobile data offloading framework based on a combination of blockchain and virtual voting," *Software: Practice and Experience*, 2020.

[3] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Mobile unmanned aerial vehicles (uavs) for energy-efficient internet of things communications," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7574–7589, 2017.

[4] M. Gapeyenko, V. Petrov, D. Moltchanov, S. Andreev, N. Himayat, and Y. Koucheryavy, "Flexible and reliable uav-assisted backhaul operation in 5g mmwave cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 11, pp. 2486–2496, 2018.

[5] V. Hassija, V. Chamola, S. Garg, N. G. K. Dara, G. Kaddoum, and D. N. K. Jayakody, "A blockchain-based framework for lightweight data sharing and energy trading in v2g network," *IEEE Transactions on Vehicular Technology*, 2020.

[6] A. Fotouhi, M. Ding, and M. Hassan, "Flying drone base stations for macro hotspots," *IEEE Access*, vol. 6, pp. 19 530–19 539, 2018.

[7] G. Bansal, V. Hassija, V. Chamola, N. kumar, and M. Guizani, "Smart stock exchange market: A secure predictive decentralised model," in *IEEE Globecom, Waikoloa, USA, Dec. 2019*, Dec 2019, pp. 1–6.

[8] A. Fotouhi, M. Ding, and M. Hassan, "Flying drone base stations for macro hotspots," *IEEE Access*, vol. 6, pp. 19 530–19 539, 2018.

[9] T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, "Blockchain applications for industry 4.0 and industrial iot: A review," *IEEE Access*, vol. 7, pp. 176 935–176 951, 2019.

[10] T. K. Vu, M. Bennis, S. Samarakoon, M. Debbah, and M. Latva-Aho, "Joint load balancing and interference mitigation in 5g heterogeneous networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6032–6046, 2017.

[11] V. Hassija, G. Bansal, V. Chamola, V. Saxena, and B. Sikdar, "Blockcom: A blockchain based commerce model for smart communities using auction mechanism," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[12] S. Garg, G. S. Aujla, N. Kumar, and S. Batra, "Tree-based attack–defense model for risk assessment in multi-uav networks," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 35–41, Nov 2019.

[13] T. Alladi, V. Chamola, J. J. Rodrigues, and S. A. Kozlov, "Blockchain in smart grids: A review on different use cases," *Sensors*, vol. 19, no. 22, p. 4862, 2019.