Trusted UAV Network Coverage using Blockchain, Machine Learning and Auction Mechanisms

Khan, A. S., Chen, G., Rahulamathavan, Y., Zheng, G., Assadhan, B. & Lambotharan, S.

DOI 10.1109/ACCESS.2020.3003894
ESSN 2169-3536

Publisher: Institute of Electrical and Electronics Engineers (IEEE)

Received May 19, 2020, accepted June 14, 2020, date of publication June 22, 2020, date of current version July 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3003894

Trusted UAV Network Coverage Using Blockchain, Machine Learning, and Auction Mechanisms

AMJAD SAEED KHAN[1], (Member, IEEE), GAOJIE CHEN[2], (Senior Member, IEEE), YOGACHANDRAN RAHULAMATHAVAN[3], (Member, IEEE), GAN ZHENG[4], (Senior Member, IEEE), BASIL ASSADHAN[5], (Member, IEEE), AND SANGARAPILLAI LAMBOTHARAN[4], (Senior Member, IEEE)

[1]School of Computing, Electronics and Mathematics, Coventry University, Coventry CV1 5FB, U.K.
[2]School of Engineering, University of Leicester, Leicester LE1 7RH, U.K.
[3]Institute for Digital Technologies, Loughborough University London, London E20 3BS, U.K.
[4]Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, Loughborough LE11 3TU, U.K.
[5]Electrical Engineering Department, King Saud University, Riyadh 11451, Saudi Arabia

Corresponding author: Sangarapillai Lambotharan (s.lambotharan@lboro.ac.uk)

This work was supported in part by the Engineering and Physical Sciences Research Council under Grant EP/R006385/1, Grant EP/N007840/1, and Grant EP/R006377/1, in part by the Leverhulme Trust under Grant RPG-2017-129, in part by the U.K.–India Education Research Initiative (UKIERI) under Grant UGC-UKIERI-2016-17-019, and in part by the International Scientific Partnership Program (ISPP) with King Saud University under Grant ISPP 134.

ABSTRACT The UAV is emerging as one of the greatest technology developments for rapid network coverage provisioning at affordable cost. The aim of this paper is to outsource network coverage of a specific area according to a desired quality of service requirement and to enable various entities in the network to have intelligence to make autonomous decisions using blockchain and auction mechanisms. In this regard, by considering a multiple-UAV network where each UAV is associated to its own controlling operator, this paper addresses two major challenges: the selection of the UAV for the desired quality of network coverage and the development of a distributed and autonomous real-time monitoring framework for the enforcement of service level agreement (SLA). For a suitable UAV selection, we employ a reputation-based auction mechanism to model the interaction between the business agent who is interested in outsourcing the network coverage and the UAV operators serving in closeby areas. In addition, theoretical analysis is performed to show that the proposed auction mechanism attains a dominant strategy equilibrium. For the SLA enforcement and trust model, we propose a permissioned blockchain architecture considering Support Vector Machine (SVM) for real-time autonomous and distributed monitoring of UAV service. In particular, smart contract features of the blockchain are invoked for enforcing the SLA terms of payment and penalty, and for quantifying the UAV service reputation. Simulation results confirm the accuracy of theoretical analysis and efficacy of the proposed model.

INDEX TERMS Blockchain, auction, support vector machine, service level agreement, unmanned aerial vehicles, ergodic capacity.

I. INTRODUCTION

Unmanned aerial vehicles (UAVs) have the potential to boost capacity and coverage of existing cellular networks [1]. In particular, UAVs can be deployed as aerial base stations to support wireless communications and internet of things (IoT) in various scenarios such as remote areas [2], emergency situations [3], sports events, and festivals where the installation of terrestrial base stations is too expensive if not impossible [4]. Applications also include military, security, medicine, disaster management, structural inspection, and traffic-monitoring applications [5], [6]. The rapid growth of UAV technology coupled with its flexibility of deployment and connectivity is creating promising new business opportunities and potential for generating significant revenue for cellular operators [7].

Besides the fact that the deployment of UAVs offers numerous advantages, there are still many technical and economic challenges that need to be addressed, while adhering to national security and public safety regulations and guidelines as stipulated in for example [8], [9]. The main challenges are

The associate editor coordinating the review of this manuscript and approving it for publication was Essam A. Rashed.

not limited to the technological aspects of UAV deployment but should include the economical aspect and trustworthiness of UAV operators. For example, there may exist malicious UAV operators that can misbehave and provide inadequate service which could compromise the advantages of adopting UAV-based services. Therefore, ignoring a UAV operator's track record of service provisioning can leave the customer in a vulnerable position. This is known as soft security threat, which is mainly addressed by adopting a trust and reputation model [10]. For example, recently an innovative blockchain based reputation system has been proposed to encourage participants' good behavior to improve market quality for trading in [11].

In addition to achieve reliability, a proper mechanism of operator selection is important for reasonable cost of service. Absence of a proper mechanism for example organizing a competitive selection process, could lead the UAV operators to be untruthful for seeking profits at the expense of internal standards of service, which may cause a customer to pay high service cost. In this regard, economic models and pricing using game theory and auctioning have been extensively analyzed to address resource allocation and various security issues in wireless network [12], [13]. In particular, auction is considered as a well known strategy to ensure fairness, efficiency and truthfulness, specifically, if the participants are rational, intelligent and competing [14]–[17]. Vickrey auction is one of the well-known auction mechanisms due to its unbiased and truthful enforcement nature, where bidding truthfully is the only dominant strategy for the bidders [18], [19]. It is simple to implement yet can provide an effective platform for the distributed and decentralized competitive market. In this context, auction was proposed in [20], [21] as a solution for decentralized users' offloading in a heterogeneous cellular network. Moreover, auction was studied in [22] for spectrum trading between two different cellular service providers as a solution to achieve maximum trading fairness.

In the context of outsourcing services, the trading between the involved parties must be mediated by a service level agreement (SLA) [23]. It provides a clear understanding of responsibilities and requirements which eliminate the risk of disputes. Thus, SLA is considered as an essential part of the trading relationship. However, contracting through SLA opens various challenges to performance measurement. For example, without a proper mechanism of service monitoring, there is a possibility of opportunistic behavior of service in terms of not providing adequate services during the contract duration. In order to address this issue and to ensure accountability of violations against quality of service (QoS) provisioning, regular tracking and periodic monitoring (testing) of service quality is a key characteristic of performance measurement. Monitoring plays a major role in determining whether the SLA has been violated, and thereby facilitates the penalty terms that must be invoked as a consequence. In this context, machine learning, in particular the support vector machine (SVM) [24] is considered as one of the powerful tools for real time monitoring of QoS provisioning [25].

Due to its distributed, transparent, trust-free and highly secure nature, Blockchain technology [26], [27] has attracted tremendous interest in many disciplines including those in finance [28], healthcare [29], transportation [30], energy sector [31], and defense [32]. It is mainly employed for transparency, integrity of the information, processing of claims, auditing of operations, identity management, and to address the threat of malicious entities. In particular, blockchain can enable decentralized operation without a need of trusted central authority. Tempering of information is extremely challenging due to the use of highly cryptographic data structure [33]. More importantly, smart contract features of blockchains deployment of applications over mutually distrusting nodes without the need for an external trusted authority. For example, smart contracts automatically enforce the blockchain systems to only validate the transactions that take place under the condition of agreed upon terms. This makes blockchains act vigorously for resolving issues related to lack of trust, which conventionally require a central trusted party [34]–[37]. Recent years have also witnessed a growing research trend on the application of blockchains in UAV-enabled businesses for solving many critical challenges [38], [39]. For instance, blockchain has been proposed to enable commercial operators to share real time flight plans and establish high quality of audit. Blockchain-enabled systems can assign a unique digital identity to every UAVs and could maintain a record of their airspace activities and related information such as maintenance history and their operators. This allows the regulators to control the operations of UAVs, track missions and identify malicious activities [40]. Furthermore, the blockchain could enable the UAVs to directly interact with each other, share resources and make decisions about their actions through peer-to-peer networking [41], [42]. Fascinatingly, blockchain could introduce new business models in UAV market, where UAVs can directly perform trading activities not only with other UAVs but also with human users in exchange of their services [43]. Blockchain has also found in various UAV assisted applications including data security and resource allocations in wireless networks [44]–[46]. For instance, it has been proposed in [47] and [48] for the security of UAV based data acquisition system in IoT networks. Blockchain has been proposed in [49] for achieving privacy preserving secure spectrum trading in UAV assisted cellular networks. It has also been proposed for conducting secure and distributed auctioning to address the economic challenges of resource allocation in both heterogeneous and co-operative wireless networks [50], [21]. Moreover, blockchain has been applied for the security of UAV assisted health monitoring in [51]. However, none of these works have considered selection criterion of UAV operator and the monitoring process of its service provisioning. By exploiting the intrinsic amalgam of auction based game theory, machine learning and blockchain, we have proposed a novel framework for autonomous selection and operation of UAV for network coverage. The auction framework allows automatic trading for selecting a low-cost UAV while the machine learning and blockchain technology facilitate real-time monitoring of trust and SLA management. Particularly, the proposed framework not only maintains immutable and secure log of UAV's service provisioning but also establishes a fair reputation mechanism of UAV operators in an autonomous and distributed manner. To the best of our knowledge, this is the first study that jointly considers machine learning, blockchain and game theory for autonomous selection of UAV, its real-time service monitoring and SLA management in wireless networks.

The key motivations of this work are twofold: (i) To propose an incentive mechanism that jointly addresses the problem of UAV selection for low cost network outsourcing and the problem of adverse selection of a UAV operator; and (ii) To build a novel blockchain architecture that relies on machine learning technique to monitor and penalize UAVs who violate SLAs. To the best of our knowledge, this work represents the first attempt to present a holistic framework that addresses the problem of UAV-based network outsourcing and its compliance enforcement. The main contributions are summarized as follows:

1) Theoretical expression that evaluates the channel ergodic capacity over a specific UAV coverage area where users (or IoT devices) are randomly distributed according to Binomial Point Process (BPP) is derived. And a resource allocation model is proposed to determine the minimum power required for a UAV to provide a specific QoS over the desired coverage area.
2) Reputation based truthful auction mechanism is proposed to model the interaction between UAV operators and a business agent, where the business agent is interested in outsourcing the network coverage of a specific area, while the UAV operators sell their service based on their cost.
3) A framework is proposed that integrates the benefits of both the blockchain and SVM-based machine learning techniques for SLA enforcement and for the development of service reputation based trust model.
4) Extensive simulations are conducted to verify the accuracy of the analytical expressions for resource allocations, and to demonstrate the efficacy of the reputation based system.

The rest of this paper is organized as follows: Section II describes the system model and problem statement. Section III presents a high level architecture environment and summarizes the considered model. Theoretical expressions for the ergodic channel capacity of the ground users are derived in Section IV and the proposed resource allocation model and auction mechanism are presented. Blockchain preliminaries are presented in Section V and a detailed description of the proposed blockchain framework is presented in Section VI. Results are discussed in Section VII followed by conclusions in Section VIII.

II. SYSTEM MODEL AND PROBLEM STATEMENT

Consider a group of users (or IoT devices) located in a remote geographical area, which is outside the coverage of ground BSs. All the users or IoT devices are randomly distributed in a circular disc D of radius R_{D} according to the BPP as shown in Fig. 1. There is a set of n_{u} UAVs distributed randomly according to a uniform distribution, near to D at an altitude H. One of the UAVs is expected to provide network coverage to users in D. Fig. 1 depicts UAV i that has its own users in area E_i, but located optimally at $O(x_i, y_i, H)$ to serve users in both the areas E_i and D. The optimal location and power needed will be computed based on the QoS requirement as explained in Section IV. Each UAV could belong to a different cellular operator or service provider. We assume that there is always a backhaul connection between a UAV and its corresponding ground BS. Furthermore, each UAV communicates through an orthogonal frequency band, such that there is no interference between UAV transmissions. We consider that there is a third party business agent interested in outsourcing network coverage of D to one of the UAV operators through auctioning. The business agent could be the network operator for users in D or its representative that can be contacted by UAV operators who are willing to provide network service for remuneration. During auctioning, the service requirement and network scenario, such as the location and the radius of coverage area D, the number of users n_{D} and their target QoS in terms of minimum ergodic data rate τ_{D} will be announced by the auctioneer/business agent. Based on this requirement, a number of UAV operators already serving in the neighborhood would compute the cost of providing service to the users/IoT devices in D based on the additional transmission power and submit their bids. The winner UAV operator will be expected to provide network coverage as per a service level agreement that specifies a certain quality of service based on the payment, which the business agent needs to pay if the agreement has been fulfilled.

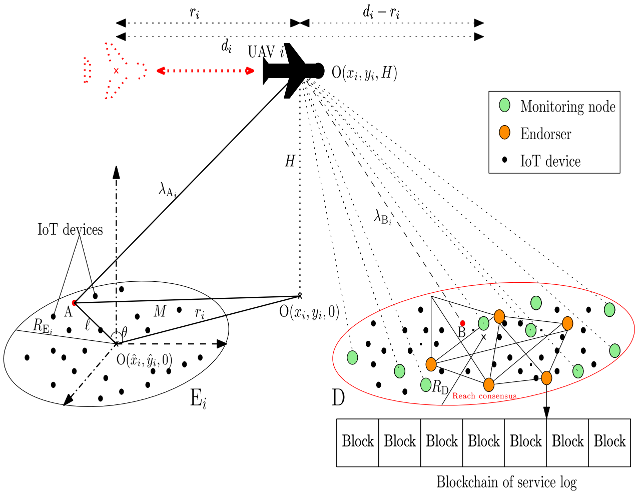


FIGURE 1. A UAV located at $O(x_i, y_i, H)$ intends to serve two pockets of areas - region E_i of its existing service area and region D of new service area in order to earn profit out of its extra resources.

It is important for the UAV to maintain adequate QoS in order to ensure users' satisfaction. Without a proper mechanism for SLA monitoring, various malicious activities could manifest. For example, a selfish UAV operator can cheat and misbehave for increasing his revenue by not providing the agreed level of service in terms of QoS, i.e., not transmitting signals with adequate power to users/IoT devices to achieve the desired data rate τ_D. On the other hand, while anticipating this behavior, a rational business agent will not necessarily trust the UAV operator and will pay less than the agreed amount.

Traditionally, SLA can be monitored through a centralized third-party agent or soliciting users' feedback. However, monitoring through a central agent may not be technically feasible. In addition, since the agent is given a complete authority of decision making, it can also cheat for his own benefits. For example, the agent can be bribed by either service provider or customers for positive reporting and favourable outcomes. On the other hand, monitoring through soliciting users' feedback is also vulnerable to deception and collusion. For example, the malicious soliciting users may collude and provide false information in order to decrease the reputation of the service provider or may intend to pay fewer than negotiated amount. Moreover, in case of SLA violation, there is a lack of mechanism for penalty enforcement. For example, traditionally a responsible party cannot be charged any penalty if it does not acknowledge any violation. This creates a lack of trust between the parties, and would undermine efficient operation of the systems. Thus, in order to address the aforementioned SLA compliance issues, blockchain and machine learning technologies are considered for distributed monitoring mechanism, and guaranteeing trust-free and autonomous SLA monitoring and service reputation system.

III. HIGH LEVEL ARCHITECTURE ENVIRONMENT

The high level architecture of the considered model is depicted in Fig. 2, comprising three main components including: a business agent, UAV service providers, and blockchain service. There are two layers. The first layer has a number of UAVs that are willing to provide network coverage to users in D of Fig. 1. There is a business agent that acts as an auctioneer and selects the winning UAV for service provision. The layer 1 is also responsible for conducting negotiations (about the payments, service duration, QoS requirements, and terms and conditions of penalty) between the business agent and the selected UAV operator. After the negotiation, SLA is signed between the two parties as a contractual agreement. This SLA is then passed to the second layer which contains a blockchain network, where it is deployed as a smart contract. For the case of serving IoT devices, we have considered that there are fully functional nodes among the IoT devices which have adequate computing and storage power. These functional nodes can fully support blockchain protocols and are selected by blockchain administration considering permissioned Blockchain. This blockchain network is responsible for QoS monitoring and SLA compliance enforcement. For example, the blockchain ensures that the QoS at the coverage area is satisfied as per SLA, and the payment is correctly made to the UAV operator. In this regard, the blockchain keeps a record of QoS provisioning. It identifies SLA violations if the QoS requirement at any point of the coverage area is not satisfied, and enforces UAV operator to pay the penalty as a compensation of violations. In addition, based on the statistics of QoS provisioning the blockchain network is also enabled to evaluate the reputation of UAV operator, and to share it with the business agent as a feedback for future agreements. The rest of this paper presents the key functionality of both the layers. In particular, corresponding to layer 1, wireless model of the network is analyzed, and an auction mechanism for suitable interaction between the business agent and the UAV operators is presented in Section IV. Section VI focuses on layer 2 in terms of the development of blockchain for SLA monitoring as well as the establishment of reputation system about the service provider (UAV operators).

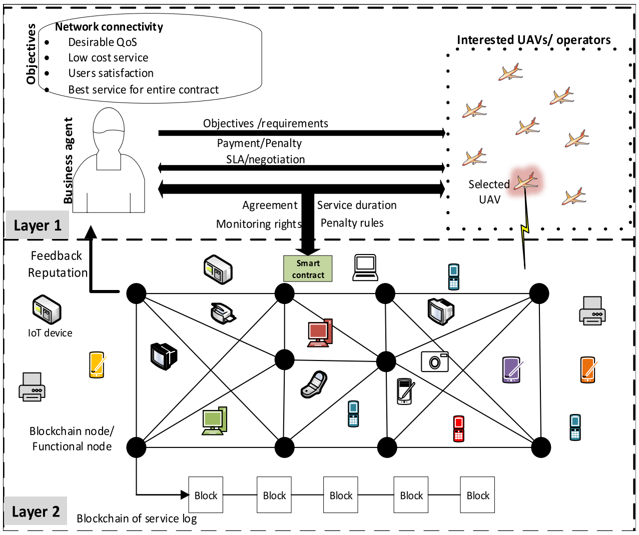


FIGURE 2. High level architecture environment.

IV. WIRELESS MODEL AND AUCTIONING

The cost of a UAV to provide a specific service (data rate over certain duration) depends on the transmission power, bandwidth and other operational costs. Once a business agent announced the service requirement such as QoS and the coverage area, a UAV operator needs to determine the cost of providing the services and submit a bid for the auction. Hence, a UAV needs to include all the operational costs including the bandwidth requirement. We consider all the costs excluding the transmission power as a pre-determined fixed cost to the UAV operators and the transmission power as a time-varying cost that would depend on the locations of the serving UAV and the users/IoT devices. As shown later, due to the truthfulness of the Vickery auction mechanism, the UAV operators will be submitting the real cost incurred to them as their bids. This cost is likely to be identical for all UAV operators except for the transmission power which depends on the location of the serving UAV. Hence, in this section, we characterize the transmission power required for a UAV to satisfy the target data rate τ_{D} for each users/IoT devices. We analytically quantify the ergodic capacity of the link connecting a UAV at an arbitrary location and a ground user placed randomly according to BPP within the coverage area D as shown in Fig. 1. As discussed in Section II, we assume that each UAV i is already serving its own host users located in a disc E_i of radius R_{E_i}. Hence, in order to optimize the transmission power, UAV i will be expected to move from its current location (center of disk E_i) towards center of disk D. Thus, the derived ergodic capacity equations will be used for determining the optimum location ($O(x_i, y_i, H)$ as shown in Fig. 1) for the UAV in terms of minimizing the required transmission power for serving the existing users in E_i and the new users in D.

In order to evaluate the ergodic capacity at E_i corresponding to UAV i, let us first consider a point A over E_i. Assume UAV i is located at (x_i, y_i, H), where x_i and y_i represent the x-axis and y-axis locations from a global referencing point $\bar{\text{O}}(0, 0, H)$ with H being its altitude. Similarly, the center of E_i can be represented as $\text{O}(\hat{x}_i, \hat{y}_i, 0)$, such that $\hat{x}_i$ and $\hat{y}_i$ are the x-axis and y-axis locations of $\text{O}(\hat{x}_i, \hat{y}_i, 0)$ from the origin $(0, 0, 0) \in \mathbb{R}^3$. The air-to-ground link normally considers the path-loss rather than the small scale fading [1], therefore, the path loss model in this paper is assumed as $\lambda_{A_i}^{-\alpha}$, where $\alpha \in (2, 7)$ is the path loss exponent, and λ_{A_i} is the distance between the ith UAV and an arbitrary point A in disk E_i. Let $r_i = \sqrt{(x_i - \hat{x}_i)^2 + (y_i - \hat{y}_i)^2}$ is the Euclidean distance in the two dimensional plane between the UAV and the center of E_i. The distance M between the UAV and the point A can be evaluated as:

$$M = \sqrt{r_i^2 + \ell^2 - 2r_i\ell\cos\theta}, \tag{1}$$

where ℓ is the Euclidean distance between A and $\text{O}(\hat{x}_i, \hat{y}_i, 0)$ and θ is the angle of its elevation. Thus, λ_{A_i} is equal to:

$$\begin{aligned} \lambda_{\text{A}_i} &= \sqrt{M^2 + H^2} \\ &= \sqrt{r_i^2 + \ell^2 - 2r_i\ell\cos\theta + H^2}. \end{aligned} \tag{2}$$

When the ith UAV transmits a signal $x_{u_i}(n)$ at any time instant n with power $P_{\text{E}_i}^{r_i}$, the signal $y_{\text{A}_i}(n)$ received at point A in the disk E_i can be expressed as:

$$y_{\text{A}_i}(n) = \frac{\sqrt{P_{\text{E}_i}^{r_i}}}{\lambda_{\text{A}_i}^{\alpha/2}} x_{u_i}(n) + n_0(n), \tag{3}$$

where $n_0(n)$ is the Additive White Gaussian Noise (AWGN) with zero mean and variance of σ^2. Thus, the instantaneous channel capacity can be expressed as:

$$C_{\text{E}_i}^{r_i} = \log_2 \left(1 + \frac{P_{\text{E}_i}^{r_i}}{\lambda_{\text{A}_i}^{\alpha}/\sigma^2}\right) \tag{4}$$

We assume that the noise variances σ^2 is normalized to one, as otherwise, the noise variance can be absorbed into λ_{A_i} by considering $\lambda_{\text{A}_i} = \lambda_{\text{A}_i}/\sigma^2$. This implies that the ergodic capacity over the cluster E_i can be evaluated by integrating (4), as follows:

$$\bar{C}_{\text{E}_i}^{r_i} = \frac{1}{\pi R_{\text{E}_i}^2} \int_0^{R_{\text{E}_i}} \int_0^{2\pi} \ell \log_2 \left(1 + \frac{P_{\text{E}_i}^{r_i}}{\lambda_{\text{A}_i}^{\alpha}}\right) d\theta d\ell. \tag{5}$$

The above equation can be evaluated for a given set of parameters by using standard numerical integration techniques or software. However, in order to further investigate the performance of the proposed system, we provide closed form solution using an approximation for $\alpha = 2$ as the free space scenario and validate the approximation in the simulation section. The approximation of ergodic capacity is obtained as:

$$\begin{aligned} \bar{C}_{\text{E}_i}^{r_i} \simeq & \frac{1}{R_{\text{E}_i}^2 \ln 2} \\ & \Big\{ \big(r_i^2 + H^2 + R_{\text{E}_i}^2 + P_{\text{E}_i}^{r_i}\big) \ln(r_i^2 + H^2 + R_{\text{E}_i}^2 + P_{\text{E}_i}^{r_i}) \\ & - (r_i^2 + H^2 + P_{\text{E}_i}^{r_i}) \ln(r_i^2 + H^2 + P_{\text{E}_i}^{r_i}) - (r_i^2 + H^2 + R_{\text{E}_i}^2) \\ & \ln(r_i^2 + H^2 + R_{\text{E}_i}^2) + (r_i^2 + H^2) \ln(r_i^2 + H^2) \Big\}. \end{aligned}$$

Similarly, if $P_{\text{D}}^{d_i - r_i}$ denotes the transmission power to serve a user in D, then we can use the same method to calculate the approximated ergodic capacity over D denoted by $\bar{C}_{\text{D}}^{d_i - r_i}$, where, $d_i - r_i$ is the Euclidean distance between the UAV and the center of D and d_i is the distance between the two disks.

Thus, the cost for a UAV to serve all the users in D such that $\bar{C}_{\text{D}}^{d_i - r_i} \geq \tau_{\text{D}}$, while preserving its service at E_i is equal to:

$$Cost_i = n_{\text{E}_i}(P_{\text{E}_i}^{r_i} - P_{\text{E}_i}^{0}) + n_{\text{D}} P_{\text{D}}^{d_i - r_i}, \tag{6}$$

where n_{E_i} and n_{D} specify the number users in disk E_i and D, respectively. $P_{\text{E}_i}^{0}$ is the minimum transmission power required for satisfying the QoS requirement at E_i, when UAV is located at its center, that is $r_i = 0$. The first term specifies the additional cost for serving E_i when the UAV moves towards D, such that $r_i > 0$. The second term is equal to the cost of serving users at D. From (6), it is apparent to understand that when the UAV moves towards D, the value of the first term increases while the second term decreases.

The minimum required transmission power for serving all the users in E_i and D can be calculated through the following resource allocation model.

A. RESOURCE ALLOCATION MODEL

We determine the optimal power allocations $P_{\text{D}}^{d_i - r_i}$ and $P_{\text{E}_i}^{r_i}$ and the optimal value of r_i (i.e. optimal location of UAV over a line connecting the center of disks E_i and D) to obtain the minimum cost of service that satisfies the targeted QoS requirement at D, while preserving the QoS for users in E_i as follows:

$$[r_i^*, P_{\text{E}_i}^{r_i^*}, P_{\text{D}}^{d_i - r_i^*}] = \arg \min_{r_i, P_{\text{E}_i}^{r_i}, P_{\text{D}}^{d_i - r_i}} Cost_i \tag{7}$$

$$\text{subject to} \quad \bar{C}_{\text{D}}^{d_i - r_i} \geq \tau_{\text{D}} \tag{8}$$

$$\bar{C}_{\text{E}_i}^{r_i} \geq \tau_{\text{E}_i}, \tag{9}$$

where the objective function (7) represents the service cost corresponding to the minimum values of $P_{\mathrm{E}_i}^{r_i}$ and $P_{\mathrm{D}}^{d_i-r_i}$ and the optimal value of Euclidean distance r_i. Constraints (8) and (9) ensure that the ergodic capacity of users in D and E_i is not less than the threshold rate τ_{D} and τ_{E_i}, respectively. The constraints (8) and (9) are non convex in terms of their associated transmission power and r_i jointly, therefore, the optimization problem is non convex. However, both the constraints are convex in terms of the power separately.

Thus, in order to solve (7), both the bisection-based line search method and a gradient descent method are employed. In particular, the bisection method is used to find a suitable value of r_i, and for each fixed value of r_i minimum values of $P_{\mathrm{E}_i}^{r_i}$ and $P_{\mathrm{D}}^{d_i-r_i}$ are calculated through the following convex optimization problem:

$$[P_{\mathrm{E}_i}^{r_i}, P_{\mathrm{D}}^{d_i-r_i}] = \arg \min_{P_{\mathrm{E}_i}^{r_i}, P_{\mathrm{D}}^{d_i-r_i}} \{n_{\mathrm{E}_i} P_{\mathrm{E}_i}^{r_i} + n_{\mathrm{D}} P_{\mathrm{D}}^{d_i-r_i}\} \quad (10)$$

$$\text{subject to} \quad \bar{C}_{\mathrm{D}}^{d_i-r_i} \geq \tau_{\mathrm{D}} \quad (11)$$

$$\bar{C}_{\mathrm{E}_i}^{r_i} \geq \tau_{\mathrm{E}_i}. \quad (12)$$

In order to solve (10), Algorithm 1 which is based on the gradient descent technique [52], employed for each $P_{\mathrm{D}}^{d_i-r_i}$ and $P_{\mathrm{E}_i}^{r_i}$ independently to satisfy the related constraint (11) and (12), respectively. It converges to the optimal value with a specific tolerance ϵ to the constraints. Thus, repeating the same procedure for different values of $\hat{r}_i$ obtained through the bisection method leads to the solution of (7).

Algorithm 1 Gradient Descent-Based Iterative Method

```
Notations: $x \in \{P_{\mathrm{D}}^{d_i-r_i}, P_{\mathrm{E}_i}^{r_i}\}$, $C_z \in \{\bar{C}_{\mathrm{D}}^{d_i-r_i}, \bar{C}_{\mathrm{E}_i}^{r_i}\}$, and $\tau_z \in \{\tau_{\mathrm{D}}, \tau_{\mathrm{E}_i}\}$
Initializations: choose $\mu > 0$, $i = 0$, set $Error = 1$, and initialize $x^0$.
Iteration i:
step 1: Evaluate capacity $C_z$ corresponding to $x^i$
$x^{i+1} = x^i + \mu \times Error$
$Error = \tau_z - C_z$
if $|Error| \leq \epsilon$ for a given tolerance $\epsilon \geq 0$ then terminate, otherwise set $i = i + 1$ and go to step 1
```

B. AUCTION FRAMEWORK AND UTILITY FUNCTIONS

A single round sealed bid reverse auction is organized between UAV operators (sellers) offering the network connectivity service and the business agent (buyer) who is interested in outsourcing the network coverage of users in D. We assume that the business agent itself also acts as an auctioneer. The main objective is to select a suitable low cost UAV that can satisfy users' demand of QoS as discussed in Section IV, with whom the agent would contract for a long period of time. At the beginning, before the auction process to start, it is assumed that all UAVs are well informed about the desired QoS requirement. Each UAV operator at first calculates its own cost of service provisioning $\mathcal{C}_i$, such that $\mathcal{C}_i = \tau \times (Pcost_i + Ocost_i)$, where $Pcost_i$ is the cost due to transmission power obtained from (7), $Ocost_i$ is the remaining operational cost including the cost of radio frequency bandwidth, and τ represents the service duration. The UAV operator then submits a sealed bid $b_i = \mathcal{C}_i$ (in truthful bidding) to the auctioneer. After receiving all the sealed bids, the auctioneer will determine a winner and the corresponding payment. Thus, the auction mechanism can be divided into two phases: (i) Winner determination; and (ii) payment allocation, as described below.

1) WINNER DETERMINATION

We adopt a reputation based winner determination model where the selection of a winning UAV is not only based on its bid value but also on its reputation which is developed based on users' past experience, as considered in [53]. According to this model a winner is determined as follows:

$$a^* = \arg \min_i (b_i + HC_i), \quad (13)$$

where HC_i represents an unexpected hidden cost associated with the operator's reputation based on past experiences of its service provisioning. This implies that if the UAV i wins, the business agent may suffer by HC_i amount of cost in addition to the bid price b_i. The cost HC_i can be incurred because of the inadequate service provisioning as compared to the desired QoS. Mathematically, it can be expressed as:

$$HC_i = (1 - \mathcal{R}_i) C_{\mathrm{d}}, \quad (14)$$

where C_{d} is the cost of deviation from the desired service. $\mathcal{R}_i \in (0, 1)$ represents the reputation of the UAV which is based on the past experience of ground users, and provides a measure of its reliability for future contracts. Thus, (14) implies that a UAV with poor reputation may cause high hidden cost to the agent. Note that, we assume that the hidden costs are only known to the business agent. The reputation of UAV can be effectively developed through the feedback of distributed monitoring nodes, which will be discussed in Section VI. We assume that all the participating UAV operators have a history of past performance, and thus have been associated to a specific reputation score.

2) PAYMENT ALLOCATION

For truthfulness, we adopt the payment rule of Vickery auction mechanism [18], that is, the winning UAV is awarded by the price $\mathcal{P}_{win}$ equal to the second best bid. Mathematically, $\mathcal{P}_{win}$ can be expressed as: $\mathcal{P}_{win} = \min(\mathbf{b}_{-i})$, where $\mathbf{b}_{-i}$ is a vector of bids except b_i, such that, each element in $\mathbf{b}_{-i}$ is greater than or equal to b_i. Note that, the auction mechanism ignores all the bids lower than b_i but causing higher hidden cost. After both the winner determination and payment allocation process, the auctioneer notifies the winner and shares the outcome with all the UAV operators for transparency. The utility of the selected UAV operator can be expressed as:

$$U_s = \mathcal{P}_{win} - \mathcal{C}_i.$$

Similarly the utility of the business agent can be calculated as:

$$U_b = \alpha_1 \pi R_D^2 (1 - \eta) - \mathcal{P}_{win},$$

where πR_D^2 specifies the desired coverage area, and α_1 represents its unit valuation for the business agent. In addition, η represents the percentage commission which the monitoring nodes charges the business agent for facilitating the SLA compliance monitoring. The key parameters have been summarized in Table 1 for quick reference.

TABLE 1. Key parameters of the network model.

Notation	Description
n_{u}	Number of UAVs
n_{D}	Number of ground users in disc D
H	Altitude of UAV
$\lambda_{A_i}^{-\alpha}$	Path loss model
α	Path loss exponent
R_{D}	Radius of disc D
R_{E_i}	Radius of disc E_i
τ_{D}	Target data rate for users in D
τ_{E_i}	Target data rate for users in E_i
$C_{\mathrm{E}_i}^{r_i}$	Instantaneous channel capacity at E_i
$\bar{C}_{\mathrm{E}_i}^{r_i}$	Ergodic channel capacity at E_i
τ	Duration of service
$Cost_i$	Cost of i^{th} UAV service at disc D
C_{d}	Cost of UAV deviation from the service
HC_i	Hidden cost of service due to i^{th} UAV
$\mathcal{R}_i$	Reputation of i^{th} UAV operator
$Pcost_i$	Cost due to UAV transmission power
$Ocost_i$	Operational cost due to other resources
$\mathcal{C}_i$	Total cost of service provisioning at D
$\mathcal{P}_{win}$	Winning bid price
U_s	Utility of winning UAV operator
U_b	Utility of business agent

Definition 1: Dominant strategy equilibrium is reached when each player performs its own optimal action independent of the other players' action.

Lemma 1: In the proposed auction mechanism bidding one's own cost ($b_i = \mathcal{C}_i$) is a weekly dominant action. Therefore, the auction attains the dominant strategy equilibrium.

Proof: The proof follows the same line of reasoning as that of the Vickery auction mechanism. For example, given that, in the proposed auction mechanism the winner is always being paid with the second minimum bid, and HC is unknown to the bidders, therefore likewise Vickery mechanism, if a bidder wins by bidding lower than its cost and someone else's bid, then it will be paid less than its true cost. Thus, it is optimal for the bidders to announce their true cost and lose. Secondly, a winner with truthful bidding will always be paid higher than its cost, independently to its bid value. Therefore, it is again optimal to bid truthfully and get benefit, which completes the proof. □

V. BLOCKCHAIN PRELIMINARIES

The blockchain setup and network operations are mainly based on three core components: Asymmetric key cryptography, digital signature, and consensus mechanism, which are described as follows:

A. ASYMMETRIC KEY CRYPTOGRAPHY

Asymmetric key cryptography, also known as public key cryptography, is a cryptographic system that uses a pair of public key and private key [54]. The public key can be widely distributed over all the network, whereas the private key must be kept secret. Both the keys can encrypt a message, such that, the opposite key from the one used to encrypt the message can be used to decrypt it. Blockchain network exploits this feature of public key cryptography for secure operation of the blockchain. For example, in blockchain, private keys are used to digitally sign transactions, which helps to ensure authenticity and integrity of messages.

B. DIGITAL SIGNATURE

Digital signature is one of the fundamental aspects of guaranteeing the security and integrity of data that is recorded in the blockchain network [55]. It is mainly based on asymmetric cryptography and a mathematical algorithm that creates a hash of the input data. For example, in order to create a digital signature, one first creates the hash of the data to be signed, and then the private key is used to encrypt this hash. Given that the value of a hash is always unique to the hashed data, therefore, the integrity of the data can be easily verified using the signer's public key to decrypt the encrypted hash value. A digital signature also makes it difficult for the signer to deny after signing something, assuming that its private key is not compromised. Thus, the digital signature enables the blockchain to ensure non-repudiation of transactions conducted over the network.

C. CONSENSUS MECHANISM

Consensus mechanisms can be defined as the protocols that make sure that all the blockchain nodes (that maintain the blockchain also known as miners) are synchronized with each other and agree on all the legitimate transactions to be added in the blockchain [56]. One of the major objectives of consensus mechanism is to stop users from double spending [57] or from making fake transactions. Most of the blockchains have many features in common and function in a similar way, but they can be uniquely characterized based on their adopted consensus mechanism. There are various types of consensus mechanisms, and some of the well known mechanism include: proof of work, proof of stack [58], proof of burn [59], and proof of authority [60]. On account of permissions, blockchain networks can be categorized into two classes: Permissionless blockchains and permissioned blockchains [61].

D. PERMISSIONLESS BLOCKCHAIN

Permissionless blockchains are known as public blockchains. As the name implies, these networks are completely open

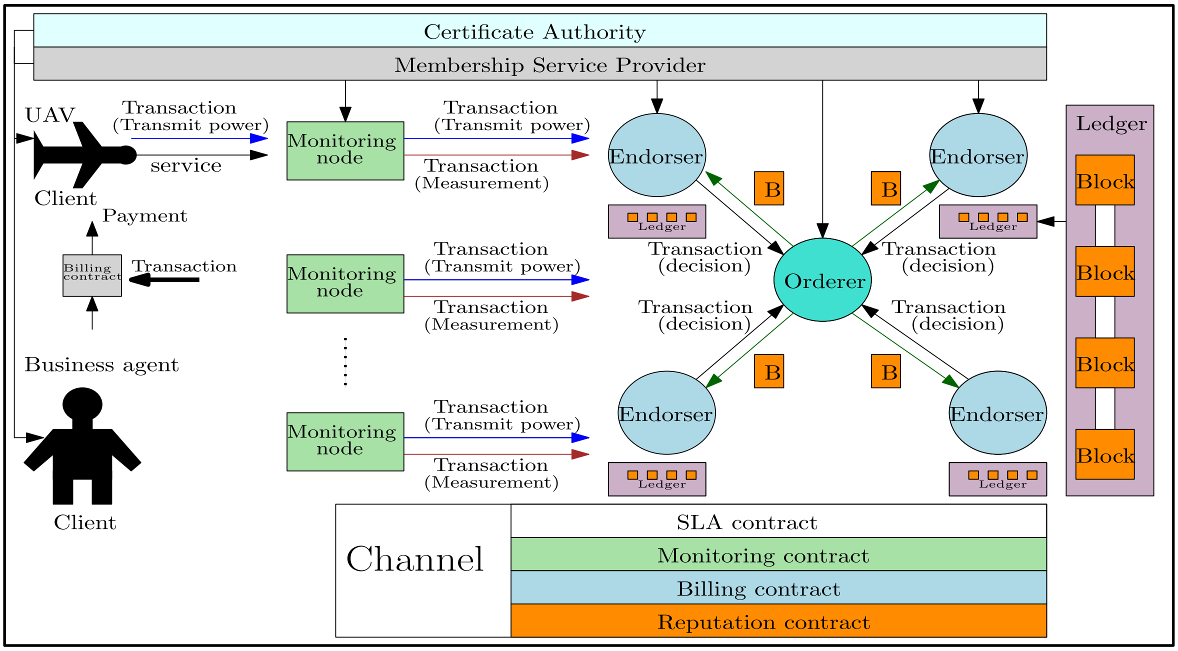


FIGURE 3. Proposed blockchain infrastructure.

such that anyone can join and participate as a blockchain node (known as miner) to serve the network and seek a reward. In addition, a miner can leave and join a network as a node at its will. Bitcoin and Ethereum [27] are the most well known examples of public blockchains. Public blockchains are completely decentralized in nature, where control is distributed over the entire network. More importantly, being honest is in everyone's best interest in public blockchains, and malicious participants would suffer from high cost if they were to cheat. However, there are many drawbacks in adopting the public blockchain for real time applications. For example, they are less efficient in terms of speed, energy and scalability, and require a large number of nodes to ensure security and immutability [62].

E. PERMISSIONED BLOCKCHAIN

Permissioned blockchains can be referred to as private blockchain, e.g., Hyperledger. These blockchains permit only authorized entities to participate in a close network. For example, a consortium of members in a permissioned blockchain decides who can join the network and who can serve the network by writing new blocks into the chain. Private blockchains are usually designed for specific features. They are much faster than public blockchains and can process thousands or even hundreds of thousands of transactions per second. In addition, they are more customizable and have high scalability and energy efficiency benefits. However, since the number of participants in these systems is lower than that of the public blockchains, they are more centralized in nature and semi-reliable [63]. The well known examples of private blockchains include Ripple, Hyperledger [64], and Consortium blockchain. Private blockchains follow different consensus mechanism compared to the public blockchains. Most commonly used consensus mechanisms are: Proof of Authority [60], Proof of elapsed time, Proof of Importance, and Practical Byzantine Fault Tolerance [65].

VI. PROPOSED BLOCKCHAIN FRAMEWORK

A. BLOCKCHAIN BASED INFRASTRUCTURE

We exploit the Hyperledger fabric framework [64] to propose a private blockchain architecture for our application, comprising three different types of nodes including: monitoring nodes, endorsers and orderer, as shown in Fig. 3. Both the UAV operator and the business agent interact as clients to the blockchain. Monitoring nodes are the subset of users within the private blockchain who monitor the data rate offered by the UAV through invoking a monitoring contract. In our work, we use the received signal power at the monitoring terminal for quantifying the data rate. Similarly, the endorsers are a subset of the blockchain network users excluding the monitors, who is responsible for analyzing the measured data and for making a verdict about the QoS. Additionally, endorsers contain digital ledger for blockchain storage. The orderer is a member of the blockchain network, who is however not part of the monitors or endorsers, and is responsible for generating a block of transactions. As customarily, each element is authorized by membership service provider to partake in the network, and has been assigned a unique digital identity through a certificate authority. In addition, each node is given a separate role to play. For instance, once the service contract begins and the UAV submits a transaction for notifying the quality of its service delivery during the contract, all the monitoring nodes measure the quality of network connectivity periodically. Through peer-to-peer communication, these measured values are then forwarded to endorsers as transactions.

These transactions will not be updated in the ledger as they are only for the endorsers for estimating the service quality and endorsing in support or against the UAV claim about the QoS delivery. Each endorser after validating the incoming transactions from the monitoring nodes, employs a machine learning technique to evaluate the level of QoS provisioning, as discussed in Section VI-C. After evaluation of the QoS, each endorser shares its decision to the orderer. Please note that, not all the endorsers will have measurements from all of the monitoring nodes, due to geographically distributed locations of the monitoring nodes as well as the endorsers and their non-homogeneous channel conditions. Hence, each endorser may make its decision based on possibly non-identical measurements. The orderer based on the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism [66] makes a final decision about the quality of received service, and generates a block of transactions (as a service log), which will be broadcasted to all the endorsers to update their ledger. At this stage, the endorsers will verify if the decision made and recorded by the orderer is consistent with its own decision before updating their ledger. Note that, in order to avoid a single point of failure and thus to support a distributed ordering mechanism, the orderer can be replaced with multiple orderers as proposed in [67]. Since, we consider the Fabric platform for our proposed work, the block size and other necessary parameters in the blockchain are assumed to be set to their default values.

Smart contract contains a set of rules under which the parties are required to interact with each other. In addition, the smart contract facilitates, verifies and enforces the performance of an agreement. Note that, all the blockchain nodes are registered to the same channel and hosting a group of all the relevant smart contracts (chaincode), that can be queried and updated by the blockchain application as shown in Fig. 3. The proposed framework is mainly based on four different smart contracts that are installed in the monitoring nodes, given as:

1) SLA contract: articulates a set of rules agreed by both the UAV operator and the business agent, and concerns about monitoring, obligations, prohibitions, and the duration of service.
2) Monitoring contract: aims for autonomous and periodic monitoring of QoS provisioning.
3) Billing contract: evaluates the payment and the penalty based on QoS provisioning and SLA violations, and bills the business agent to pay as per agreement.
4) Reputation contract: evaluates the service provider's reputation based on SLA violations, which at the end of the service contract will be sent to the business agent for future agreements through auctioning as discussed in section IV.

We assume that both the UAV operator and the business agent are also a part of the Ethereum network containing an Ethereum wallet, therefore instead of introducing a new digital currency for our framework, all the payments will be made in ether. This also enables the network to change the world state of their assets in Ethereum blockchain. Finally, the channel is a private subnet of communication between specific network members that join the channel, for the purpose of conducting private and secure transactions. Note that, a smart contract installed in the peers can only be instantiated by the channel members.

B. SERVICE LEVEL AGREEMENT CONTRACT

Once the business agent subscribes the UAV service with certain terms and conditions offered by the UAV operator, a contract is created between the two parties, which is deployed as a smart contract in the blockchain framework. This smart contract can be invoked on the read-only basis as a reference to contractual terms. However, a change in the contract can only be possible in layer 1 and with the consent of both the trading parties. The SLA contract is mainly based on four components including: participant, the service description, service duration, obligations, payment and penalty. The participant identifies the contractual parties including their names, network address and public keys. The service description specifies the QoS and its observable parameters, such as, coverage area, response time, ergodic capacity or throughput. The service duration is the time interval over which the SLA is assumed to be valid. The service obligations define some constraints that may be imposed on SLA parameters. The payment and penalty element (i.e., last element of SLA) defines the payment rules, currency, and the regulation of penalty in case of any violation. The SLA template for network connectivity service is shown in Table 2.

TABLE 2. SLA template for network connectivity.

SLA components	Description
Participants	Customer-name=xx, customer-id: p_{k_i}, seller-name:xx, p_{k_j}, seller-id: p_{k_j}
Service description	Network connectivity for area: xyz, location: xyz, ergodic capacity=xx, throughput=xx, response time=xx
Duration	Startdate: 2019-04-02 00:00:00.. Enddate: 2019-04-10 00:00:00..
Obligations	Ergodic capacity $\geq$ Threshold
....	......

Payment and penalty	Payment=xxx crypto coins/min,
	Penalty= penalty-rule $\times$ Payment,
	penalty-rule= xyz

C. REAL TIME MONITORING PROTOCOL

This protocol allows real-time periodic monitoring of QoS provisioning at the coverage area. Note that, a QoS violation

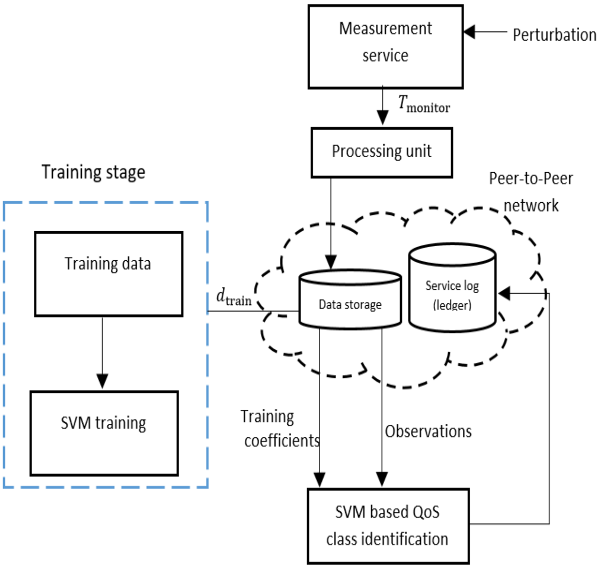


FIGURE 4. Flow diagram of QoS monitoring.

is considered if the ergodic capacity (determined through the estimate of SNR) of the link connecting the UAV and the ground user at any point in the coverage area is less than the threshold rate τ_D, as discussed in Section II. In order to determine if the level of QoS provisioning is satisfied, a one-class support vector machine (SVM) is employed. For this purpose, distributed monitoring nodes are appointed over the coverage area for periodic measurement of instantaneous channel capacity of network connectivity. Note that, we assume that all the monitoring nodes have perfectly synchronized clocks, such that, they perform measurement at the same time over some constant periodic interval. The SVM is then employed over the measured values to detect the breach of satisfactory QoS as an anomaly. Note that we have employed one-class SVM because of its simplicity, low complexity and robust performance [68]. The flow diagram of the monitoring protocol is shown in Fig. 4. The protocol is mainly based on two stages: (i) training stage and (ii) monitoring stage.

1) TRAINING STAGE

The training stage is organized in a convenient time duration well before the initiation of a series of actual contractual services. During this stage, a trusted training UAV is temporarily deployed for network connectivity, such that, it transmits pilot signals with power greater than or equal to the power needed to satisfy the target data rate τ_D, as discussed in Section IV. Meanwhile, corresponding to each pilot transmission, instantaneous ergodic capacity values are computed based on the received signal power measured over all n monitoring nodes. These measurements are then represented by an n dimensional vector $\mathbf{x}_i \in R^n$ for $i = 1, 2, \ldots, m$, where m is the number of training instances. At each training instance, the training UAV will transmit signals with a power level that is drawn according to a uniform random distribution between minimum required power level for attaining desired QoS and a maximum power limit. Thus, for m training instances, training data $\{\mathbf{x}_1, \mathbf{x}_2 \ldots, \mathbf{x}_m\}$ is constructed, such that, each element $\mathbf{x}_i$ is labeled with normal-service class. The training data with its class label is then used as input to a one-class SVM. Traditionally, the SVM first maps the training data into high dimensional feature space and then determines the maximal margin hyperplane that best separates the training data from the origin. This can be obtained by solving the following optimization problem [69]:

$$\min_{w,\epsilon,\rho} \left\{ \frac{||\mathbf{w}||^2}{2} - \rho + \frac{1}{\nu n} \sum_{i=1}^{n} \epsilon_i \right\}$$
$$\text{subject to: } \mathbf{w}^T \phi(x_i) \geq \rho - \epsilon_i, \quad \epsilon_i \geq 0, \tag{15}$$

where $\phi(\mathbf{x}_i)$ is a kernel function which projects the data into a high dimensional feature space [70], ϵ_i are slack variables introduced to relax the constraint in certain cases for some training data sets. In addition, $\rho \geq 0$ characterizes the hyperplane that has maximum distance from the origin in the feature space, and $\nu \in \{0, 1\}$ controls the tradeoff between the number of data points contained by the hyperplane and the maximum distance between the hyperplane and the origin. After solving the optimization problem, the following decision function $f(\mathbf{x})$ is employed to identify the class of input data $\mathbf{x}$ [69]:

$$f(\mathbf{x}) = \text{sign}(\mathbf{w}^T.\phi(\mathbf{x}) - \rho). \tag{16}$$

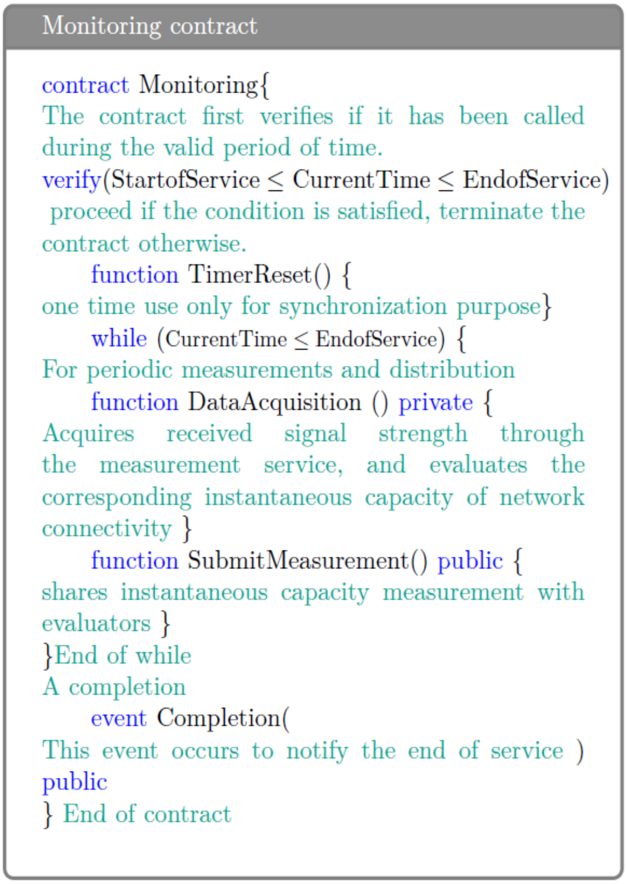
This decision function is used during the monitoring stage to identify the class of real time monitoring data $\mathbf{x}$. For example, $\mathbf{x}$ will be identified as normal-service class if $f(\mathbf{x}) > 0$, otherwise it will be detected as violated-service. We note that the theoretical minimum power for satisfying the target data rate may differ slightly in practice due to reasons such as weather condition etc. Hence to allow a possible margin of error ρ should be set to $\rho - \epsilon_0$ for an appropriate positive small constant ϵ_0 chosen carefully based on the experience. Thus, the resulting outcome of training unit d_{train} composed of vector $\mathbf{w}$ and ρ along with their hash values are distributed to all the endorsers for QoS identification during the actual service time. It can be expressed as:

$$d_{\text{train}} = (\mathbf{w}||\rho||\mathbf{H}(\mathbf{w}||\rho)),$$

where $\mathbf{H}(:)$ is a hash function employing the SHA256 algorithm as discussed, and $||$ denotes concatenation operation.

2) MONITORING STAGE

The monitoring stage of the protocol begins (i.e., during the actual service contract) when the selected UAV starts delivering its service and makes a transaction to notify about its transmission power (P_{UAV}). During this stage each monitoring node triggers the monitoring contract (as presented) for periodic measurement (over the time period T_{monitor}) of the instantaneous channel capacity, and for sharing with endorsers. The contract is composed of different functions. For example, the function **DataAcquisition**() acquires the



```
Monitoring contract

contract Monitoring{
The contract first verifies if it has been called
during the valid period of time.
verify(StartofService ≤ CurrentTime ≤ EndofService)
 proceed if the condition is satisfied, terminate the
contract otherwise.
    function TimerReset() {
one time use only for synchronization purpose}
    while (CurrentTime ≤ EndofService) {
For periodic measurements and distribution
    function DataAcquisition () private {
Acquires received signal strength through
the measurement service, and evaluates the
corresponding instantaneous capacity of network
connectivity }
    function SubmitMeasurement() public {
shares instantaneous capacity measurement with
evaluators }
}End of while
A completion
    event Completion(
This event occurs to notify the end of service )
public
} End of contract
```

value of the received signal strength through measurement service (e.g. using a sensor), and evaluates the instantaneous capacity $\tilde{c}_i$ through processing unit. This measured value is signed by the monitoring node's private key sk_{m_i}, and is then transmitted towards the endorsers as a transaction T_{m_i} using the **SubmitMeasurement**() function and through peer-to-peer communication. It is important to note that, each monitoring node can only submit a single transaction using its private key, represented as:

$$T_{m_i} = Enc_{sk_{m_i}}(P_{\text{UAV}}||\tilde{c}_i||Time||\mathbf{H}(P_{\text{UAV}}||\tilde{c}_i||Time)), \quad (17)$$

where $Enc_{sk_{m_i}}(:)$ represents an asymmetric key encryption algorithm. Each endorser after receiving the transactions first verifies all the transactions using asymmetric key decryption algorithm $Dec_{pk_{m_i}}(:)$ (through public keys pk_{m_i}), and then recovers the measurements $\tilde{\mathbf{x}}_i = \{\tilde{c}_1, \tilde{c}_2, \ldots, \tilde{c}_n\}$ of all the monitoring nodes. Afterward, it employs (16) on $\tilde{\mathbf{x}}_i$ to identify the class of the QoS provisioning using the training values of $\mathbf{w}$ and ρ, and shares the outcome with the orderer as its endorsement in support or against the UAV claim of service provisioning. Note that, likewise (17), the endorsers will sign the transactions to the orderer using their private keys. The orderer after collecting all the endorsements employs the PBFT consensus mechanism to make a final decision on whether the SLA is satisfied or violated. In addition, the orderer stacks together all the incoming transactions and generates a block (as a service log), which also contains the final decision about the SLA provisioning. This block is then timestamped and published (along with its hash value) in the network as a new block to the chain of service log, as shown in Fig. 5, while all the endorsers verify this block and store into their service ledger. Thus, a block generation process takes in total $T_{\text{monitor}} + \xi$ amount of time, where ξ represents some constant amount of time delay occurring during peer-to-peer communication and transactions verification process. It is important to note that, likewise conventional bitcoin mechanism, each block is linked to the previous block through a hash pointer.

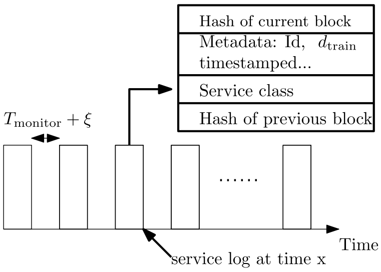
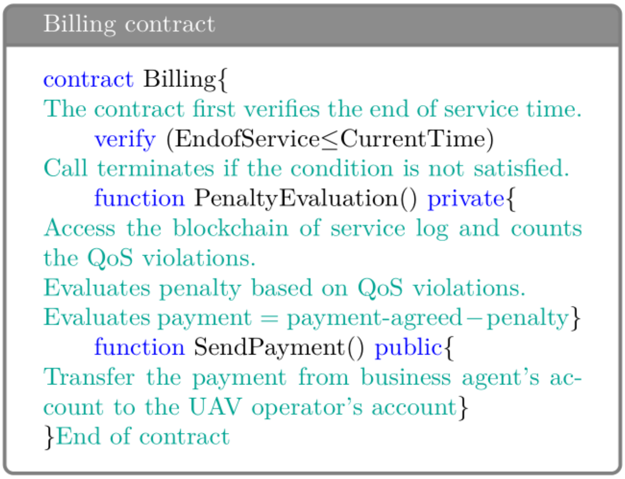


FIGURE 5. Blockchain of service log.

D. PAYMENT

The transfer of payment from the business agent's account to the UAV operator is automatically performed through the Billing contract. This contract is instantiated at the end of service time. The contract first calculates the penalty on QoS violations that must be paid by the UAV operator according to pre-defined terms in SLA, and then evaluates the payment which the business agent is required to pay to the UAV operator. Note that, the contract can access the Ethereum wallets of both the entities. Therefore, it automatically credits the payment from one's account to another. The contract is mainly based on three functions, as shown.



```
Billing contract

contract Billing{
The contract first verifies the end of service time.
    verify (EndofService≤CurrentTime)
Call terminates if the condition is not satisfied.
    function PenaltyEvaluation() private{
Access the blockchain of service log and counts
the QoS violations.
Evaluates penalty based on QoS violations.
Evaluates payment = payment-agreed−penalty}
    function SendPayment() public{
Transfer the payment from business agent's ac-
count to the UAV operator's account}
}End of contract
```

The function **PenaltyEvaluation**() pulls the service log and simply counts the number of violations over the entire service duration, and evaluates the violation penalty using an exponential expressions, as follows:

$$Penalty = \exp(-\frac{N_{\mathrm{I}} - no.violations}{no.violations}) \times \mathcal{P}_{\mathrm{win}},$$

where N_{I} specifies the total number of monitoring intervals throughout the service duration, $no.violations$ represents the number of violations, and $\mathcal{P}_{\mathrm{win}}$ is the payment obtained through auctioning as discussed in Section IV, which is the payment under no violation. After evaluating the penalty of service violations, the contract calls the **SendPayment**() function which directly credits the payment below to the UAV operator through the business agent's wallet using its private key,

$$Payment = \mathcal{P}_{\mathrm{win}} - Penalty.$$

E. REPUTATION

The reputation of service provider is mainly based on the QoS provisioning during the entire service time. It is evaluated using the Reputation contract, as presented. After evaluating the reputation, the contract stores the information in the blockchain and also shares it with the business agent to take into account the trustworthiness of UAV operator for future interactions. Intuitively, the rating of the service provider is actually reflecting its reliability and certainty for service provisioning. In order to evaluate the reputation of the serving UAV operator, the contract invokes **EvaluateReputation**() function. This function first accesses the entire blockchain of service log to take into account all the time instances $n \leq N_{\mathrm{I}}$ at which the QoS violation has occurred, and then assigns normalized weight w_n to the violation instances corresponding to the total number of monitoring intervals N_{I}, such that $\sum_{n=1}^{N_{\mathrm{I}}} w_n = 1$. Based on the QoS provisioning, the service reputation can be evaluated as:

$$\mathcal{R}_i = 1 - \sum_{n=1}^{N_{\mathrm{I}}} \Bigg(w_n \delta_n, \tag{18}$$

where δ_n is an indicator function such that it is equal to 1 at time instance n when QoS violation happens, and 0 otherwise. At the beginning of service time, because of the operational adjustment, the UAV may provide bad service such that QoS violations can be observed. Therefore in order to ignore violation instances at the beginning of service, the normalized coefficients w_n are set such that the violations in the distance past have smaller weights according to an exponential forgetting model [71] given as:

$$w_n = \frac{\exp\{\lambda(n - N_{\mathrm{I}})\}}{\sum_{n=1}^{N_{\mathrm{I}}} \exp\{\lambda(n - N_{\mathrm{I}})\}},$$

where λ is a scaling factor. Thus, the reputation of the service provider for the future contract can be aggregated as:

$$\mathcal{R}_{i+1} = \mathcal{R}_{i-1} + \kappa(\mathcal{R}_i - \mathcal{R}_{i-1}),$$

where $\mathcal{R}_{i-1}$ represents the reputation score during the past experience, and $0 \leq \kappa \leq 1$ is a small constant value. The resultant reputation score along with its hash value is digitally signed and shared with the business agent through the function **ShareReputation**().

Reputation contract

```
contract Reputation{
/*The contract first verifies the end of service time.
    verify (EndofService≤CurrentTime)
/*call terminates if the condition is not satisfied.
    function EvaluateReputation () private{
Reads blockchain and find the violation instances.
Evaluates service provider's reputation based on violation instances.
Stores the reputation score in blockchain.}
    function ShareReputation () private{
Shares reputation score with the business agent}
}
```

VII. NUMERICAL RESULTS

This section provides three kinds of results for the evaluation of the performance. At first, simulation results are presented to verify the tightness of the derived theoretical approximations for the ergodic capacity that has been presented in Section IV. Then the robustness of the considered SVM model is evaluated in terms of the probability of true classification and the probability of false alarm as a function of the number of monitoring nodes. Finally, the performance of the proposed auction mechanism along with the blockchain enabled reputation system is presented. All the results presented in this sections are obtained through a MATLAB simulation platform, while considering the necessary parameters of the blockchain have been set to their default values.

For simulation settings, we consider that all the monitoring nodes and the endorsers are located randomly over the coverage area. The other key parameters are provided in Table 3.

TABLE 3. Parameter values for simulation.

Variable	Value	Variable	Value
α	2	R_{D}	30
n_{D}	10	τ_{D}	8.8
H	50m	n_{E_i}	[5, 40]
σ^2	-130dBm	τ_{E_i}	[1, 12]
N_{I}	100	R_{E_i}	[50, 100]

Fig. 6 exhibits the agreement between simulation and analytical results for $\bar{C}_{\mathrm{E}_i}^{r_i}$ (denoted by $\bar{C}_{\mathrm{E}_i}$) and $\bar{C}_{\mathrm{d}}^{d_i - r_i}$ (denoted by $\bar{C}_{\mathrm{d}}$), which confirms the tightness of our derived theoretical approximations. For a constant transmission power, the figure also illustrates the effect of UAV position (reflected by r_i) over the ergodic capacity values. As expected, with the increase of r_i that is when the UAV moves from disk E_i towards D, the ergodic capacity $\bar{C}_{\mathrm{E}_i}$ reduces while C_{D} increases.

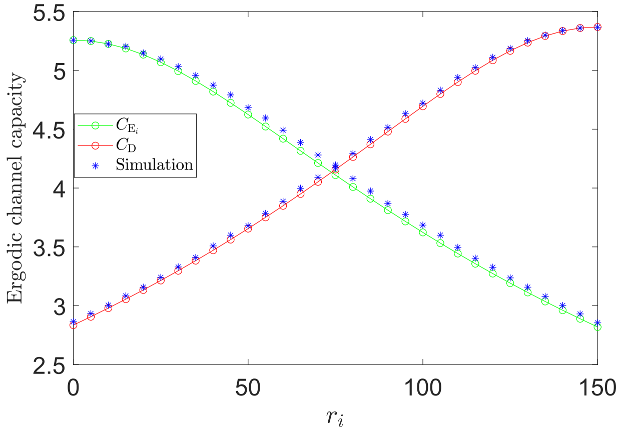


FIGURE 6. Comparison between simulation and theoretical results for ergodic capacity as a function of r_i, when $P_{\mathrm{D}}^{d_i-r_i} = P_{\mathrm{E}_i}^{r_i} = -77.12$dBm.

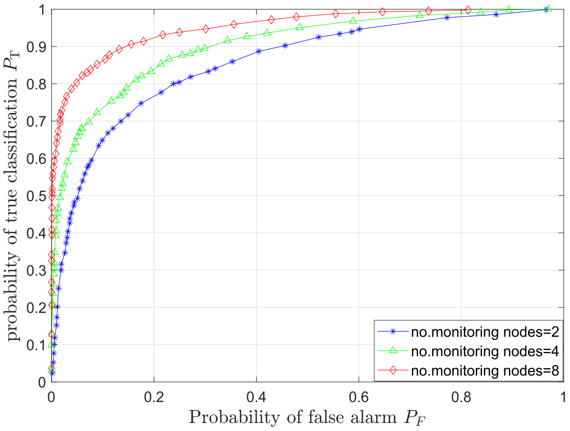


FIGURE 8. Effect of the number of monitoring nodes on the probability of true classification versus the probability of false alarm.

To evaluate performance of the one-class SVM, a Monte Carlo simulation platform was developed. Instantaneous capacity values were calculated using the estimate of SNR over the random locations in disk D, while considering 300 random instances of transmissions with power equal to or greater than the required power level for the QoS satisfaction. Furthermore, during the true service provisioning, all the instances were counted when the QoS requirement over D was satisfied, and averaged over 10^4 realizations to compute the probability of true classification of service. Similarly, the probability of false alarm was calculated during the incorrect service provisioning. Note that, we employed Gaussian Radial Base function as kernel function for SVM, and set 0.05 outlier fraction in the training data.

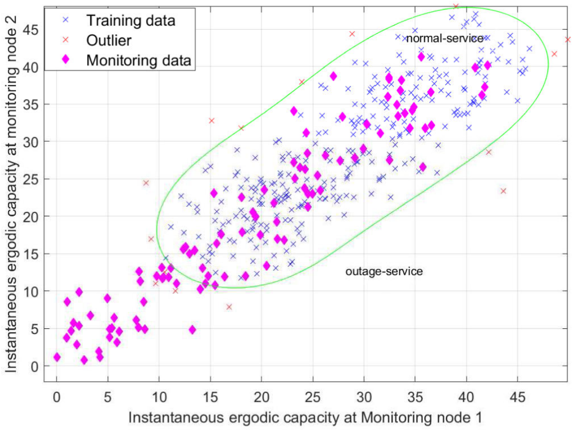


FIGURE 7. Classification of UAV service provisioning using one class SVM, when only two monitoring nodes are considered.

Fig. 7 exhibits the training data description learned by the considered SVM model, obtained through two randomly located monitoring nodes. In addition, it shows the behavior of SVM against the monitoring data that is collected over the monitoring stage of UAV service. For the SVM training, we consider the transmit power range between −50dBm to 30dBm for $\tau_D = 15$. It can be seen that all the training instances belong to the normal service class except 5% of them which are predicted as outage-service class and referred to as outliers (as expected). The robustness of the SVM is exhibited in Fig. 8 in terms of the receiver operating characteristics (ROC), i.e., probability of true classification P_{T} versus the probability of false alarm P_{F}. Clearly, exponential increase of P_{T} can be noticed for a small change in the probability of false alarm P_F. Moreover, the figure demonstrates that this performance is further improved by increasing the number of monitoring nodes.

Fig. 9 studies the performance of the proposed feedback-based reputation (referred as FBR) system in terms of the average cost ($cost_{\mathrm{Average}}$ which includes the payment $\mathcal{P}_{\mathrm{win}}$ and the hidden cost HC) of service versus the probability of certainty (denoted by $P_{\mathrm{certainty}}$) that the selected UAV will serve the users in D according to its reputation score. For simulation purposes, we considered up to 20% deviation (both positive and negative) in UAV service provisioning. Initially, we randomly assign reputation scores to participating UAV operators and run our experiment for 10^3 iterations

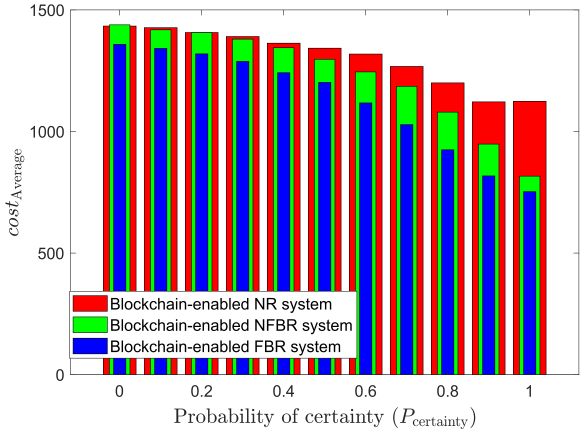


FIGURE 9. Performance comparison between the proposed blockchain-enabled FBR system and NFBR and NR systems in terms of the total service cost as a function of certainty, when the number of monitoring nodes is 10, $\kappa = 0.5$, and $n_{\mathrm{u}} = 50$ (number of UAV operators).

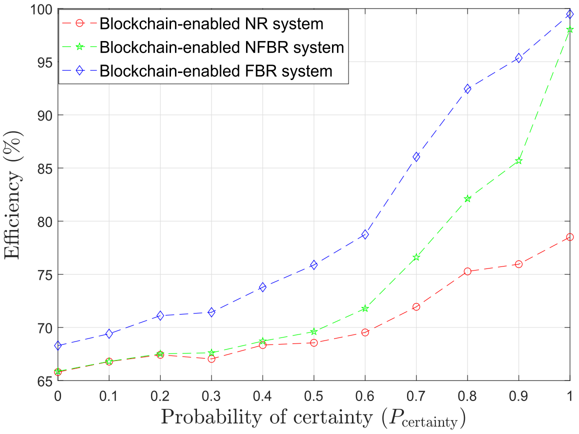


FIGURE 10. Percentage efficiency of blockchain-enabled FBR, NFBR and NR systems as a function of probability of certainty, when the number of monitoring nodes is 10, $\kappa = 0.5$, and $n_{\text{u}} = 50$.

for the development of fair reputation of each UAV according to its service history. The performance is compared with no-feedback-based reputation (referred as NFBR) system (i,e., considering constant reputation score), and with no-reputation (referred as NR) system. Clearly, the proposed FBR system outperforms both the NFBR and NR systems. Moreover, it is important to note that the cost of service reduces significantly with the increase of probability of certainty $P_{\text{certainty}}$. In addition, the performance gap between FBR and NR also increases with $P_{\text{certainty}}$, which gives rise to the intuition for the need for the autonomous and truthful reputation system. On the other hand, Fig. 10 compares the percentage efficiency of the three systems, where the efficiency of system is evaluated as: Efficiency $= \frac{Cost_{\text{Average}}-Penalty}{Cost_{\text{Average}}} \times 100$. The figure demonstrates that based on the value of $P_{\text{certainty}}$, using FBR system the efficiency of NR system and NFBR systems can be improved to $2.5-20\%$ and $2.5-11\%$, respectively, which further strengthen the results of Fig. 9.

VIII. CONCLUSION

This paper proposed an auction mechanism that jointly addresses the economic aspect of UAV-based network coverage and the mitigation of adverse selection of service providers. Using a theoretical analysis, we have shown that truthful bidding is the only weakly dominant strategy in the auction. To aid submission of appropriate bids for the service provision by UAV operators, we have determined the cost in terms of transmission power for serving users that are distributed according to BPP in a geographical area. Simulation results confirmed the tightness of the derived analytical approximations. Moreover, we proposed a framework which integrates the benefits of SVM and smart contract features of blockchain for distributed and periodic monitoring of quality of UAV service and SLA enforcement. In addition, based on the UAV service, the proposed framework quantifies the UAV reputation which is then shared privately through blockchain for future interactions. Through simulations, we have investigated the robustness of the SVM and the potential improvement by increasing the number of monitoring nodes. Furthermore, we demonstrated that a superior performance in terms of average cost and efficiency of service provisioning can always be achieved through the FBR system as compared to both the NR and NFBR systems.

REFERENCES

[1] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2334–2360, 3rd Quart., 2019.

[2] L. Amorosi, L. Chiaraviglio, F. D'Andreagiovanni, and N. Blefari-Melazzi, "Energy-efficient mission planning of UAVs for 5G coverage in rural zones," in *Proc. IEEE Int. Conf. Environ. Eng. (EE)*, Milan, Italy, Mar. 2018, pp. 1–9.

[3] M. Erdelj, M. Król, and E. Natalizio, "Wireless sensor networks and multi-UAV systems for natural disaster management," *Comput. Netw.*, vol. 124, pp. 72–86, Sep. 2017.

[4] S. Hayat, E. Yanmaz, and R. Muzaffar, "Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2624–2661, 4th Quart., 2016.

[5] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018.

[6] K. P. Valavanis and G. J. Vachtsevanos, "UAV applications: Introduction," in *Handbook of Unmanned Aerial Vehicles*. Berlin, Germany: Springer, 2015, pp. 2639–2641.

[7] J. Kuzma, S. O'Sullivan, T. Philippe, J. Koehler, and R. Coronel, "Commercialization strategy in managing online presence in the unmanned aerial vehicle industry," *Int. J. Bus. Strategy*, vol. 17, no. 1, pp. 59–68, 2017.

[8] M. Tillman. (Nov. 17, 2019). *Drone Flying in the UK and US: All the Rules and Regulations Explained*. Accessed: May 18, 2020. [Online]. Available: https://pocket-lint.com/drones/news/141667

[9] D. Hodgkinson and R. Johnston, *Aviation Law and Drones: Unmanned Aircraft and the Future of Aviation*. Evanston, IL, USA: Routledge, 2018.

[10] C. Zhu, H. Nicanfar, V. C. M. Leung, and L. T. Yang, "An authenticated trust and reputation calculation and management system for cloud and sensor networks integration," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 118–131, Jan. 2015.

[11] K. N. Khaqqi, J. J. Sikorski, K. Hadinoto, and M. Kraft, "Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application," *Appl. Energy*, vol. 209, pp. 8–19, Jan. 2018.

[12] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, and Z. Han, "Applications of economic and pricing models for wireless network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2735–2767, 4th Quart., 2017.

[13] N. C. Luong, P. Wang, D. Niyato, Y.-C. Liang, Z. Han, and F. Hou, "Applications of economic and pricing models for resource management in 5G wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3298–3339, 4th Quart., 2019.

[14] X. Qian, M. Huang, L. H. Lee, X. Wang, and S. Tang, "Mechanism design of unknown bidding preference and discrete cost structure in multi-attribute reverse auctions," *IEEE Access*, vol. 7, pp. 68540–68556, 2019.

[15] J. Du, C. Jiang, E. Gelenbe, H. Zhang, Y. Ren, and T. Q. S. Quek, "Double auction mechanism design for video caching in heterogeneous ultra-dense networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 3, pp. 1669–1683, Mar. 2019.

[16] X. Duan, H. Liu, H. Tang, Q. Cai, F. Zhang, and X. Han, "A novel hybrid auction algorithm for multi-UAVs dynamic task assignment," *IEEE Access*, vol. 8, pp. 86207–86222, 2020.

[17] J. Du, C. Jiang, H. Zhang, Y. Ren, and M. Guizani, "Auction design and analysis for SDN-based traffic offloading in hybrid satellite-terrestrial networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 10, pp. 2202–2217, Oct. 2018.

[18] W. Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," *J. Finance*, vol. 16, no. 1, pp. 8–37, Mar. 1961.

[19] L. M. Ausubel and P. Milgrom, "The lovely but lonely Vickrey auction," *Combinat. Auctions*, vol. 17, pp. 22–26, Aug. 2006.

[20] B. Basutli, J. M. Chuma, and S. Lambotharan, "Network capacity enhancement in HetNets using incentivized offloading mechanism," *IEEE Access*, vol. 6, pp. 39307–39323, 2018.

[21] T. Chen, A. S. Khan, G. Zheng, and S. Lambotharan, "Blockchain secured auction-based user offloading in heterogeneous wireless networks," *IEEE Wireless Commun. Lett.*, early access, Mar. 23, 2020, doi: 10.1109/LWC.2020.2982634.

[22] R. Zong, X. Gao, and X. Feng, "Truthful double auction of spectrum trading for femtocell service provision," *Wireless Commun. Mobile Comput.*, vol. 16, no. 17, pp. 2924–2938, Dec. 2016.

[23] S. Mubeen, S. A. Asadollah, A. V. Papadopoulos, M. Ashjaei, H. Pei-Breivold, and M. Behnam, "Management of service level agreements for cloud services in IoT: A systematic mapping study," *IEEE Access*, vol. 6, pp. 30184–30207, 2018.

[24] R. Gandhi, "Support vector machine—Introduction to machine learning algorithms," *Towards Data Sci.*, Jun. 2018. Accessed: Sep. 2019. [Online]. Available: https://towardsdatascience.com/support-vector-machine-introduction-to-machine-learning-algorithms-934a444fca47

[25] Z. Gao, C. Cecati, and S. X. Ding, "A survey of fault diagnosis and fault-tolerant techniques—Part I: Fault diagnosis with model-based and signal-based approaches," *IEEE Trans. Ind. Electron.*, vol. 62, no. 6, pp. 3757–3767, Jun. 2015.

[26] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*. 2016, pp. 225–253.

[27] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014, vol. 3, no. 37. [Online]. Available: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf

[28] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innov.*, vol. 2, no. 1, p. 24, Dec. 2016.

[29] W. Suberg. (2015). *Factom—Latest Partnership Takes on us Healthcare*. [Online]. Available: http://cointelegraph.com/news/factoms-latestpartnership-takes-on-us-healthcare

[30] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[31] H. Lu, K. Huang, M. Azimi, and L. Guo, "Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks," *IEEE Access*, vol. 7, pp. 41426–41444, 2019.

[32] R. Doty, *Blockchain for Embedded Systems*. Scottsdale, AZ, USA: Military Embedded Systems, May 2018. Accessed: Jun. 30, 2019. [Online]. Available: http://mil-embedded.com/guest-blogs/blockchain-for-embedded-systems

[33] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, vol. 107, pp. 841–853, Jun. 2020.

[34] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized BlockChain for IoT," in *Proc. 2nd Int. Conf. Internet–Things Design Implement.*, Apr. 2017, pp. 173–178.

[35] A. Stanciu, "Blockchain based distributed control system for edge computing," in *Proc. 21st Int. Conf. Control Syst. Comput. Sci. (CSCS)*, May 2017, pp. 667–671.

[36] M. Conoscenti, A. Vetro, and J. C. De Martin, "Peer to peer for privacy and decentralization in the Internet of Things," in *Proc. IEEE/ACM 39th Int. Conf. Softw. Eng. Companion (ICSE-C)*, Buenos Aires, Argentina, May 2017, pp. 288–290.

[37] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Bhubaneswar, India, Dec. 2017, pp. 1–6.

[38] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan, "Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3417–3442, 4th Quart., 2019.

[39] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned UAV networks: Challenges, solutions, and comparisons," *Comput. Commun.*, vol. 151, pp. 518–538, Feb. 2020.

[40] S. Choudhary. (Jul. 8, 2019). *What Problems Can Blockchain Solve in the Drone Industry?* Accessed: May 12, 2020. [Online]. Available: https://hackernoon.com/what-problems-can-blockchain-solve-in-the-drone-industry-956b7f748512

[41] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, "Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs," in *Proc. Workshop Res., Edu. Develop. Unmanned Aerial Syst. (RED-UAS)*, Oct. 2017, pp. 84–89.

[42] T. M. Fernández-Caramés, O. Blanco-Novoa, I. Froiz-Míguez, and P. Fraga-Lamas, "Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management," *Sensors*, vol. 19, no. 10, p. 2394, May 2019.

[43] E. C. Ferrer, "The blockchain: A new framework for robotic swarm systems," in *Proc. Future Technol. Conf.* Vancouver, BC, Canada: Springer, 2018, pp. 1037–1058.

[44] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1392–1431, 2nd Quart., 2020.

[45] Y. Dai, D. Xu, S. Maharjan, Z. Chen, Q. He, and Y. Zhang, "Blockchain and deep reinforcement learning empowered intelligent 5G beyond," *IEEE Netw.*, vol. 33, no. 3, pp. 10–17, May 2019.

[46] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Veh. Commun.*, vol. 23, Jun. 2020, Art. no. 100249.

[47] A. Islam and S. Y. Shin, "BUS: A blockchain-enabled data acquisition scheme with the assistance of UAV swarm in Internet of Things," *IEEE Access*, vol. 7, pp. 103231–103249, 2019.

[48] A. Islam and S. Y. Shin, "BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things," *J. Commun. Netw.*, vol. 21, no. 5, pp. 491–502, Oct. 2019.

[49] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 451–466, Jan. 2020.

[50] A. S. Khan, Y. Rahulamathavan, B. Basutli, G. Zheng, B. Assadhan, and S. Lambotharan, "Blockchain-based distributive auction for relay-assisted secure communications," *IEEE Access*, vol. 7, pp. 95555–95568, 2019.

[51] A. Islam and S. Y. Shin, "BHMUS: Blockchain based secure outdoor health monitoring scheme using UAV in smart city," in *Proc. 7th Int. Conf. Inf. Commun. Technol. (ICoICT)*, Kuala Lumpur, Malaysia, Jul. 2019, pp. 1–6.

[52] S. Ruder, "An overview of gradient descent optimization algorithms," 2016, *arXiv:1609.04747*. [Online]. Available: http://arxiv.org/abs/1609.04747

[53] M. Rekik and S. Mellouli, "Reputation-based winner determination problem for combinatorial transportation procurement auctions," *J. Oper. Res. Soc.*, vol. 63, no. 10, pp. 1400–1409, Oct. 2012.

[54] J. W. Bos, J. A. Halderman, N. Heninger, J. Moore, M. Naehrig, and E. Wustrow, "Elliptic curve cryptography in practice," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Christ Church, Barbados: Springer, 2014, pp. 157–175.

[55] S. S. Gupta, *Blockchain*. Hoboken, NJ, USA: Wiley 2017.

[56] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[57] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, p. 2, 2015.

[58] D. Larimer, "Delegated proof-of-stake (DPOS)," Bitshare White Paper, 2017. Accessed: May 2020. [Online]. Available: https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper

[59] S. S. Hazari and Q. H. Mahmoud, "Comparative evaluation of consensus mechanisms in cryptocurrencies," *Internet Technol. Lett.*, vol. 2, no. 3, p. e100, May 2019.

[60] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain," in *Proc. Italian Conf. Cyber Secur.*, Milan, Italy, Jun. 2018, p. 11.

[61] X. Xu, I. Weber, and M. Staples, *Architecture for Blockchain Applications*. Berlin, Germany: Springer, 2019.

[62] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[63] M. Vukolić, "Rethinking permissioned blockchains," in *Proc. ACM Workshop Blockchain, Cryptocurrencies Contracts (BCC)*, Abu Dhabi, United Arab Emirates, 2017, pp. 3–7.

[64] E. Androulaki, A. Barger, V. Bortnikov, and C. Cachin, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, New York, NY, USA, 2018, pp. 1–15.

[65] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, Nov. 2002.

[66] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

[67] J. Sousa, A. Bessani, and M. Vukolic, "A Byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform," in *Proc. 48th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Luxembourg City, Luxembourg, Jun. 2018, pp. 51–58.

[68] M. Fernández-Delgado, E. Cernadas, S. Barro, and D. Amorim, "Do we need hundreds of classifiers to solve real world classification problems?" *J. Mach. Learn. Res.*, vol. 15, no. 1, pp. 3133–3181, 2014.

[69] C.-C. Chang and C.-J. Lin, "LIBSVM: A library for support vector machines," *ACM Trans. Intell. Syst. Technol.*, vol. 2, no. 3, pp. 1–27, 2011.

[70] B. Scholkopf and A. J. Smola, *Learning With Kernels: Support Vector Machines, Regularization, Optimization, and Beyond*. Cambridge, MA, USA: MIT Press, 2001.

[71] K. G. White, "Forgetting functions," *Animal Learn. Behav.*, vol. 29, no. 3, pp. 193–207, Aug. 2001.

AMJAD SAEED KHAN (Member, IEEE) received the B.Eng. degree in computer engineering from the COMSATS Institute of Information Technology, Pakistan, in 2010, and the M.Sc. degree in digital signal processing and intelligent systems and the Ph.D. degree in communication systems from Lancaster University, U.K., in 2013 and 2018, respectively. From 2018 to 2020, he was a Research Associate in signal processing for 5G networks with the Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, U.K. He is currently a Lecturer with the School of Computing, Electronics and Mathematics, Coventry University, U.K. His research interests include 5G networks, network coding, secure wireless communication, digital signal processing, non-orthogonal multiple access, embedded systems design, machine learning, and block chain technology.

GAOJIE CHEN (Senior Member, IEEE) received the B.Eng. and B.Ec. degrees in electrical information engineering and international economics and trade from Northwest University, China, in 2006, and the M.Sc. (Hons.) and Ph.D. degrees in electrical and electronic engineering from Loughborough University, Loughborough, U.K., in 2008 and 2012, respectively. From 2008 to 2009, he was a Software Engineering with DTmobile, Beijing, China. From 2012 to 2013, he was a Research Associate with the School of Electronic, Electrical and Systems Engineering, Loughborough University. He was a Research Fellow with 5GIC, Faculty of Engineering and Physical Sciences, University of Surrey, U.K., from 2014 to 2015. He was also a Research Associate with the Department of Engineering Science, University of Oxford, U.K., from 2015 to 2018. He is currently a Lecturer with the School of Engineering, University of Leicester, U.K. His current research interests include information theory, wireless communications, cooperative communications, cognitive radio, the Internet of Things, secrecy communication, and random geometric networks. He received the Exemplary Reviewer Certificates from the IEEE Wireless Communications Letters, in 2018, and the IEEE Transactions on Communications, in 2019. He serves as an Associate Editor for the IEEE Communications Letters and *IET Electronics Letters*.

YOGACHANDRAN RAHULAMATHAVAN (Member, IEEE) received the B.Sc. degree (Hons.) in electronic and telecommunication engineering from the University of Moratuwa, Sri Lanka, in 2008, and the Ph.D. degree in signal processing from Loughborough University, U.K., in 2011. From April 2008 to September 2008, he was an Engineer with Sri Lanka Telecom, Sri Lanka. From November 2011 to March 2012, he was a Research Assistant with the Advanced Signal Processing Group, School of Electronic, Electrical and Systems Engineering, Loughborough University. He was a Research Fellow with the Information Security Group, School of Engineering and Mathematical Sciences, City University London, U.K. He is currently a Faculty Member with Loughborough University London. His research interests include signal processing, machine learning, block chain technology, and information security and privacy. He received the Scholarship from Loughborough University to pursue the Ph.D. degree.

GAN ZHENG (Senior Member, IEEE) received the B.Eng. and M.Eng. degrees in electronic and information engineering from Tianjin University, Tianjin, China, in 2002 and 2004, respectively, and the Ph.D. degree in electrical and electronic engineering from The University of Hong Kong, in 2008. He is currently a Reader of signal processing for wireless communications with the Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, U.K. His research interests include machine learning for communications, UAV communications, mobile edge caching, full-duplex radio, and wireless power transfer. He was a first recipient of the 2013 IEEE Signal Processing Letters Best Paper Award. He received the 2015 GLOBECOM Best Paper Award and the 2018 IEEE Technical Committee on Green Communications and Computing Best Paper Award. He serves as an Associate Editor for the IEEE Communications Letters.

BASIL ASSADHAN (Member, IEEE) received the M.S. degree in electrical and computer engineering from the University of Wisconsin and the Ph.D. degree in electrical and computer engineering from Carnegie Mellon University. He is currently an Associate Professor with the Electrical Engineering Department, King Saud University. His research interests include cyber security, network security, network traffic analysis, and anomaly detection.

SANGARAPILLAI LAMBOTHARAN (Senior Member, IEEE) received the Ph.D. degree in signal processing from Imperial College London, London, in 1997. He was a Visiting Scientist with the Engineering and Theory Centre, Cornell University, USA, in 1996. He has been a Postdoctoral Research Associate with Imperial College London, since 1999. From 1999 to 2002, he was with Motorola Applied Research Group, U.K. He has investigated various projects, including physical link layer modeling and performance characterization of GPRS, EGPRS, and UTRAN. He was a Lecturer with King's College London and a Senior Lecturer with Cardiff University, from 2002 to 2007. He is currently a Professor of digital communications and the Head of the Signal Processing and Networks Research Group, Wolfson School Mechanical, Electrical and Manufacturing Engineering, Loughborough University, Loughborough, U.K. He has authored more than 200 journals and conference papers in these areas. His current research interests include 5G networks, MIMO, radars, smart grids, machine learning, network security, and block chain technology. He serves as an Associate Editor for the IEEE Transactions on Signal Processing.

• • •