Article:

Zheng, J. orcid.org/0000-0002-4035-8520, Xu, J., Du, H. orcid.org/0000-0002-8220-6525 et al. (4 more authors) (2024) Trust Management of Tiny Federated Learning in Internet of Unmanned Aerial Vehicles. IEEE Internet of Things Journal. ISSN 2327-4662

https://doi.org/10.1109/jiot.2024.3363443

Trust Management of Tiny Federated Learning in Internet of Unmanned Aerial Vehicles

Jie Zheng, Jipeng Xu, Hongyang Du, Dusit Niyato, *Fellow IEEE*, Jiawen Kang, Jiangtian Nie, Zheng Wang

***Abstract*—Lightweight training and distributed tiny data storage in local model will lead to the severe challenge of convergence for tiny federated learning (FL). Achieving fast convergence in tiny FL is crucial for many emerging applications in Internet of Unmanned Aerial Vehicles (IUAVs) networks. Excessive information exchange between UAVs and IoT devices could lead to security risks and data breaches, while insufficient information can slow down the learning process and negatively system performance experience due to significant computational and communication constraints in tiny FL hardware system. This paper proposes a trusting, low latency, and energy-efficient tiny wireless FL framework with blockchain (TBWFL) for IUAV systems. We develop a quantifiable model to determine the trustworthiness of IoT devices in IUAV networks. This model incorporates the time spent in communication, computation, and block production with a decay function in each round of FL at the UAVs. Then it combines the trust information from different UAVs, considering their credibility of trust recommendation. We formulate the TBWFL as an optimization problem that balances trustworthiness, learning speed, and energy consumption for IoT devices with diverse computing and energy capabilities. We decompose the complex optimization problem into three sub-problems for improved local accuracy, fast learning, trust verification, and energy efficiency of IoT devices. Our extensive experiments show that TBWFL offers higher trustworthiness, faster convergence, and lower energy consumption than the existing state-of-the-art FL scheme.**

***Index Terms*—Trust Management, Blockchain, Tiny Wireless Federated Learning, Internet of Unmanned Aerial Vehicle (IUAV).**

I. Introduction

Recently, federated learning (FL) has emerged as a viable means to build intelligent systems to support tasks like traffic monitoring and digital healthcare [1] [2]. With wirelesss FL (WFL), a base stations (BS) or unmanned aerial vehicle (UAV) collects information (e.g., model parameters) from multiple user equipments (UEs). A global model can be trained on the BS or UAV, then the parameter of which is distributed to users to be fine-tuned to create a local model on their local device (using local training data) [3]. The parameters generated by these local models are then transmitted back to a centralized server to update the global parameter [4]. FL mitigates many privacy concerns when performing crowd-sourcing learning as the central server does not need to directly access user data during training. Moreover, compared to traditional distributed tiny machine learning, tiny FL can better cope with the heterogeneity of data and computing power owned by all involved parties [5].

Although promising, there are key challenges in training the tiny WFL model training [6] due to the openness of the wireless link. As it uses a broadcast channel, the security of data during communication cannot be guaranteed, and it is easy to be tampered [7]. Most importantly, this problem occurs even when FL is used for supervised learning: Internet of Things (IoT) users participating in FL are not necessarily trusted, and data owners at the UE may send deceptive parameters to the edge server in the UAV, which breaks the FL process. Specifically, malicious devices intentionally alter a small portion of the parameters of the local model or inject toxic data into the local data set and form a false data injection attack [8] [9]. Furthermore, lightweight training and distributed tiny data storage in tiny FL will results in the slow convergence of global model in internet of unmanned aerial vehicles (IUAVs).

To address the issue that IoT UEs participating in WFL are untrustworthy and therefore easy to cause data poisoning attacks, the blockchain has been shown to enhance the reliability of FL tasks in wireless IoT networks [10] [11]. However, existing works did not verify the performance under distributed tiny data storage conditions that the data are not independent and identically distributed, and also ignored an increase in cost of resources of the overall learning process after joining the blockchain in IUAVs. While [12] proposed a novel WFL algorithm by only assuming strongly convex and smooth loss functions, denoted as the FEDL algorithm, which is suitable for wireless networks and shows higher accuracy and convergence speed than those of the federated average (FedAvg) algorithm [13]. This is due to the fact that the algorithm provides more parameters in the local update stage of the UE upload. However, the FEDL can easily suffer poisoning attacks when transmitted on untrusted channels, and is more destructive, as demonstrated by our experiments results.

This research is supported by the National Natural Science Foundation of China (Grants nos. 62072362 and 62072373), by the National Research Foundation, Singapore, and Infocomm Media Development Authority under its Future Communications Research Development Programme, DSO National Laboratories under the AI Singapore Programme (AISG Award No: AISG2-RP-2020-019 and FCP-ASTAR-TG-2022-003), and MOE Tier 1 (RG87/22).(Corresponding author: Jie Zheng.)

Jie Zheng and Jipeng Xu are with State-Province Joint Engineering and Research Center of Advanced Networking and Intelligent Information Services, School of Information Science and Technology, Northwest University, Xian, 710127, Shaanxi, China.(jzheng@nwu.edu.cn,xujipeng202021317@163.com)

Hongyang Du, Dusit Niyato, and Jiawen Nie are with the School of Computer Science and Engineering, Nanyang Technological University, Singapore, 639798.(hongyang001@e.ntu.edu.sg, dniyato@ntu.edu.sg, jnie001@e.ntu.edu.sg)

Jiawen Kang is with the Automation of School, Guangdong University of Technology, Guangzhou,510006, China.(kjwx886@163.com)

Zheng Wang is with School of Computing, University of Leeds, LS2 9JT United Kingdom.(z.wang5@leeds.ac.uk)

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2024.3363443

Meanwhile, blockchain can provide secure transactions [14], and trust management of blockchain can be referred to as a potent way of assessing the actions of UEs, serving to dampen the influence of malicious devices, in which a trust model can be used to compute the trust value to quantify the trustworthiness of a given UE as the participant [15]. In this paper, a trust management framework for tiny blockchain-enabled wireless federated learning (BWFL) implemented in a semi-central manner for UAVs is proposed with the consideration of local learning time, wireless transmission time and block validation time. The local time is subject to the level of local accuracy and the hyper-learning rate, and the wireless transmission time is subject to the wireless resource allocation, and the block validation time is affected by the frequency of block generation and the size of block. Furthermore, a resource allocation optimization problem for our proposed tiny trust blockchain-enabled wireless federated learning (TBWFL) is formulated to capture the trade-off between the trustworthy learning time and energy costs for UEs with heterogeneous computing and power resources. To our best knowledge, this work is the first proposed trust model to evaluate and quantify the trust characteristics of blockchain-enabled tiny WFL in IUAVs.

The main contributions of this paper are summarized as follows.

- We propose a novel trust management model for a tiny WFL enabled by semi-centralized blockchain considering direct and indirect trust values from the single UAV domain and the multiple UAVs domain. By considering both direct and indirect trust, the model provides more robustness against attacks, better scalability, and dynamic trust update, essential for coverage and timeliness operations in IUAV systems. Direct trust is computed using historical experiences of the evaluated UE by applying a decay function with the parameters of communication time, computation time, and block producing time in every round of tiny WFL. Indirect trust can be derived by consolidating recommendations from UAVs within and across domains. The credibility of trust recommendations from UAVs can be computed with their respective actions of recommendation provision.
- We present a trust, fast, and energy-efficient blockchain tiny WFL framework for IUAV systems. Beyond the assumption of a strongly convex and smooth loss function, our proposed TBWFL not only considers the heterogeneous data of UEs but also characterizes the trade-off between local computing time, global communication time, block producing time, and energy cost of UE to update the trustworthy tiny WFL model for IUAV systems. Our proposed TBWFL scheme implemented in a semi-centralized manner appears to be an effective compromise, offering the advantages of both centralized and distributed systems in the potentially large number of small devices, the limited energy resources of IoT tiny devices, and the highly heterogeneous data in tiny WFL of IUAV systems.
- We design an optimization problem of computing and communication resource allocation for TBWFL to optimize jointly the trust value, block producing time and training time and UE energy consumption. The trust value of UE is computed before their parameters aggregation. The spread of malicious information across the wireless network is significantly suppressed by strategically selecting the appropriate UE with the higher trust value as the participant. The effectiveness of our proposed TBWFL system is extensively evaluated. The experimental results affirm that our TBWFL model is effective in capturing dynamic malicious actions of UE in each round of WFL. Comparative analysis reveals that our proposed TBWFL model outperforms existing trust models. Our approach effectively combats poisoning attacks and recovers convergence even in the face of malicious UE attacks.

II. Related work

Federated Learning in IUAV: FL has drawn great attention due to its advantages of data partitioning, privacy protection, the decentralized machine learning paradigm, communication interaction, and the heterogeneity of data and system [16] [17]. Recently, the integration of FL into UAV networks has raised concerns for many research endeavors, such as FL for multiaccess edge computing assisted by UAVs [18], FL for 6G UAVs [19], FL for UAV-Assisted in multitiered networks [20]. With the evolution of IoT networks, FL has been suggested for an array of IoT applications [2] [21]. Due to the limited computing capacity, transmitting bandwidth, and energy in IoT networks, WFL in resource-constrained mobile IoT networks has received gradually more attention [22]. By jointly optimizing communication efficiency and resource allocation, fast convergence and accurate FL over lossy radio channels and limited communication resources have been investigated in mobile IoT networks [23].

Tiny Federated Learning in IUAV: Recently, tiny federated learning has been attracted more attention gradually. A pruning model for FL was proposed to generate tiny distributed machine learning for resource-constrained IoT devices [24]. The tiny federated learning with bayesian classifiers was proposed by distributing tiny data storage on IoT devices to increase energy efficiency, reduce delay as well as communication cost on IoT devices [25]. An online tiny federated meta-learning was proposed to jointly train a solid initialization for the model of neural network [26]. However, these works do not consider the wireless transmission and fast convergence of global model in tiny FL for IUAV. Meanwhile, in IUAV networks where the UE communicates via wireless links, the radio reliability of UEs has a significant influence on model security for tiny FL in IUAVs [8]. The integration of blockchain to improve the security of WFL has attracted considerable attentions [27]. The blockchain-enabled FL (BFL) framework in digital twin wireless networks was proposed to improve the dependability and security of systems [28]. The blockchain-enabled trustworthy FL architecture was introduced to improve accountability and fairness in the FL system [29].

Trust management for Tiny Federated Learning in IUAV: In addition, tiny WFL in IUAV networks faces the lack of mutual trust among mobile users for the broadcast character of the wireless channel and different radio access points. A reputation mechanism for BFL has been proposed to incentivize UEs to participate in BFL to carry out high-quality model aggregation [30]. An adaptive framework integrating federated learning and blockchain was proposed to estimate the trust values of mobile UE by handling the trust with probability in different networks [31]. In contrast to the majority of studies that utilize existing, standard blockchain-enabled WFL algorithms, our work presents a novel trust management scheme for tiny WFL in IUAVs. It is essential for evaluating the trustworthiness of parameters aggregation in every round and the whole trustworthy for fast FL convergence so as to identify malicious IoT devices in IUAVs systems. We investigate how the communication and computation properties can affect the trustworthiness of blockchain-enabled tiny WFL algorithms in IUAVs. In the future, our work can be extended with two aspects: covert communication [9], secrecy rate [32] and privacy protect [33]; UAV trajectory with the integration of reconfigurable intelligent surface and unmanned aerial vehicle (RIS-UAV) networks [34] [35] for tiny WFL in the IUAV system.

III. System model

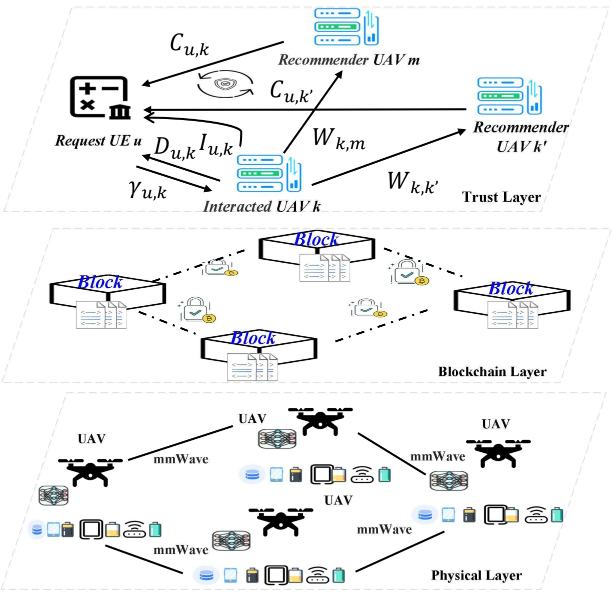


Figure 1: Architecture of Trust IUAV System.

In the context of WFL-enabled IUAV networks, wireless communication between UEs and UAVs is not only resource-intensive, but also lacks consistent reliability. Moreover, IoT devices are constrained by their limited resources. To facilitate trust management and reduce the storage and computation overhead associated with blockchain, a comprehensive TB-WFL IoT network framework can be structured into three tiers: the physical layer, the blockchain layer, and the trust layer, as depicted in Figure 1. Trust verification using blockchain occurs within the blockchain layer. Following this verification, trust management and trust resource allocation can be carried out in the trust layer. Using different types of FL, the framework can contain two domains: intradomain and interdomain. Communication within a single domain (intradomain) is significantly more frequent than communication between different domains (interdomain). The UE can associate with a UAV by considering the reference signal received power (RSRP) in the downlink, and the access of uplink is the same UAV as the downlink. In this paper, a domain can be defined as a cluster of UEs situated within the identical physical space such as UEs connecting to the same UAV in this paper.

Table I: Parameters and descriptions

Parameters	Descriptions
U	Maximum number of UEs participating in federated learning
S_u	Size of data owned by UE u
e_u^n	Parameters of local model for UE u at the n-th round
∇g_u	Gradient of loss function for UE u
γ	Trust parameter used to balance local and global gradient estimates
μ	Accuracy of local level
T_c	Time of local computation for one round
T_r	Time of communication for one round
T_o	Total time of one round for BWFL
T_b	Time of identifying aggregation parameter for the blockchain
N_l	Amount of rounds for the local model
N_g	Amount of rounds for the global model
$E_{u,c}$	Energy costs of UE u for computation
$E_{u,r}$	Energy costs of UE u for communication
E_o	Energy costs of federated learning for one round
p_u	Transmitting power of UE u
f_k^v	Required CPU cycles for UAV k to verify one block
f_u	Computing frequency of UE u
f_k^b	CPU frequency assigned to the blockchain by UAV k
ξ	Required trust threshold of TBWFL
τ	Total time of TBWFL
$R_{u,k}^\tau$	Response trust of UE u to UAV k at the period of τ
$M_{u,k}^p$	Number of positive responses from UAV k to UE u
$M_{u,k}^\tau$	Total interaction number of UE u to UAV k within the period of τ
$L_{u,k}$	Trust level of UE u to UAV k
$Q_{u,k}$	Quality scoring of u for UAV k
$A_{u,k}$	Decay degree of quality scoring
χ_d	Decay constant parameter of direct trust
χ_i	Decay constant parameter of indirect trust
Ψ	Set of recommendation UAVs
$D_{u,k}$	Direct trust value of UAV k to UE u
$I_{u,k}$	Indirect trust value of UAV k to UE u
$C_{k,u}$	Recommendation credibility of UE u from another base station k
$B_{k,u}$	Decay degree of each recommendation trust rating
$W_{k,k'}$	Recommendation trust rating of u for UAV k from k'
$O_{k,u}^\tau$	Number of recommendations from UAV k to UE u within τ

A. Tiny Federated Learning Model

FL problems can be divided into local computing problems and global aggregation problems. The WFL system consists of a total of U UEs and K UAVs with edge servers. UAVs play a crucial role in parameter aggregation, collecting the parameters of each UE's local model in the FL process. As UAVs are interconnected via mmWave, the transmission delay of information between UAVs can be ignored. Tiny FL can train distributed data located at tiny IoT devices such as microcontrollers with ultra-low-power e.g., 1mW [36], while the power for each UAV can be up to 200 W [37]. In this paper, we focus on the energy and delay of tiny UE leaving the costs of communication and computation between UAVs as future work.

Each UE, denoted by u, has a local data set of size S_u, and the total size of the data set is obtained with $S = \sum_{u=1}^{U} S_u$, where $S_u = \{(x_1, y_1), \cdots, (x_{S_u}, y_{S_u})\}$ represents the data set of UE u. The component x_u refers to the data generated or collected by UE, while y_u denotes the corresponding label of

x_u. The goal of FL is to determine the parameters of model e that characterize the result y_u through the loss function $g_u(e)$, which is associated with the data set of UE u expressed as follows:

$$G_u(e) := \frac{1}{S_u} \sum_{u=1}^{S_u} g_u(e). \tag{1}$$

Then, the FL model by minimizing global loss function can be derived as follows:

$$\min_{e \in R^d} G(e) := \sum_{u=1}^{U} \frac{S_u}{S} \times G_u(e). \tag{2}$$

For given $\forall e, e' \in R^d$, the loss function $G_n()$ in tiny FL can be assumed as L-smooth and β-strongly convex with

$$\begin{aligned} G_u(e') + \langle \nabla G_u(e'), e - e' \rangle + \frac{\beta}{2} ||e - e'||^2 \le G_u(e) \\ \le G_u(e') + \langle \nabla G_u(e'), e - e' \rangle + \frac{L}{2} ||e - e'||^2, \end{aligned} \tag{3}$$

where $\langle e, e' \rangle$ is the inner product of e and e', and $|| \cdot ||$ represents l_2 norm.

It is worth noting that the properties of strong convexity and smoothness have broad applications, encompassing areas such as l_2 regularized linear regression models and l_2 regularized logistic regression [17] [38]. Additionally, we define $\rho = \frac{L}{\beta}$ as the condition number of the Hessian matrix for $G_u(\cdot)$.

B. Blockchain Model

To mitigate the risk of parameter poisoning attacks during the wireless communication process of FL by malicious IoT devices, we consider the UAV equipped with blockchain technology to identify the safety and trustworthiness of aggregation parameters. The Ethereum blockchain, operating through smart contracts, is used to verify the parameters through the Solidity programming language. UAVs connected through mmWave maintain the distributed ledger to verify transactions, thereby ensuring the system security, which can be referred to a semi-distributed implementation.

The aggregation of local model parameters will activate smart contracts, which are recorded and transmitted to other UAVs to verify via the blockchain. These smart contracts are treated as transactions and packaged into blocks. The blockchain conducts a consensus process to validate transactions within these blocks. The time cost associated with block verification is attributable to the activation of the smart contract following the parameters upload by UEs. The smart contract manifests as a transaction within the blockchain. These transactions are collected by block producers to be assembled into the block. The block is produced to verify the consensus in Ethereum. Thus, the time cost of blockchain operations is computed by

$$T_b = \max_k \frac{l_b f_k^v}{f_k^b}, \tag{4}$$

where f_k^v denotes the CPU cycles required at the UAV k to verify a block, l_b represents the size of block, and f_k^b is the CPU frequency assigned to the blockchain by UAV k.

C. Trust Calculation Management Model of IUAV

In the process of WFL, a device is deemed untrustworthy if it fails to provide the correct data or delivers malicious data. The trust value attributed to an UE by an UAV is predicted based on the historical behavior exhibited in their past interactions. Here, our evaluation of an objective entity can be computed with direct and indirect approaches, as shown in the trust layer of Figure 1.

1) Direct trust model: For devices that are directly connected to the UAV, we can compute direct trust to evaluate the trustworthiness of UE. On one hand, the ability of a UE to provide timely uploads of model parameters is critical to enable fast convergence of FL. On the other hand, the quality of the model parameters uploaded by UE is also particularly significance to the FL process. The longer the time interval between UE and UAV, the less accurately it reflects the ongoing or prospective parameters updating of UE, thereby necessitating a discounting of its trustworthiness. Therefore, we first examine the time scale of trust parameters and define the period τ of effective trust parameters, in order to decrease the data storage overhead and the workload of trust calculation. The participation of UE in FL in terms of its timeliness and trustworthiness is obtained from response and rating of trust. Furthermore, we introduce the decay function to update the trust rating for more time-efficient trust values.

We define response trust as the probability that UE u can participate and provide the correct model parameters to UAV k in a timely manner. Assuming that the user is connected with only one UAV during one round in the FL process, so the response trust of UE u connected with UAV k in the n-th global round can be denoted as $R_{u,k}^n$, or simply as R_u^n, which is calculated as follows:

$$R_u^n = \frac{M_u^p}{M_u^\tau}, \tag{5}$$

where M_u^p is the number of responses from UAV k for user u and M_u^τ is the total number of interactions between the UAV k and UE u in the period of τ. The response of trust in the period τ are valid, and τ is the total time of TBWFL, that is, $\tau = N_g * T_g$, where N_g is total number of global rounds and T_g is the cumulative time of communication, computing and blockchain within each TBWFL round.

The quality of trust ratings of model parameters updated by the devices involved in each round is crucial for the whole FL process. We set a trustworthiness score to indicate the level of trust for UE u with respect to the UAV. That is, the ability of UE u to provide reliable data in accordance with the requirements of UAVs, as measured by the quality of the parameters uploaded by UE u in their past interactions. We use L_u^n to denote the trust level of UE u to UAV in the n-th global round, which can be calculated as follows:

$$L_u^n = \frac{\sum\limits_{n'=1}^{n-1} \left(Q_u^{n'} \times A_u^{n'} \right)}{\sum\limits_{n'=1}^{n-1} A_u^{n'}}, \tag{6}$$

where $Q_u^{n'}$ is the trust rating value of UE u for the model parameters provided by UAVs at the n'-th round, and $A_u^{n'}$ is the degree of attenuation of the trust rating.

The trust rating value should have a reasonable period and the trust rating obtained from a previous interaction is subject to time-based discounting. The validity of trust is for a period set by τ, and the trust rating follows a decay function within the period τ. If it is beyond this period, the trust rating value will be disregarded. We can select the decay function with the principle of cooling by Newton [39]. The level of decay, $A_u^{n'}$, for the rating $S_u^{n'}$ that occurs at time n', with $n' \in [1, n-1]$ is modeled as follows:

$$A_u^{n'} = \exp\left(-\frac{\chi_d}{M_u^p} \times (n - n')T_g\right), \tag{7}$$

where χ_d denotes a fixed parameter for direct trust referred to the certain FL application, and M_u^p represents the quantity of positive responses received from UAVs, and $n - n'$ is the different of rounds to identify the time of decay function.

According to the above equation, the decay function of trust rating is influenced by three aspects M_u^p, T_g, and $n - n'$. As the number of positive interactions from UE u to UAV k increases, the A_u will augment closing to 1, which means that the trust rating of UE u decays at a lower rate. As the number of aggregation rounds from UE to UAV increases, the trust rating is outdated leading to a greater degree of decay.

Both the timely positive response rate and the quality rating of trust represent an inherent impression of UAV for UE u, which can be referred to as direct trust. Therefore, we can obtain the direct trust value UE u, denoted by D_u^n, using the following calculation:

$$D_u^n = R_u^n \times L_u^n, \tag{8}$$

In summary, the confidence level of a UE is positively associated with the positive response proportion and the trust rating value. It represents the reliability of UE verified by UAVs specifically that the UE can provide a trustworthy local model parameters in a timely manner.

2) Indirect trust: When a UE has never interacted with a UAV or the number of interactions is insufficient to determine exactly the direct trust, it becomes indispensable for UE to compute the indirect trust to ensure the belief of the UE. In the following, we detail the modeling of indirect trust, the verification of recommendation credibility, and the selection of recommenders.

Considering the transferability characteristic of UE to UAV and trust relationships across different rounds in FL, the model of indirect trust is formulated by the direct trust value that other UAVs hold in regard to the objective UE. The indirect trust value of the target UE u associated with the UAV k for time n is represented by I_u^n, which is calculated by weighting the trust values of those UAVs connected to the k'-th UAV to the target UE as follows:

$$I_u^n = \frac{\sum\limits_{k' \in \Psi} \left(D_{k,k'}^n \times C_{u,k'}^n\right)}{\sum\limits_{k' \in \Psi} C_{u,k'}^n}, \tag{9}$$

where $D_{k,k'}^n$ denotes the direct trust quality between UAV k' and UAV k at round n, $C_{u,k'}^n$ is the recommendation credibility of UAV k' when recommending UAV k, and Ψ denotes the set of recommendations for UAV k.

We introduce the concept of recommendation trustworthiness referring to the reliability of trust information offered by UAVs. When the UAV k' aims to assess the indirect trust value the UE u at round n', the direct trust assessed before by another UAV k' can be termed a recommendation $D_{u,k'}^n$. Here, UAV k' is directly connected to UAV k, and we express the prior trust rating of UAV k for UE u by $Q_{u,k}^{n'}$ through the previously perceived trust rating. Initially, we measure the difference between $Q_{u,k}^{n'}$ and $D_{u,k'}^n$, denoted by $\mathrm{V}_{k,k'}^{n'}$ as follows:

$$\mathrm{V}_{k,k'}^{n'} = \left|Q_{u,k}^{n'} - D_{u,k'}^{n'}\right|. \tag{10}$$

We further calculate the recommendation trust rating as follows:

$$W_{k,k'}^{n'} = \max\left(1 - \mathrm{V}_{k,k'}^{n'} *2, 0\right). \tag{11}$$

The recommendation rating is in the range of 0 to 1 to indicate the trustworthiness of UAV k for the trust information provided by UAV k' for UE u.

Given that the trust values are dynamic and change with each round, the credibility of the recommendation is calculated by introducing a decay function. This approach allows the trustworthiness of a recommendation to adapt over time, reflecting changes in the behavior of the UE or the conditions of the wireless network. Thus, the credibility of the recommendation is given as follows:

$$C_{u,k'}^n = \frac{\sum\limits_{n'=1}^{n-1} W_{k,k'} \times B_{u,k'}^{n'}}{\sum\limits_{n'=1}^{n-1} B_{u,k'}^{n'}}, \tag{12}$$

where $B_{u,k'}^{n'}$ denotes the decay degree of each recommendation rating $W_{k,k'}^{n'}$

$$B_{u,k'}^{n'} = \exp\left(-\frac{\chi_i}{O_{u,k'}^{\tau}} \times (n - n')\right), \tag{13}$$

where χ_i denotes a fixed factor for indirect trust related to the certain FL application and $O_{u,k'}^{\tau}$ represents the amount of recommendations of UAV k' and UE u during the period τ. The recommendation trust rating is updated before every recommendation is made.

3) Overall Trust Calculation: For all devices, we can calculate their total trust value on the basis of direct trust and indirect trust. Therefore, the whole trust value indicates the trustworthiness of the target UEs that provide the model parameters to UAVs, and it guides the elimination of malicious UEs and the attack of wireless link for UEs from candidate UEs that are not contributing effectively to the convergence of WFL.

Thus, for UE u connected with UAV k, we can obtain its total trust value, denoted by γ_u^n, in the n-th global round through a combination of direct trust and indirect trust.

$$\gamma_u^n = \omega \cdot D_u^n + \eta \cdot I_u^n, \tag{14}$$

where ω and η represent the weight factors to balance direct trust and indirect trust, respectively. These weights are devised dynamically with adaptation as follows:

$$\omega = \frac{log_{a+1}(1+i)}{log_{a+1}(1+i) + log_{b+1}(1+j)}, \tag{15}$$

$$\eta = \frac{log_{b+1}(1+j)}{log_{a+1}(1+i) + log_{b+1}(1+j)}, \tag{16}$$

where the cardinal number $i = \min(M_u^p, a)$ and the cardinal number $j = \min(\Psi, b)$. With the increasing M_u^p, both ω and i also increase. This leads to the direct trust being given more weight when calculating the total trust. Additionally, when a large number of credible UAVs offer their recommendations to the UE, the weight given by the indirect trust becomes greater.

The weight values can be used based on specific use cases or scenarios, for example, $\eta = 0$ denotes that there is no interaction or recommendation for UE u to other UAVs k and the total trust only can be computed by direct trust. Another scenario arises when a new UE enters the TBWFL system or an UE has no prior interactions with UAV, then ω and η are set to 0, and the initial total trust value can be taken as 0.5 in this work. Furthermore, the weight can be modeled for horizontal and vertical federated learning, which is out of this paper and can be investigated jointly in the future.

IV. Trust Blockchain Wireless FL Algorithm

Our proposed TBWFL algorithm is described as Algorithm 1. To address the problem (2), TBWFL utilizes the iterative method that necessitates N_g global rounds to update the global model. The exchanges between UEs and UAVs in each global round are described below.

UEs trust update local models: In the local training stage of UE, the UE u obtains the local model e_u^n in the global round n. The UE gets the information e^{n-1} and $\nabla\bar{G}^{t-1}$ from the UAV to minimize its surrogate function as follows:

$$\min_{e\in R^d} H_u^n(e) = G_u(e) + \left\langle \gamma_u^n \nabla\bar{G}^{n-1} - \nabla G_u\left(e^{n-1}\right), e\right\rangle . \tag{17}$$

Furthermore, we have

$$\nabla H_u^n(e) = \nabla G_u(e) + \gamma_u^n \nabla\bar{G}^{n-1} - \nabla G_u(e^{n-1}), \tag{18}$$

where γ_u^n denotes the trust value of the global gradient estimated for local gradient of UE u in round n. γ_u^n will influence the convergence of tiny WFL from Theorem 2. Compared to the conventional FedAvg [13], TBWFL needs to get more information e_n and $\nabla G_u(e^{n-1})$ from UEs to provide three key advantages of linear, fast and trust convergence for the tiny WFL in IUAV system. Furthermore, our theoretical analysis of the TBWFL model is noteworthy in that it does not rely on the gradient divergence bound. This assumption is often a prerequisite in studies dealing with non-strongly convex problems, as indicated in previous research [38] [40]. This removes one of the constraints often applied to more scenarios.

Algorithm 1 TBWFL

```
Input: $e^0$, $\mu \in [0,1]$,$\gamma > 0$
for $n = 1$ to $N_g$ do
    Computation: UE $u$ can obtain $e^{n-1}$,$\nabla\bar{G}^{n-1}$, $\gamma_u^n$, and the trust resource allocation solutions $\phi$ from UAVs, and figure out (17) at rounds $N_l$ to realize $\mu$-approximation solution $e_u^n$ satisfying (19).
    Communication: UE $u$ transmits $e_u^n$ and $\nabla G_u\left(e_u^n\right)$ to UAV according to the trust resource allocation solutions $\phi$ obtained from UAVs.
    Trust Verification: The blockchains in the UAVs use cross-validation to verify the model parameters of all UEs, computing the trust value of the model parameters updated by each UE in the round. If the trust value of UE falls below the predetermined threshold, the UE is flagged as providing potentially malicious parameters, leading to its exclusion from the current round.
    Trust Resource Allocation: Each UAV performs the wireless resource allocation in the single domain for the tiny UEs with algorithm 2 from the problem (27).
    Consensus: Multiple UAVs maintain a complete copy of the trust information within the blockchain ledger, and it is imperative to keep the ledgers of all UAVs in the consensus state.
    Aggregation and Feedbacks: The UAV verifies the local parameters of the UE from the blockchain, updates the global model and computes the trust value of UE $\gamma_u$, $e^n$, and $\nabla\bar{G}^n$ as in (14), (20) and (21) respectively. Then the UAV sends $\gamma_u$, $e^n$, $\nabla\bar{G}^n$, and the solutions of the trust resource allocation to all UEs.
end for
```

Then, the UE can solve (17) within the local round of N_l to acquire an approximate solution e_u^n, which should satisfy the following condition:

$$\left\|\nabla H_u^n\left(e_u^n\right)\right\| \le \mu \left\|\nabla H_u^n\left(e^{n-1}\right)\right\|, \forall u, \tag{19}$$

where $\mu \in (0,1)$ denotes the accuracy level of local training to balances the number of local and global rounds for the convergence of FL. Subsequently, e^n and $\nabla\bar{G}^n$ are updated according to (17) and (19) and return to the UAVs. The process should be iteratively executed until the global loss function has achieved convergence.

UAVs trust global aggregation model with blockchain: The UE u sends the local model parameters e_u^n and gradient $\nabla G_u\left(e_u^n\right)$ to the UAV, and then the UAV verifies the trust value of these transmitted components with (14) and proceeds to aggregate these reliable components through the following equations:

$$e^n = \sum_{u=1}^{U} \frac{S_u}{S} e_u^n, \tag{20}$$

$$\nabla\bar{G}^n = \sum_{u=1}^{U} \frac{S_u}{S} \nabla G_u\left(e_u^n\right). \tag{21}$$

The UAV broadcasts e^n and $\nabla\bar{G}^n$ to all UEs. Participating

UEs have a critical role in minimizing their surrogate function $H_u^{n+1}(e)$ in the subsequent global round $n+1$. It is worth noting that UAVs do not require access to local data set S_n, $\forall n$, thereby ensuring the preservation of data privacy.

Theorem 1. With L-smooth convex and β-strongly convex $G_n(\cdot)$ and the $H_u^n(e)$ satisfying a linear convergence rate $c(1-\sigma)^n$, the number of local rounds N_l required for UEs to update local models and achieve a μ-approximation condition can be obtained as follows:

$$N_l = \frac{1}{\sigma} \ln \frac{v\rho}{\mu^2}. \tag{22}$$

Proof: Refer to Appendix A.

Theorem 2. For given $G(e^n) - G(e^*) \leq \delta$ for $\forall n \geq N_g$, the number of global rounds N_g for TBWFL can be denoted as

$$\begin{aligned} N_g =& \frac{2\rho\left((1+\mu)^2\gamma^2\rho^2+1\right)}{\gamma\left(2(\mu-1)^2-\mu(\mu+1)(3\gamma+2)\rho^2-\gamma\rho^2(\mu+1)\right)} \\ &\times \log \frac{G\left(e^0\right)-G\left(e^*\right)}{\delta}. \end{aligned} \tag{23}$$

Proof: Refer to Appendix B.

Time cost: Given the robust computational capability of the edge server and the relatively small volume of parameters that require global aggregation in each round, we can neglect the aggregation time. However, the time of blockchain to verify the trust of aggregation parameter can not be neglected due to the heavy computational requirement of blockchain in the UAV. Furthermore, we consider the local computation time of UE in mobile IoT network. Since the downlink rate surpasses the uplink in mobile wireless network, we can neglect the downlink time of the global parameter from UAV to UE and focus on the uplink time of the UE. In our study, we take into account synchronous communication. This approach necessitates that all UEs resolve their local problems (17) prior to entering the parameter transmission phase in the uplink direction. In summary, the total time consumption of our TBWFL consists of three components: local computation time, uplink communication time, and the blockchain time.

The computation time for a local round is denoted by T_c. Therefore, given that there are N_l local rounds within a global round, the overall computation time for a global round can be calculated as $N_l T_c$. And T_r represents the communication time of a global round. Then the total time consumption of a BTWFL global round can be formulated as follows:

$$T_g = N_l T_c + T_r + T_b. \tag{24}$$

Energy Consumption: We use a_u to denote the computational cost required by UE to train one data sample. Assuming that all samples $\{x_u, y_u\}_{u \in S_u}$ are the same size, the computational cost in terms of CPU cycles in the UE to complete a local round calculation can be denoted as $a_u S_u$. With the frequency of CPU f_u and the effective coefficient of the computing chip-set $\frac{\theta_u}{2}$ for UE u, the CPU energy consumption for each round can be expressed as [41]:

$$E_{u,c} = \frac{\theta_u}{2} a_u S_u f_u^2. \tag{25}$$

Thus, the computing time can be obtained in each local round for the UE u $\frac{a_u S_u}{f_u}$.

We can assume that the sizes of vectors e_u and $\nabla G_n(e_n)$ remain constant underpinned by the fact that the dimensions of these vectors are fixed, and the data size of e_u and $\nabla G_n(e_n)$ is described as d_n. The transmitting rate for UE u can be obtained $r_u = B \ln(1 + \frac{h_u p_u}{N_0})$ with Shannon capacity, where B denotes the wireless bandwidth, and N_0 denotes the noise of background, and h_u denotes the average channel gain. Thus, the scale of transmission time for UE u is obtained with $c_u = d_u / r_u$. Then, the energy costs for one round are given by $E_{u,r} = c_u p_u$.

The energy consumption of local computation also relies on the amount of local rounds, so the overall energy costs of a TBWFL global round is obtained by

$$E_o = \sum_{u=1}^{U} (E_{u,r} + N_l E_{u,c}). \tag{26}$$

V. Trust Optimization and Solution

In this section, we investigate the wireless resource optimization for TBWFL over IUAV system. As the number of tiny UEs in the IUAV network continues to grow, the requirements of UEs participating in tiny WFLs are manifested in low latency, low power consumption, high security, and high accuracy. Therefore, how to decrease the delay and energy cost of model training while ensuring the trust accuracy of the model in WFL applications has become an important issue. Considering that minimizing the time and communication cost while guaranteeing high-quality trust tiny WFL is our core problem, which requires finding the balance between model accuracy, model trustworthy and the delay in the tiny WFL processes. Therefore, we formulate the trust resource allocation problems as follows:

$$\mathscr{P}: \min_{\{f,c,\mu,T_r,T_c,T_b\} \in \phi} N_g \left[E_o + \lambda T_g\right] \tag{27}$$

$$s.t. \sum_{u=1}^{U} c_u \leq T_r, \tag{27a}$$

$$\max_u \frac{a_u S_u}{f_u} = T_c, \tag{27b}$$

$$F_u^m \leq f_u \leq F_u, \forall n \in \mathcal{N}, \tag{27c}$$

$$P_u^m \leq p_u \leq P_u, \forall n \in \mathcal{N}, \tag{27d}$$

$$0 \leq \mu \leq 1, \tag{27e}$$

$$F_k^{b,m} \leq f_k^b \leq F_k^b, \tag{27f}$$

$$0 < \gamma_u < 1, \forall u \in \mathcal{U}, \tag{27g}$$

$$\gamma_u \geq \xi, \forall u \in \mathcal{U}. \tag{27g}$$

When the UE reduces its own power consumption, it will definitely increase the time of the local training model, and then it is contradictory to decrease the delay and energy consumption simultaneously. To strike a trade-off between the training delay and the cost of energy consumption, a weight λ *(joules/second)* is introduced into the objective function to represent the extra energy consumption that the algorithm is prepared to endure to reduce the training delay. At the same time, according to the optimization theory, $1/\lambda$ is a Lagrange multiplier [42]. The problem of resource management for TBWFL (27) is non-convex due to multiple product with two functions in the goal function and constraint (27b).

First, we can select UEs with a given trust value from UAVs. These UEs should satisfy the condition $\gamma_u \geq \xi$ in order to participate in the following subproblems $\mathscr{P}_1$, $\mathscr{P}_2$, and $\mathscr{P}_3$. These subproblems are optimized and decomposed from the origin problem $\mathscr{P}$.

Then, for given the fixed values of μ and γ, we can decompose the objective function into the following two subproblems $\mathscr{P}_1$ and $\mathscr{P}_2$ when the UE trust is not considered.

$$\mathscr{P}_1 : \min_{f_u, T_c} \sum_{u=1}^{U} E_{u,c} + \lambda T_c \tag{28}$$

$$s.t. \max_{u} \frac{a_u S_u}{f_u} = T_c, \tag{28a}$$

$$F_u^m \leq f_u \leq F_u, \forall n \in N. \tag{28b}$$

Obviously,$\mathscr{P}_1$ illustrates a CPU cycle optimization of local computing delay and energy consumption, while $\mathscr{P}_1$ is regarded as power control of uplink, determining the time-sharing ratio of the device to minimize the energy and transmitting time of UEs. It is obvious that $\mathscr{P}_1$ is a convex problem. Thus, we obtain the solutions of TBWFL optimization based on the KKT method [42].

For $\mathscr{P}_1$, the optimal CPU frequency of UE can be divided into three cases according to their execution capabilities. We set the optimal f_u to be f_u^* and the optimal T_c to be T_c^*, so UEs in set $\mathcal{U}_1$ always run at the highest frequency $f_u^* = f_u^{\max}$; UEs in set $\mathcal{U}_2$ can complete the task quickly even if they run at the lowest frequency $f_u^* = f_u^{\min}$; UEs in set $\mathcal{U}_3$ have the best frequency inside its feasible set $f_u^* = \frac{a_u S_u}{T_c^*}$. T_c^* can be obtained $\max\{T_{\mathcal{U}_1}, T_{\mathcal{U}_2}, T_{\mathcal{U}_3}\}$, where $T_{\mathcal{U}_1} = \max_{u \in \mathcal{U}_1} \frac{a_u S_u}{F_u}$,$T_{\mathcal{U}_2} = \max_{u \in \mathcal{U}_2} \frac{a_u S_u}{F_u^m}$, and $T_{\mathcal{U}_3} = \left(\sum_{u \in \mathcal{U}_3} \theta_u \left(a_u S_u\right)^3 / \lambda\right)^{1/3}$.

Furthermore, we can observe that the optimal solutions reply not only on these subsets, but also on their cut-off $T_{\mathcal{U}_1}$, $T_{\mathcal{U}_2}$, and $T_{\mathcal{U}_3}$, where the longest cut-off among the subsets will influence the optimal cut-off T_c^*. The optimal frequency at the UE is determined by T_c^* and the specific subset that the UE belongs to.

Then the optimal solution of $\mathscr{P}_1$ varies with λ. When $\lambda \leq \min_{u \in \mathcal{U}} \theta_u \left(f_u^{\min}\right)^3$, only devices that can operate at the lowest frequency are allowed to exist at this time $T_c^* = \max_{u \in \mathcal{U}} \frac{a_u S_u}{f_u^{\min}}$, $f_u^* = f_u^{\min}$. When $\min_{u \in \mathcal{U}} \theta_u \left(f_u^{\min}\right)^3 < \lambda \leq \left(\max_{u \in \mathcal{U}_2} \frac{a_u S_u}{f_u^{\min}}\right)^3$, the devices that can operate at the lowest frequency and the devices with the best frequency within their feasible set are allowed to exist, at this time $T_c^* = \max\{T_{\mathcal{U}_2}, T_{\mathcal{U}_3}\}$,$f_u^* = \max\left\{f_u^{\min}, \frac{a_u S_u}{T_c^*}\right\}$. When $\left(\max\limits_{u \in \mathcal{U}_2} \frac{a_u S_u}{f_u^{min}}\right)^3 < \lambda \leq \frac{\sum_{u \in \mathcal{U}_3} \theta_u (a_u S_u)^3}{\left(\max\limits_{u \in \mathcal{U}} \frac{a_u S_u}{f_u^{max}}\right)^3}$, only the devices with the best frequency inside their feasible set can operate at this time $T_c^* = T_{\mathcal{U}_3}$,$f_u^* = \frac{a_u S_u}{T_{\mathcal{U}_3}}$. When $\frac{\sum_{u \in \mathcal{U}_3} \theta_u (a_u S_u)^3}{\left(\max\limits_{u \in \mathcal{U}} \frac{a_u S_u}{f_u^{max}}\right)^3} < \lambda$, only the devices in $\mathcal{U}_1$ are running at this time $T_c^* = T_{\mathcal{U}_1}$, $f_u^* = f_u^{\max}$.

The subproblem 2 is described as follows:

$$\mathscr{P}_2 : \min_{c_n, T_r} \sum_{u=1}^{U} E_{u,r} + \lambda T_r \tag{29}$$

$$s.t. \sum_{u \in U} c_u \leq T_r, \tag{29a}$$

$$P_u^m \leq p_u \leq P_u, \forall n \in N. \tag{29b}$$

We can also observe that the $\mathscr{P}_2$ is convex problem. For $\mathscr{P}_2$, we know $T_r^* = \sum_{u=1}^{N} c_u^*$. With the power function $p_u = \frac{N_0}{h_u}\left(e^{\frac{r_u}{B}} - 1\right)$ and the constraint (29b), we can derive the maximum and minimum time ratio required for UE when UE transmits at its minimum and maximum power. We introduce an indirect power control function, the power of which can be controlled by the weight λ to adjust the time ratio to transmit an amount of data d_u.

$$h_u(\lambda) = \frac{d_u/B}{1 + W\left(\frac{\lambda N_0^{-1} h_n - 1}{e}\right)}, \tag{30}$$

where $W(\cdot)$ represents the *Lambert W-function.*

The optimum solution of $\mathscr{P}_2$ varies according to the weight λ. When $\lambda \leq h_u^{-1}\left(c_u^{\max}\right)$, it means that the device always runs at the maximum power at this time $c_u^* = c_u^{\max}$. When $h_u^{-1}\left(c_u^{\max}\right) < \lambda < h_u^{-1}\left(c_u^{\min}\right)$, it means that the device will find a suitable power to send data at this time $\tau_u^{\min} < c_u^* < c_u^{\max}$. When $\lambda \geq g_u^{-1}\left(c_u^{\min}\right)$, the device is willing to run at the minimum power at this time $c_u^* = c_u^{\min}$. Furthermore, we can obtain $T_r^* = \sum_u c_u$.

We observe that the solutions of $\mathscr{P}_1$ and $\mathscr{P}_2$ after adding the trust constraint also do not depend on μ and γ, so we can get the optimal value T_c^*, T_r^* ,f^*,c^*,$E_{u,c}^*$ and $E_{u,r}^*$. These values will affect the third sub-problem of TBWFL as follows:

$$\mathscr{P}_3 : \min_{\mu > 0} \frac{1}{Z}\left(\lambda\left(T_r^* + N_l T_c^* + T_b^*\right) + \sum_{u=1}^{U} E_{u,r}^* + N_l E_{u,c}^*\right) \tag{31}$$

$$s.t. 0 < \mu < 1, 0 < Z < 1. \tag{31a}$$

where $Z = \frac{\gamma\left(2(\mu-1)^2 - \mu(\mu+1)(3\gamma+2)\rho^2 - \gamma\rho^2(\mu+1)\right)}{2\rho((1+\mu)^2\gamma^2\rho^2+1)}$.

Although $\mathscr{P}_3$ is non-convex, we can see that the only one variable need to be optimized in $\mathscr{P}_3$. Thus, we utilize the numerical optimization to solve the optimal solution.

The trust resource allocation can be performed in UAVs together with the blockchain in a semi-centralized manner, and the solutions of resource allocation are sent to all UEs. Then, the UEs carry out local training and transmit the aggregation parameters to the UAV based on the trust resource allocation solutions in ψ. The TBWFL can be implemented as follows: the trusted UEs are selected with trust quantification in blockchain-enabled UAVs at each FL round, and then the energy consumption of the UEs and the overall delay of FL are optimized with resource allocation using the trust value γ_u to capture the trade-off between the number of local and global rounds. In local round of FL, the trust value γ_u determined by

Algorithm 2 Trust Resource allocation

```
Input: $N_g$, $E_o$, $\lambda$, $T_g$, $T_r$, $T_c$, $F_u$, $F_u^{min}$, $P_u$, $P_u^m$, $F_k^b$,$F_k^{b,m}$, $\mu \in [0,1]$,$\gamma_u$
1: Trust user selection: The UEs are selected for participation in the resource allocation of subproblems based on the computed trust value $\gamma_u \geq \xi$ of UE in UAVs.
2: Subproblem 1: For given the fixed values of $\mu$ and $\gamma$, the optimal computation frequency $f_u$ and the optimal computation time $T_c$ of the CPU can be obtained by solving the subproblem $\mathscr{P}_1$ based on the KKT method.
3: Subproblem 2: For given the fixed values of $\mu$ and $\gamma$, the transmission time scale $c_u$ for UEs can be determined with the power control by weight $\lambda$ from the subproblem $\mathscr{P}_2$.
4: Subproblem 3: After having obtained the solution of $\mathscr{P}_1$ and $\mathscr{P}_2$, the only variable $\mu$ can be optimized by utilizing the numerical optimization to solve the subproblem $\mathscr{P}_3$.
```

T_b will affect the local and global gradient estimate to further determine the communication time T_r. Thus, the total time of each round is determined by $T_g = N_l T_c + T_r + T_b$. For the global round in FL, the μ by balancing the number of local and global rounds can optimize the energy and delay of tiny UE to determine the convergence of TBWFL. For the resource allocation of $\mathscr{P}$, the λ (Joules/second) is used to strike the trade-off between the energy cost of UE and the training time of the TBWFL. Therefore, our proposed TBWFL can strike a trade-off between the energy cost of UE and the local computing time, global communication time, and block production time for TBWFL in IUAV systems.

A. Stationary and Complexity Analysis

Then we discuss the complexity analysis on the combined solution of our approach. The problems $\mathscr{P}_1$ and $\mathscr{P}_2$ are solved separately, which means that each device usually takes two independent procedures: 1) local computing for the CPU and 2) transmission of parameters with wireless communication. The $\mathscr{P}_1$ and $\mathscr{P}_2$ are independent of μ since the wireless transmission in $\mathscr{P}_2$ has no influence on local accuracy, while the computation cost in $\mathscr{P}_2$ should be considered for each local round. We can see that the solutions to $\mathscr{P}_1$ and $\mathscr{P}_2$ play a significant role in discerning to what extent the communication cost outweighs the computation cost, which is a critical aspect in determining the optimal local accuracy. Thus, $\mathscr{P}_1$, $\mathscr{P}_2$, and $\mathscr{P}_3$ can be solved sequentially so that we can achieve the solutions to TBWFL. Furthermore, the complexities associated with our approach can also be summarized as follows: it will be $O(N^2)$ for $\mathscr{P}_1$, it will be $O(1)$ for $\mathscr{P}_2$, and it will be $O(N)$ for $\mathscr{P}_3$.

Moreover, the solutions of these subproblems $\mathscr{P}_1$, $\mathscr{P}_2$, and $\mathscr{P}_3$ should be stationary for TBWFL. The idea is straightforward by using the KKT condition to obtain the stable solutions of TBWFL. The KKT conditions are decomposed into three separate sets of expression with decoupling variables. The first two sets align with the KKT conditions of $\mathscr{P}_1$ and $\mathscr{P}_2$ that are addressed using closed-form expressions, and the final set for $\mathscr{P}_3$ can be solved using numerical optimization.

Table II: Experimental Parameters

Parameters	Value	Parameters	Value
Bandwith B	125 kHz	Tx power of UE p_u	$0.2 \sim 1$ mW
Data size of UE S_u	$300 \sim 800$ KB	Update size of UE d_u	0.5 KB
Max frequency of UE F_u	$36 \sim 64$ MHz	*Min* frequency of UE F_u^m	1 MHz
Capacitance coefficient of the UE chipset θ_u	2×10^{-28}	CPU cycles to one sample of data of UE a_u	$10 \sim 30$ cycles/bit
Requirement trust threshold ξ	0.6	Percentage of malicious UE PD	$10\% \sim 50\%$
Direct trust decay χ_d	0.5	Indirect trust decay χ_i	10

VI. Performance Evaluation

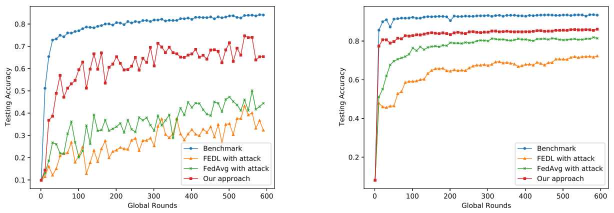
Evaluation Setting: In this section, our proposed trust management framework of TBWFL is verified with actual federated datasets MNIST and FEMNIST using multinomial logistic regression and cross-entropy error loss functions. These datasets vary in terms of sample sizes to demonstrate that FL can handle non-IID data. For MNIST, each UE encompasses three out of the total ten labels. While FEMNIST is constructed by splitting data derived from the expanded MNIST [43]. All datasets are randomly split, 75% is used for training and 25% is used for testing. The total amount of UEs is set to 100. Since FL algorithms are allowed to sample randomly, the number of UE participating in each round can be set to 10, and the maximum amount of local and global round can be set to 40 and 600, respectively. Table II gives the other experimental parameters for the simulation.

Furthermore, we conduct a comprehensive evaluation of the proposed trust-based model by incorporating it into various FL algorithms under different scenarios. The impact of the trust model on system performance is analyzed by varying parameters. The evaluation not only substantiates the effectiveness of our approach but also provides insight into how different parameters influence the performance of the WFL system. Specifically, we take into account a scenario featuring malicious behavior where a UE may provide model parameters that deliberately disrupt the FL process. This UE is known as a malicious IoT device, and we have varied its proportion from 10% to 50% in our experimental setup. Note that, as in most real-world cases, the malicious behavior of a malicious UE does not commence as a malicious UE but may suddenly deviate from previously honest behavior.

A. The effectiveness of our approach

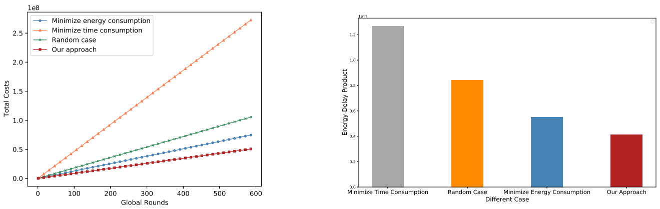
To illustrate the effectiveness of our approach, our initial experiment involved a comparison of the unattacked FEDL algorithm [12], the poisoned FEDL algorithm, the poisoned FedAvg algorithm [13], and our proposed scheme on two standard datasets. The total amount of FL rounds can be set to 600, using the unattacked FEDL algorithm as a benchmark for comparison. Figure 2a shows the experiments on the FEMNIST dataset, and Figure 2b shows the experiments on

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2024.3363443



(a) (b)

Figure 2: Comparison of our proposed algorithm with other algorithms for different cases on FEMNIST(a) and MNIST(b) datasets.



(a) (b)

Figure 3: Our proposed trust resource allocation scheme in terms of the total energy costs (a) and EDP (b)

the MNIST dataset. As observed in Figure 2, it is apparent that the benchmark algorithm demonstrates the fastest convergence amongst all schemes. Both the FEDL and FedAvg algorithms are susceptible to poisoning attacks, with FEDL more severely impacted. However, our proposed scheme significantly mitigates the impact of the poisoning attack and delivers trustworthy convergence on the WFL system.

B. Performance comparison of wireless resource allocation for TWBFL

We compare the minimize energy consumption, minimize time consumption, and random optimization methods with our proposed trust resource allocation method for TBWFL with respect to the total energy costs and the energy-delay product (EDP). The EDP is the product of the consumed energy and delay to complete the computing task and parameters transmission, which is usually employed to evaluate the trade-off between delay performance and energy consumption.

Figure 3a shows that the minimize the time consumption method requires much more energy than other schemes with the increasing amount of global rounds since all UEs operate the highest computing frequency and maximum transmitting power to minimize the delay. The minimize energy consumption scheme also leads to more energy consumption than our approach as the increasing amount of global rounds. This is because all UEs operate the lowest CPU frequency and minimum transmitting power, causing a retransmission delay in WFL increasing energy consumption. While the energy costs of the random case can be better than the minimize the time consumption method since the CPU frequency and transmitting power are set to random average value resulting in lower energy consumption. Furthermore, Figure 3b shows that our approach yields the lowest EDP because our approach can achieve the balance between energy costs and delay in TBWFL.

C. Trust Evaluation

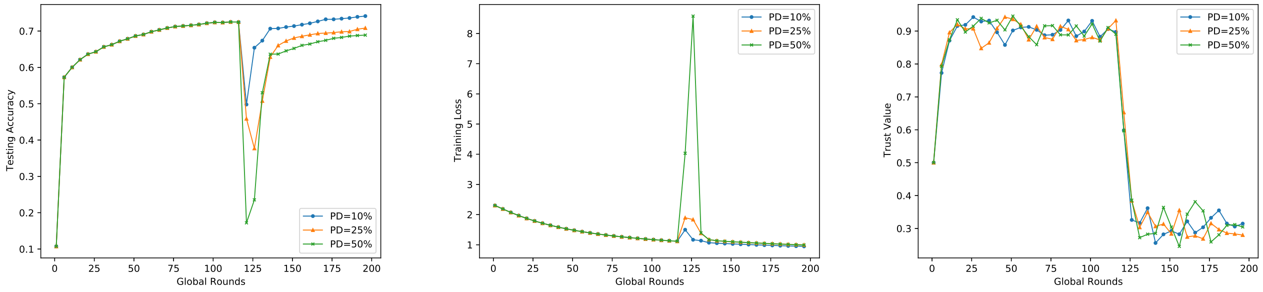
In Figure 4, the percentage of malicious user devices (PD) is set to 10%, 25%, and 50% to evaluate our approach for the FL process on the Femnist dataset. The performance of our proposed trust model is evaluated with the varying amount of UE IoT devices. All IoT devices consistently exhibit honest behavior, however, starting at round 120 the malicious IoT devices begin to alter their behavior, providing model parameters under a poisoning attack while the remaining nodes continue to contribute honest model parameters. Figure 4a and Figure 4b shows that testing accuracy and training loss with global round can recover the norm convergence for our approach from the different ratio malicious IoT devices,i.e.,from 10% to 50%. Meanwhile, Figure 4c displays the variations in trust value for the different ratio of malicious IoT devices.

As shown in Figure 4a, the accuracy drops to approximately half of its original value when 10% of devices are malicious. When this proportion increases to 25%, the accuracy is reduced to about 0.4 times its initial value. With 50% malicious devices, the FL process essentially has to restart, implying a significant negative effect on FL as the proportion of malicious devices increases. The observed drop in accuracy can be attributed to two main factors. Firstly, honest devices remain oblivious to the behavioral changes until they interact with a malicious device. Second, as the number of malicious devices increases, UAVs are more likely to be mislead into selecting malicious service devices for aggregation. However, after approximately 20 global rounds, the accuracy of TBWFL begins to converge and slowly approaches the level observed prior to the attack. The training loss values shown in Figure 4b have a similar change process as Figure 4a, which indicates that our proposed TBWFL model can efficiently secure the WFL process by mitigating the negative impact caused by malicious IoT devices.

Meanwhile, in Figure 4c, the trust values decline at a similar rate when the behavior of the device changes. Therefore, in Figure 4a and Figure 4b, the differential drop in accuracy and the differential increase in loss value can be attributed to the varying number of malicious UEs. In essence, we can infer that the decline in accuracy from round 120 to 200 is predominantly driven by malicious IoT devices supplying poisoning and attacking parameters. The UAV with edge server will adjust to change the trust value of UEs after identifying the malicious UEs, and when the trust value of UEs decreases, the UAVs no longer select the malicious service devices, which shows that our proposed TBWFL model exhibits a robust capability to accurately detect the behavioral shifts of UEs.

D. Evaluation of decay function

In Figure 5, we evaluate the impact of the decay function for our proposed trust management model. As seen in Figure 5a, the global accuracy of our TBWFL model incorporating the decay function experiences a smaller reduction after UEs alter their behaviors. Moreover, our TBWFL model integrated with

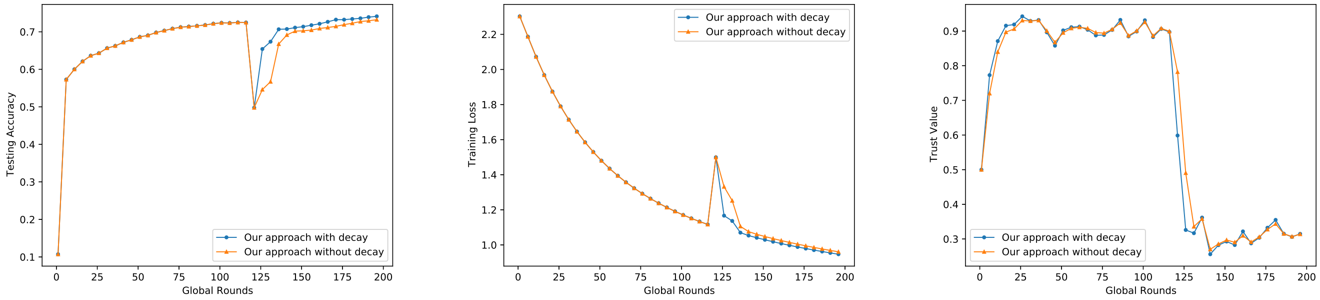


(a) accuracy with global round

(b) loss value with global round

(c) trust value with global round

Figure 4: The accuracy, loss value and trust value variation of our approach in the presence of 10%, 25% and 50% of malicious devices on the FEMNIST dataset.



(a) accuracy with global round

(b) loss value with global round

(c) trust value with global round

Figure 5: The accuracy, loss value and trust value change of the our approach in the presence of 10% of malicious devices on the FEMNIST dataset with and without the decay function

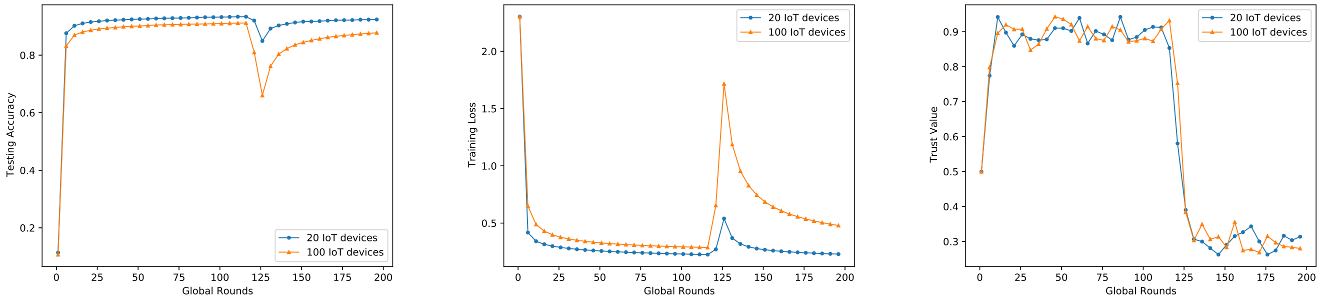
the decay function achieves a steady state faster than its counterpart that does not consider the decay function. This trend is also reflected in training loss, as depicted in Figure 5b. The quicker and more efficient adaptation can be attributed to the fact that, without the decay function, the weight of current behavior-based ratings is considered equivalent to that given to historical rating the trust computation. As a result, capturing behavioral changes becomes a slower and more extended process. Similarly, as shown in Figure 5c, the trust values in our TBWFL model with the decay function converge at a faster rate compared to the model with no consideration of the decay function. This can be explained by the higher weight assigned to new malicious behavior in trust calculations within the decay function model, causing the trust value to rapidly deteriorate. Consequently, malicious service devices are less likely to be selected for participation in a given round of aggregation in our TBWFL scheme with decay functions than these trust management scheme without decay functions.

E. Scalability Assessment

As depicted in Figure 6, we investigate the scalability of our proposed trust model in an experimental setting identical to that in Figure 5 on the MNIST data set. We configured two distinct service UE sizes: one with 15 honest UEs and 5 malicious UEs, and another with 75 honest IoT devices and 25 malicious UEs. By evaluating the scalability of our proposed model under these configurations, we can understand its performance and applicability in WFL systems, in the presence of varying numbers and proportions of honest and malicious IoT devices. Analyzing this can offer valuable insights into the reliability and robustness of our trust model under different scenarios.

In Figure 6a and Figure 6b, we can observe that with different numbers of UEs, comparable patterns can be generated by suddenly starting to provide poisoning model parameters after the 120th round, and then the global accuracy and training loss stabilize rapidly within approximately 25 global rounds. As the UE scalability increases, the global accuracy decreases slightly and the training loss values increase slightly. The reason is that the more UEs in the system lead to a greater selection pool for UAVs during trustworthy aggregating. Thus, it results in lower global accuracy and higher training loss values. Nevertheless, under both scalability settings, the global accuracy and training loss in our proposed model stabilize after a small amount of global rounds, which is beneficial for the FL process. In Figure 6c, we observe that the trust values of malicious IoT devices in our trust model demonstrate similar patterns under both scalability settings. As the amount of UEs increases, UAVs can detect changes of trust values for UE more rapidly and select other IoT devices with higher trust values. Therefore, our trust management model demonstrates robust scalability and holds potential for application in large-scale scenarios.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2024.3363443

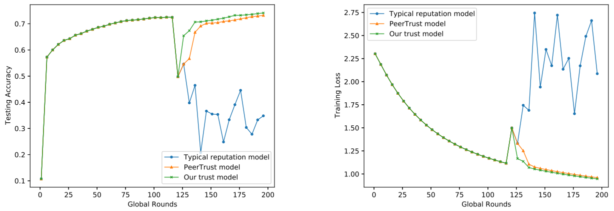


(a) accuracy with global round

(b) loss value with global round

(c) trust value with global round

Figure 6: The comparison of the accuracy, loss value and trust value of our approach in the presence of 25% malicious devices on MNIST dataset with 20 and 100 UEs



(a)

(b)

Figure 7: The comparison of the accuracy and loss value change of our approach on FEMNIST dataset for traditional trust model, PeerTrust trust model, and our proposed trust model

F. Performance Comparison of Different Trust Model

Figure 7 shows that the comparison of our trust approach with two typical schemes in the trust field: the traditional reputation scheme and the widely-applied PeerTrust scheme. We ensure that the experiment settings are the same as the conditions of the initial experiment, with the proportion of malicious IoT devices deliberately configured to 10%. The traditional reputation model computes the trust value of the UE by taking the mean of all of its trust values, therefore considering all past behaviors on an equal footing without granting any particular significance to the recent ones. While the PeerTrust model utilizes the advanced trust value model/direct trust calculation (TVM/DTC) technique to determine the trust values of UEs. This model deploys an adaptive time window-based algorithm by integrating the most recent dynamic behavior of UEs into its computations, thereby setting the nearest time window to align with three rounds, similar to our proposed trust model.

As is shown in Figure 7, our proposed trust model exhibits superior performance compared to the PeerTrust scheme, which is superior to the conventional reputation scheme. These three models display a similar trend during the FL process before any change in behavior by malicious IoT devices. However, when attacks occur, our model demonstrates marked resilience to the ensuing poisoning attacks, much more than the PeerTrust and traditional reputation models. The PeerTrust model with the adaptive time-window-based algorithm exhibits a more effective recognition of the dynamic behavior of UEs than the traditional model. However, it falls short compared to our trust model. These comparative results indicate that the unique design of our model by incorporating a trust decay function and direct and indirect trust can obtain a significant performance advantage. This underlines the potential of our model to effectively manage trust in mobile IoT devices in the context of WFL environments.

VII. Conclusions

In this paper, we proposed a semi-centralized trust management framework for blockchain-enabled tiny WFL in IUAV systems, which can provide a trust, fast, low latency and energy-efficient WFL aggregation model for IUAV systems. To mitigate the effect of malicious UEs in tiny FL, we designed the quantifiable trust model of UE by combining direct and indirect trust, including the consideration of a decay function and recommendation credibility for trust model to aggregate parameters in resource-constrained IUAV networks. To achieve the trust and energy efficiency for UEs to participate in the fast convergence of tiny WFL in IUAV networks, we embedded the trust model of tiny BWFL with wireless resource allocation to strike the trace-offs between computation time, communication time, block producing time, energy consumption and credibility evaluation for blockchain-enabled tiny WFL. The experimental results illustrated the effectiveness of our proposed TBWFL model in recognizing malicious UEs, particularly in dynamic scenarios where the behavior of UEs changes during the WFL aggregation process. The comparative results clearly showed that the superiority of our approach over the other considered typical trust management schemes. Our work has the potential to quantify the trustworthiness of UEs for the aggregation of the radio model parameters and to enhance system security together with fast convergence for tiny WFL. In the future, we can further investigate the cost of communication and computation of UAV and UAV trajectory for tiny WFL in IUAV situations.

Appendix A
Proof of Theorem 1

Since L-smooth and β-strongly convex $G_n(\cdot)$, we can obtain $\frac{||\nabla G_n(e)||^2}{2L} \leq G_n(e) - G_n(e^*) \leq \frac{||\nabla G_n(e)||^2}{2\beta}$,$\forall e$. Due to $(1-\sigma)^n \leq e^{-n\sigma}$, the μ-approximation condition $\|\nabla H_u^n(e_u^n)\| \leq$

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2024.3363443

$\mu \left\|\nabla H_u^n\left(e^{n-1}\right)\right\|$ when $c\frac{L}{\beta}e^{-n\sigma} \leq \mu^2$. With $\ln$ operation, we have $\ln c\frac{L}{\beta}e^{-n\sigma} \leq \ln\mu^2$, $\log c\frac{L}{\beta} + \ln e^{-n\sigma} \leq \ln\mu^2$, $\log v\frac{L}{\beta} - n\sigma \leq \ln\mu^2$, $\ln c\frac{L}{\beta} - \ln\mu^2 \leq n\sigma$, $\ln\frac{v\rho}{\mu^2} \leq n\sigma$, $\frac{1}{\sigma}\ln\frac{v\rho}{\mu^2} \leq n$. Therefore, the proof of Theorem 1 can be completed.

Appendix B
Proof of Theorem 2

With given UE trust local model $H_u^n(e)$ in (17), if $\hat{e}_u^n$ be the solution to $\min_{e\in\mathbb{R}^d} H_u^n(e)$, we have $\nabla H_u^n(e^{n-1}) = \gamma_u^n \nabla\bar{G}^{n-1}$ and $\nabla H_u^n(\hat{e}_u^n) = \nabla G_n(\hat{e}_u^n) + \gamma_u^n\nabla\bar{G}^{n-1} - \nabla G_u(e^{n-1}) = 0$.

Due to $G(\cdot)$ as L-Lipschitz smooth, we have as follows by using Jensen's inequality, L-smoothness, and Cauchy-Schwarz inequality

$$\begin{aligned}
&G(e_u^n) - G(e^{n-1}) \leq \left\langle \nabla G\left(e^{n-1}\right), e_u^n - e^{n-1}\right\rangle + \frac{L}{2}\left\|e_u^n - e^{n-1}\right\|^2 \\
&= \left\langle \nabla G\left(e^{n-1}\right) - \nabla\bar{G}^{n-1}, e_u^n - e^{n-1}\right\rangle \\
&\quad + \frac{L}{2}\left\|e_u^n - e^{n-1}\right\|^2 + \left\langle \nabla\bar{G}^{n-1}, e_u^n - e^{n-1}\right\rangle \\
&\leq \left\|\nabla G\left(e^{n-1}\right) - \nabla\bar{G}^{n-1}\right\| \left\|e_u^n - e^{n-1}\right\| \\
&\quad + \frac{L}{2}\left\|e_u^n - e^{n-1}\right\|^2 + \left\langle \nabla\bar{G}^{n-1}, e_u^n - e^{n-1}\right\rangle
\end{aligned} \tag{32}$$

$$\begin{aligned}
&\leq \left\|\nabla G\left(e^{n-1}\right) - \nabla\bar{G}^{n-1}\right\| \left\|e_u^n - e^{n-1}\right\| + \frac{L}{2}\left\|e_u^n - e^{n-1}\right\|^2 \\
&\quad - \frac{1}{\gamma}\left\langle \nabla G_n\left(\hat{e}_u^n\right) - \nabla G_u\left(e^{n-1}\right), e_u^n - e^{n-1}\right\rangle \\
&= \left\|\nabla G\left(e^{n-1}\right) - \nabla\bar{G}^{n-1}\right\| \left\|e_u^n - e^{n-1}\right\| + \frac{L}{2}\left\|e_u^n - e^{n-1}\right\|^2 \\
&\quad - \frac{1}{\gamma}\left\langle \nabla G_u\left(\hat{e}_u^n\right) - \nabla G_n\left(e_u^n\right), e_u^n - e^{n-1}\right\rangle \\
&\quad - \frac{1}{\gamma}\left\langle \nabla G_u\left(e_u^n\right) - \nabla G_u\left(e^{n-1}\right), e_u^n - e^{n-1}\right\rangle
\end{aligned} \tag{33}$$

$$\begin{aligned}
&\leq \left\|\nabla G\left(e^{n-1}\right) - \nabla\bar{G}^{n-1}\right\| \left\|e_u^n - e^{n-1}\right\| + \frac{L}{2}\left\|e_u^n - e^{n-1}\right\|^2 \\
&\quad + \frac{L}{\gamma}\left\|\hat{e}_u^n - e_u^n\right\| \left\|e_u^n - e^{n-1}\right\| - \frac{1}{\gamma L}\left\|\nabla G_n\left(e_u^n\right) - \nabla G_u\left(e^{n-1}\right)\right\|^2,
\end{aligned} \tag{34}$$

where $\gamma = \min\{\gamma_u^n\}$.

For above norm terms, we have $\left\|\hat{e}_u^n - e^{n-1}\right\| \leq \frac{1}{\beta}\left\|\nabla H_n^t\left(e^{n-1}\right)\right\| = \frac{\gamma_u^n}{\beta}\left\|\nabla\bar{G}^{n-1}\right\| \leq \frac{\gamma}{\beta}\left\|\nabla\bar{G}^{n-1}\right\|$ and $\left\|\hat{e}_u^n - e_u^n\right\| \leq \frac{1}{\beta}\|\nabla H_u^n(e_u^n)\| \leq \frac{\mu}{\beta}\left\|\nabla H_u^n\left(e^{n-1}\right)\right\| = \frac{\mu\gamma_u^n}{\beta}\left\|\nabla\bar{G}^{n-1}\right\| \leq \frac{\mu\gamma}{\beta}\left\|\nabla\bar{G}^{t-1}\right\|$. By using triangle inequality, we can obtain $\|e_u^n - e^{n-1}\| \leq \|e_u^n - \hat{e}_u^n\| + \|\hat{e}_u^n - e^{n-1}\| \leq (1+\mu)\frac{\gamma}{\beta}\left\|\nabla\bar{G}^{n-1}\right\|$. We also have$\|\nabla G_n(e_u^n) - \nabla G_u(e^{n-1})\| = \left\|\nabla H_u^n(e_u^n) - \nabla H_u^n(e^{n-1})\right\| \geq \|\nabla H_u^n(e^{n-1})\| - \|\nabla H_u^n(e_u^n)\| \geq (1-\mu)\|\nabla H_u^n(e^{n-1})\| \geq (1-\mu)\gamma\left\|\nabla\bar{G}^{n-1}\right\|$.

We define $\nabla F(.)$ and $\nabla\bar{F}^{t-1}$, then we can obtain

$$\begin{aligned}
&\|\nabla G(e^{n-1}) - \nabla\bar{G}^{n-1}\| = \left\|\sum_{u=1}^{U}\frac{S_u}{S}\left(\nabla G_n(e_u^n) - \nabla G_u(e^{n-1})\right)\right\| \\
&\leq \sum_{u=1}^{U}\frac{S_u}{S}\left\|\nabla G_u(e_u^n) - \nabla G_u(e^{n-1})\right\| \leq \sum_{u=1}^{U}\frac{S_u}{S}L\left\|e_n^t - e^{n-1}\right\| \\
&\leq (1+\mu)\gamma\frac{L}{\beta}\left\|\nabla\bar{G}^{n-1}\right\|.
\end{aligned} \tag{35}$$

Therefore, it is obtained with

$$\begin{aligned}
\left\|\nabla G(e^{n-1})\right\|^2 &\leq 2\left\|\nabla\bar{G}^{n-1} - \nabla G(e^{n-1})\right\|^2 + 2\left\|\nabla\bar{G}^{n-1}\right\|^2 \\
&\leq 2(1+\mu)^2\gamma^2\rho^2\left\|\nabla\bar{G}^{n-1}\right\|^2 + 2\left\|\nabla\bar{G}^{n-1}\right\|^2.
\end{aligned} \tag{36}$$

We further have

$$\left\|\nabla\bar{G}^{n-1}\right\|^2 \geq \frac{1}{2(1+\mu)^2\gamma^2\rho^2 + 2}\left\|\nabla G(e^{n-1})\right\|^2. \tag{37}$$

If we define X as $X = \frac{\gamma(-2(\mu-1)^2 + (\mu+1)\mu(3\gamma+2)\rho^2 + (\mu+1)\gamma\rho^2)}{2\rho} < 0$, then we can obtain as follows:

$$\begin{aligned}
&G(e_u^n) - G(e^{n-1}) \leq \frac{X}{\beta}\left\|\nabla\bar{G}^{n-1}\right\|^2 \\
&\leq \frac{X}{2\beta\big((1+\mu)^2\gamma^2\rho^2 + 1\big)}\left\|\nabla G(e^{n-1})\right\|^2 \\
&= -\frac{\gamma(2(\mu-1)^2 - (\mu+1)\mu(3\gamma+2)\rho^2 - (\mu+1)\gamma\rho^2)}{2\rho\big((1+\mu)^2\gamma^2\rho^2 + 1\big)} \\
&\times \big(G(e^{n-1}) - G(e^*)\big).
\end{aligned} \tag{38}$$

By subtracting $G(e^*)$ from both sides of the above, we have

$$\begin{aligned}
&G(e_u^n) - G(e^*) \\
&\leq (1 - \frac{\gamma(2(\mu-1)^2 - (\mu+1)\mu(3\gamma+2)\rho^2 - (\mu+1)\gamma\rho^2)}{2\rho\big((1+\mu)^2\gamma^2\rho^2 + 1\big)}) \\
&\times \left(G(e^{n-1}) - G(e^*)\right), \forall n.
\end{aligned} \tag{39}$$

Therefore, we can obtain

$$\begin{aligned}
&G(e^n) - G(e^*) \leq \sum_{u=1}^{U}\frac{S_u}{S}\big(G(e_u^n) - G(e^*)\big) \\
&\leq (1 - \frac{\gamma(2(\mu-1)^2 - (\mu+1)\mu(3\gamma+2)\rho^2 - (\mu+1)\gamma\rho^2)}{2\rho\big((1+\mu)^2\gamma^2\rho^2 + 1\big)}) \\
&\times (G(e^{n-1}) - G(e^*)) \\
&\leq (1 - \frac{\gamma(2(\mu-1)^2 - (\mu+1)\mu(3\gamma+2)\rho^2 - (\mu+1)\gamma\rho^2)}{2\rho\big((1+\mu)^2\gamma^2\rho^2 + 1\big)})^n \\
&\times (G(e^0) - G(e^*)).
\end{aligned} \tag{40}$$

Similar to the proof of Theorem 1 with $c(1-\sigma)^n$, $G(e^n) - G(e^*) \leq \delta$ and $\ln$ operation for both side of inequation, we can obtain N_g and complete the proof of Theorem 2.

References

[1] L. U. Khan, W. Saad, Z. Han, and C. S. Hong, "Dispersed federated learning: Vision, taxonomy, and future directions," *IEEE Wireless Communications*, vol. 28, no. 5, pp. 192–198, 2021.

[2] L. U. Khan, W. Saad, Z. Han, E. Hossain, and C. S. Hong, "Federated learning for internet of things: Recent advances, taxonomy, and open challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1759–1799, 2021.

[3] Z. Ning, Y. Yang, X. Wang, L. Guo, X. Gao, S. Guo, and G. Wang, "Dynamic computation offloading and server deployment for uav-enabled multi-access edge computing," *IEEE Transactions on Mobile Computing*, vol. 22, no. 5, pp. 2628–2644, 2023.

[4] Y. M. Saputra, D. N. Nguyen, D. T. Hoang, T. X. Vu, E. Dutkiewicz, and S. Chatzinotas, "Federated learning meets contract theory: Economic-efficiency framework for electric vehicle networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 8, pp. 2803–2817, 2022.

[5] Y. M. Saputra, D. T. Hoang, D. N. Nguyen, L.-N. Tran, S. Gong, and E. Dutkiewicz, "Dynamic federated learning-based economic framework for internet-of-vehicles," *IEEE Transactions on Mobile Computing*, vol. 22, no. 4, pp. 2100–2115, 2023.

[6] M. Chen, D. Gündüz, K. Huang, W. Saad, M. Bennis, A. V. Feljan, and H. V. Poor, "Distributed learning in wireless networks: Recent progress and future challenges," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 12, pp. 3579–3605, 2021.

[7] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato, and A. A. A. El-Latif, "A secure federated learning framework for 5G networks," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 24–31, 2020.

[8] Y.-A. Xie, J. Kang, D. Niyato, N. T. T. Van, N. C. Luong, Z. Liu, and H. Yu, "Securing federated learning: A covert communication-based approach," *IEEE Network*, vol. 37, no. 1, pp. 118–124, 2023.

[9] J. Zheng, H. Zhang, J. Kang, L. Gao, J. Ren, and D. Niyato, "Covert federated learning via intelligent reflecting surfaces," *IEEE Transactions on Communications*, pp. 1–1, 2023.

[10] J. Kang, Z. Xiong, D. Niyato, Y. Zou, Y. Zhang, and M. Guizani, "Reliable federated learning for mobile networks," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 72–80, 2020.

[11] M. Salehi and E. Hossain, "Federated learning in unreliable and resource-constrained cellular wireless networks," *IEEE Transactions on Communications*, vol. 69, no. 8, pp. 5136–5151, 2021.

[12] C. T. Dinh, N. H. Tran, M. N. H. Nguyen, C. S. Hong, W. Bao, A. Y. Zomaya, and V. Gramoli, "Federated learning over wireless networks: Convergence analysis and resource allocation," *IEEE/ACM Transactions on Networking*, vol. 29, no. 1, pp. 398–409, 2021.

[13] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Artificial intelligence and statistics*, pp. 1273–1282, PMLR, 2017.

[14] X. Wang, Z. Ning, L. Guo, S. Guo, X. Gao, and G. Wang, "Mean-field learning for edge computing in mobile blockchain networks," *IEEE Transactions on Mobile Computing*, vol. 22, no. 10, pp. 5978–5994, 2023.

[15] Z. Yang, R. Wang, D. Wu, B. Yang, and P. Zhang, "Blockchain-enabled trust management model for the internet of vehicles," *IEEE Internet of Things Journal*, vol. 10, no. 14, pp. 12044–12054, 2023.

[16] O. A. Wahab, A. Mourad, H. Otrok, and T. Taleb, "Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1342–1397, 2021.

[17] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, "A joint learning and communications framework for federated learning over wireless networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 269–283, 2021.

[18] P. Hou, X. Jiang, Z. Wang, S. Liu, and Z. Lu, "Federated deep reinforcement learning-based intelligent dynamic services in UAV-assisted mec," *IEEE Internet of Things Journal*, pp. 1–1, 2023.

[19] N. Li, X. Song, K. Li, R. Jiang, and J. Li, "Multiagent federated deep-reinforcement-learning-enabled resource allocation for an air–ground-integrated internet of vehicles network," *IEEE Internet Computing*, vol. 27, no. 5, pp. 15–23, 2023.

[20] S. Wang, S. Hosseinalipour, M. Gorlatova, C. G. Brinton, and M. Chiang, "UAV-assisted online machine learning over multi-tiered networks: A hierarchical nested personalized federated learning approach," *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1847–1865, 2023.

[21] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor, "Federated learning for internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021.

[22] A. Imteaj, U. Thakker, S. Wang, J. Li, and M. H. Amini, "A survey on federated learning for resource-constrained IoT devices," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 1–24, 2022.

[23] H. Chen, S. Huang, D. Zhang, M. Xiao, M. Skoglund, and H. V. Poor, "Federated learning over wireless IoT networks with optimized communication and resources," *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 16592–16605, 2022.

[24] H. Huang, L. Zhang, C. Sun, R. Fang, X. Yuan, and D. Wu, "Distributed pruning towards tiny neural networks in federated learning," in *2023 IEEE 43rd International Conference on Distributed Computing Systems (ICDCS)*, pp. 190–201, 2023.

[25] N. Xiong and S. Punnekkat, "Tiny federated learning with bayesian classifiers," in *2023 IEEE 32nd International Symposium on Industrial Electronics (ISIE)*, pp. 1–6, 2023.

[26] H. Ren, D. Anicic, and T. A. Runkler, "TinyReptile: TinyML with federated meta-learning," in *2023 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–9, 2023.

[27] X. Wang, X. Ren, C. Qiu, Z. Xiong, H. Yao, and V. C. M. Leung, "Integrating edge intelligence and blockchain: What, why, and how," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2193–2229, 2022.

[28] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 7, pp. 5098–5107, 2021.

[29] S. K. Lo, Y. Liu, Q. Lu, C. Wang, X. Xu, H.-Y. Paik, and L. Zhu, "Toward trustworthy AI: Blockchain-based architecture design for accountability and fairness of federated learning systems," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3276–3284, 2023.

[30] J. Qi, F. Lin, Z. Chen, C. Tang, R. Jia, and M. Li, "High-quality model aggregation for blockchain-based federated learning via reputation-motivated task participation," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18378–18391, 2022.

[31] S. Otoum, I. A. Ridhawi, and H. Mouftah, "Securing critical IoT infrastructures with blockchain-supported federated learning," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2592–2601, 2022.

[32] W. Yu, A. Chorti, L. Musavian, H. Vincent Poor, and Q. Ni, "Effective secrecy rate for a downlink NOMA network," *IEEE Transactions on Wireless Communications*, vol. 18, no. 12, pp. 5673–5690, 2019.

[33] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and privacy on 6G network edge: A survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1095–1127, 2023.

[34] H. Zhang, M. Huang, H. Zhou, X. Wang, N. Wang, and K. Long, "Capacity maximization in RIS-UAV networks: A DDQN-based trajectory and phase shift optimization approach," *IEEE Transactions on Wireless Communications*, vol. 22, no. 4, pp. 2583–2591, 2023.

[35] X. Qin, Z. Song, T. Hou, W. Yu, J. Wang, and X. Sun, "Joint optimization of resource allocation, phase shift, and UAV trajectory for energy-efficient RIS-assisted UAV-enabled MEC systems," *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 4, pp. 1778–1792, 2023.

[36] M. Chowdhary, D. Lilienthal, S. S. Saha, and K. C. Palle, "AutoML for on-sensor tiny machine learning," *IEEE Sensors Letters*, pp. 1–4, 2023.

[37] X. Wang, Z. Ning, S. Guo, M. Wen, L. Guo, and H. V. Poor, "Dynamic uav deployment for differentiated services: A multi-agent imitation learning based approach," *IEEE Transactions on Mobile Computing*, vol. 22, no. 4, pp. 2131–2146, 2023.

[38] S. Wang, T. Tuor, T. Salonidis, K. K. Leung, C. Makaya, T. He, and K. Chan, "Adaptive federated learning in resource constrained edge computing systems," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1205–1221, 2019.

[39] R. Yingjie, S. Zhongyi, Y. Chang, W. Lisa, L. Haifeng, C. Yuhua, N. Ling, and Z. Chubin, "Real-time transmission and configuration strategy of measurement data based on newton's law of cooling," in *2021 2nd International Conference on Electronics, Communications and Information Technology (CECIT)*, pp. 884–888, 2021.

[40] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," *Proceedings of Machine learning and systems*, vol. 2, pp. 429–450, 2020.

[41] T. Burd and R. Brodersen, "Processor design for portable systems," *Journal of VLSI Signal Processing*, vol. 13, no. 2-3, pp. 203–221, 1996.

[42] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

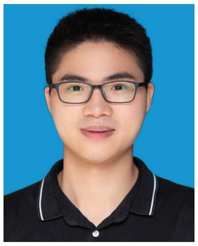
[43] G. ohen, S. Afshar, J. Tapson, and A. van Schaik, "EMNIST: Extending MNIST to handwritten letters," *in 2017 International Joint Conference on Neural Networks (IJCNN)*, pp. 2921–2926, May 2017.

Jie Zheng is currently an associate professor in the information science and technology institute at Northwest University, Xi'an, China. He received the B.Sc degree in Communications Engineering from Nanchang University, China, in 2008. He received his Ph.D. degree in the Department of Telecommunications Engineering at Xidian University in 2014. He research interests include heterogeneous networks, energy-efficient transmission, wireless resource allocation, and edge intelligence.

Jipeng Xu is currently pursuing BS degree in information science and technology institute from Northwest University. His research includes federated learning, wireless resource allocation, and edge intelligence.

Hongyang Du received the B.Sc. degree from Beijing Jiaotong University, Beijing, China, in 2021. He is currently pursuing the Ph.D. degree with the School of Computer Science and Engineering, Energy Research Institute, Nanyang Technological University, Singapore, under the Interdisciplinary Graduate Program. His research interests include semantic communications, reconfigurable intelligent surface, and communication theory. He was a recipient of the IEEE Daniel E. Noble Fellowship Award in 2022. He was recognized as an Exemplary Reviewer of the IEEE TRANSACTIONS ON COMMUNICATIONS in 2021.

Dusit Niyato Dusit Niyato (Fellow, IEEE) received the B.Eng.degree from the King Mongkuts Institute of Technology Ladkrabang, Thailand, in 1999, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Winnipeg, MB, Canada, in 2008. He is currently a Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests are in the areas of Internet of Things (IoT), machine learning, and incentive mechanism design.



Jiawen Kang received the Ph.D. degree from the Guangdong University of Technology, China, in 2018. He was a Post-Doctoral Researcher at Nanyang Technological University, Singapore, from 2018 to 2021. He is currently a Full Professor at the Guangdong University of Technology. His research interests include blockchain, security, and privacy protection in wireless communications and networking.

Jiangtian Nie received her B.Eng. degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China and the Ph.D. degree in ERI@N from Interdisciplinary Graduate School, Nanyang Technological University (NTU), Singapore. She is currently a Research Fellow with NTU. Her research interests include network economics, game theory, and crowd sensing and learning. She is currently the Editor of Computer Networks, Computer Communications, Physical Communication, and EURASIP Journal on Wireless Communications and Networking.

Zheng Wang is currently an professor with the University of Leeds. His research cut across the boundaries of parallel program optimisation,systems security, and applied machine learning. He received four best paper awards for his work on machine learning-based compiler optimisation (PACT '10, CGO '17, PACT '17, and CGO '19).