Securing Data Sharing from the Sky: Integrating Blockchains into Drones in 5G and Beyond

Jiawen Kang, Zehui Xiong, Dusit Niyato, Shengli Xie, and Dong In Kim

Abstract

5G and beyond (B5G) networks significantly promote the popularity and ubiquity of drones by providing high-throughput and low-latency communication. In B5G drone networks, data sharing among drones has great potential to improve and enrich civilian and commercial applications, such as surveillance monitoring. Nevertheless, a series of security challenges arise such as data privacy leakage due to the lack of reliable centralized supervision. In this article, we employ the permissioned blockchain technology to propose a decentralized data management system. The permissioned blockchain deployed at pre-selected ground base stations is particularly suitable and practical for ensuring efficient peer-to-peer data sharing in B5G drone networks. However, the ground base stations working as miners are widely deployed without strong security protection, which may be compromised to produce maliciously manipulated results during the block verification in the permissioned blockchain. Hence, the miner selection is crucial for the permissioned blockchain-based B5G drone networks. We therefore introduce credit as a metric and propose a secure credit-based miner selection scheme using a four-weight subjective logic model. Numerical results demonstrate that the proposed schemes are effective for secure data sharing in permissioned blockchain-based B5G drone networks.

Introduction

Along with the rapid developments in 5G and beyond (B5G) communication technologies, drone networks have evolved into B5G drone networks that not only enhance existing drone applications (e.g., remote sensing), but also introduce advanced applications with the requirement of reliable and low-latency communications (e.g., virtual reality) [1, 2]. In B5G drone networks, drones that belong to different owners share collected data to overcome visual coverage and geographical region limitation, enrich diversity of sensing data, and improve data reliability [3]. Although the B5G drone networks reap great benefits of data sharing, the public concern about data sharing security is growing since the collected data includes a large volume of sensitive information (e.g., locations and human activity information [1, 4]). On one hand, drones may be reluctant to store and share data through ground cloud/edge infrastructures under a centralized management framework because of no control over the data and few monitoring operations. On the other hand, although the problems of the centralized management framework can be solved in a peer-to-peer (P2P) data sharing manner, there are still unauthorized data access problems and security protection issues in a decentralized management framework. These challenges hinder the circulation of collected data, thus becoming a bottleneck in the future proliferation of B5G drone networks [5].

Blockchain technologies have attracted increasing attention for exploring its potential in ensuring secure data sharing over a tamper-proof and decentralized ledger recently [5]. The authors in [6] utilized blockchain to design a UAV traffic information exchange network for securely sharing traffic data. To ensure drone data integrity and achieve secure data management, a permissionless blockchain-based drone system was proposed for future Internet of Things applications [7].

Although blockchain greatly facilitates open and secure data sharing scenarios, there is an exorbitant cost to build a permissionless blockchain in ground communication infrastructures or resource-limited drones [8, 9]. Therefore, permissioned blockchains, which quickly perform consensus mechanisms on pre-defined miners with modest overhead, are proposed to develop secure vehicular data sharing systems [5] and spectrum trading [10], which are efficient and particularly practical for B5G drone networks [10, 11].

In PErmissioned blockchain-based 5G and beyond DrOne Networks (PEGDONs), communication infrastructures, such as ground base stations (GBSs), are widely deployed on the ground and easily accessible by drones [4, 5]. With the help of edge computing, GBSs, with abundant computation and storage resources, play significant roles (i.e., miners) in publicly verifying and storing sharing records [12]. However, the GBSs are vulnerable to being directly compromised if there is not sufficient security protection [5, 12]. The compromised GBSs may be selected as the pre-defined miners due to there being no secure miner selection schemes for permissioned block-

Jiawen Kang and Dusit Niyato are with Nanyang Technological University; Zehui Xiong (corresponding author) is with Singapore University of Technology and Design; Shengli Xie is with Guangdong University of Technology, the Guangdong-Hong Kong-Macao Joint Laboratory for Smart Discrete Manufacturing, and the Ministry of Education; Dong In Kim is with Sungkyunkwan University.

Digital Object Identifier:
10.1109/MNET.011.2000183

0890-8044/21/$25.00 © 2021 IEEE

chains [11]. PEGDONs suffer from a potential attack called *block verification collusion* caused by compromised miners [9, 11], who may collude with other miners internally and thus produce manipulated block verification results, or even launch double-spending attack. This attack is difficult to detect and prevent [11]. Therefore, it is essential to develop a secure and effective miner selection scheme to defend against the block verification collusion attack in the PEGDONs.

The existing studies have indicated that credit can reflect the rating of how well an entity has so far performed based on its past interaction activities [5, 12]. Inspired by this, we utilize the credit as a fair metric to design a secure and generalized miner selection scheme for the permissioned blockchain. High-credit miner candidates (i.e., reliable and trusted GBSs) are selected as miners to promote secure block verification. Each drone performs credit assessment of an interacting GBS by using a four-weight subjective logic model [5]. All the drones' credit opinions on miner candidates are collected and kept as reliable and tamper-proof credit records in the transparent permissioned blockchain for efficient credit management. Different from previous work, the major contributions of this article are summarized as follows:

- We employ practical permissioned blockchain technologies to establish a universal and secure drone data sharing system in B5G drone networks that efficiently performs consensus processes on pre-selected GBSs.
- We summarize the existing and potential miner selection challenges in permissioned blockchain-based B5G drone networks, and propose a universal credit-based secure miner selection scheme to defend against the block verification collusion attack.
- To achieve secure and efficient credit management, we apply a four-weight subjective logic model with high accuracy to assess miner credit, and also record the credit in a decentralized and tamper-proof manner.

Permissioned Blockchain for Secure Data Sharing in Drone Networks

Permissioned Blockchains for Drone Networks

Recently, blockchain has been applied in various networks and distributed systems, such as drone networks [1, 3, 4, 6–8]. Blockchains can be divided into two categories: permissionless and permissioned blockchains. A permissionless blockchain has better information transparency and auditability without access limitation. {However, both exorbitant mining overhead and high block verification delay make permissionless blockchains impractical for resource-limited, time-sensitive, and high-mobility drone networks. Compared to permissionless blockchains, recently, permissioned blockchains have attracted enormous attention because of modest overhead, good scalability, and low consensus delay [11]. The permissioned blockchain can perform lightweight and low-latency consensus algorithms among a set of pre-selected miners to maintain the distributed ledger [9], which is particularly suitable and practical for drone networks with high-mobility unmanned aerial vehicles [11]. Recent studies have utilized permissioned blockchains to establish efficient and secure resource sharing systems, for example, vehicular data sharing in [5] and spectrum trading [10], which shows great potential of permissioned blockchains on secure data sharing in B5G drone networks [10].

The compromised miners may arbitrarily insert, modify, drop, or delay some unverified transactions during block verification process. This causes serious security problems for PEGDONs. Therefore, it is inevitable to propose a universal and secure miner selection scheme for improving security of PEGDONs, given the following challenges.

Motivations and Challenges

Although permissioned blockchains pave the way for good-performance blockchain-based drone networks, there are still critical security challenges in PEGDONs, such as miner collusion issues. In PEGDONs, GBSs are widely deployed on the ground or buildings to efficiently communicate with drones through B5G protocols. Therefore, GBSs can work as pre-selected miners to execute important tasks including block mining and verification [5, 12]. However, the openness and complexity of drone network architectures pose significant challenges for B5G drone networks. As a result, GBSs without sufficient security protection are susceptible to arbitrary manipulation by attackers, and might become compromised GBSs. If a compromised GBS is selected as a miner, this compromised miner can collude with other compromised miners to launch a special kind of security attack named *block verification collusion* for generating false block verification results. More specifically, the compromised miners may arbitrarily insert, modify, drop, or delay some unverified transactions during the block verification process [5]. This causes serious security problems for PEGDONs. Therefore, it is inevitable to propose a universal and secure miner selection scheme for improving security of PEGDONs, given the following challenges [13].

Evaluation Metrics for Miner Candidates: In traditional blockchain systems, miners are usually selected randomly through metrics of resource competition, for example, computing-power based proof-of-work and stake based proof of stake [12]. However, the computation-intensive and energy-hungry methods are not suitable and practical for PEGDONs. It is necessary to propose a reliable metric for PEGDONs to fairly evaluate the behavior and performance of miner candidates.

Miner Selection Schemes for PEGDONs: Unlike permissionless blockchains that select miners through proof-based algorithms, the existing permissioned blockchains select miners either by a centralized manager suffering from single point of failure problems, or in a decentralized way with insecurely random selection mechanisms [11]. As such, the miner selection schemes are arbitrary, which cannot avoid the negative influence of malicious nodes. For PEGDONs, without a fair and reliable metric, it is difficult to design an effective, universal, and secure miner selection scheme in order to avoid compromised miner candidates, and thus ensure a secure consensus process in permissioned blockchains.

Surveillance Methods for Selected Miners: Due to the decentralized nature of permissioned blockchains, it is difficult and inefficient to achieve real-time surveillance of selected miners. If a selected miner is compromised and misbehaved in PEGDONs, the miner cannot be removed from the system due to the lack of timely and flexible surveillance methods. Worse, compromised miners may be selected to be miners again without time-accumulated metrics to update the behavior and performance of the miner candidates.

Credit Management for Secure Data Sharing in PEGDONs

In terms of secure resource sharing, recent studies have utilized credit to improve resource sharing security in blockchain-based wireless networks. Generally, credit is treated as a metric to identify whether a node is well-behaved or malicious according to its credit points. The credit metric has been used to select trusted nodes for reliable message routing and resource sharing in wireless communications [5]. For example, the authors in [12] proposed a decentralized trust management system using blockchain in vehicular networks, where the vehicles assess the credibilities of received messages through trust value (i.e., credit). Similarly, to ensure high-quality data sharing among vehicles, a credit-based data sharing scheme was proposed for vehicular edge networks in [5]. Therein, the credit is regarded as a criterion to select high-quality data providers with high credit that provide good-quality data.

Inspired by the great potential of credit in coping with resource sharing problems in blockchain-based systems, we adopt credit as a metric to select secure and reliable miners for blockchain-based drone networks. In this article, we apply the practical permissioned blockchain technologies to establish a much more generalized data sharing system without the requirement of specific consensus algorithms. A universal credit-based miner selection scheme with an enhanced subjective logic model is also proposed to enable secure data sharing. More details are depicted as follows.

As shown in Fig. 1, drones equipped with B5G communication devices can obtain reliable and communication services from nearby GBSs in a drone-to-GBS manner, and also achieve superfast information transmission in a drone-to-drone manner. All the GBSs can be connected with each other through ultra-reliable low-latency internal communication networks. These GBSs provide 5G communication interfaces between the drones and other entities (e.g., drones and miners). On one hand, the drones can collect local sensing data, perform simple computation, and send the data to drone owners through the GBSs [2, 4]. On the other hand, drones acting as data providers share the data with data requesters and obtain rewards from the data requesters. The data providers send their data sharing records as "transactions" to nearby GBSs (① of Fig. 1). Next, the pre-selected miners can flexibly choose and execute practical and energy-saving consensus algorithms, for example, Practical Byzantine Fault Tolerance (PBFT) or Raft, to decrease consensus delay and resource consumption [11]. We consider that the credit can reflect how well an entity has so far performed in block mining and verification. GBSs with high credit are more likely to be selected as miners. Here, we use a four-weight subjective logic model (more details are described below) to calculate the credit values of the GBSs. Finally, the data sharing records among the drones are included in data blocks, and become proof of presence of data sharing when being added into the permissioned blockchain, named drone blockchain.

Credit opinions about GBSs play a significant role in PEGDONs; hence, these opinions should be securely stored and managed. Therefore, the credit opinions are also maintained in the drone blockchain as transparent, trusted, and persistent evidence [5, 14]. As depicted in Fig. 1, drones assess the behaviors of the GBSs (that offer communication services) as well as the pre-selected miners (that perform the consensus process), and generate and upload their direct credit opinions

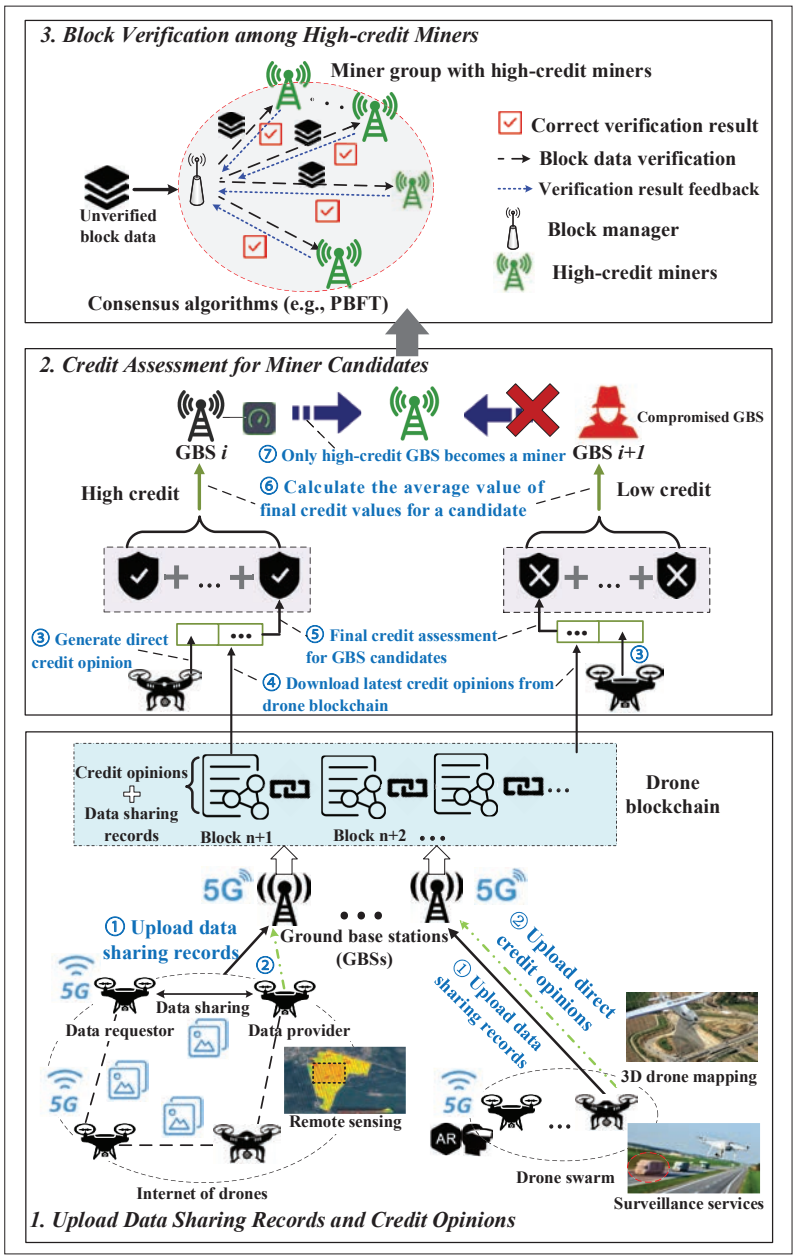

FIGURE 1. Permissioned blockchain-based B5G drone networks for secure data sharing.

(② and ③ in Fig. 1). When calculating the credit values of miner candidates, the drones first download the latest credit opinions about the candidates as indirect credit opinions from the drone blockchain. After that, the drones assess credit values of the candidates through combining their direct credit opinions with the indirect credit opinions, and upload these credit values with digital signatures as new credit opinions to the pre-selected miners [12] (④ and ⑤ in Fig. 1). Similar to that in data sharing, the miners carry out the same consensus process. After the credit opinions are updated on the drone blockchain, all the drones and GBSs can reliably obtain block data including the new credit opinions of GBSs from the open access drone blockchain. Lastly, average credits of the GBSs are calculated by the system manager for next-round miner selection based on the latest credit opinions [14] (⑥ and ⑦ in Fig. 1).

Credit Assessment for Secure Miner Selections in PEGDONs

To evaluate the trust levels of miner candidates (i.e., GBSs), credit opinions from drones should be gathered and used to assess the final credit values of the candidates for secure miner selection. As such, we adopt a subjective logic model to evaluate the final credit values of the candidates according to interaction histories and indirect credit opinions. Compared to the existing credit assessment schemes, the subjective logic model can precisely evaluate the trust relationship among peers while preventing potential security risks of cooperative cheating and slandering done by malicious peers. The subjective logic model is a framework for probabilistic information fusion operated on subjective beliefs about the world, which is normally used to formulate an individual credit opinion. The "opinion" is the representation of a subjective belief that is used to model negative and positive statements and uncertainty in the subjective logic. For example, in drone networks, an objective-tracking drone applies for surrounding map service from a GBS during flight. The subjective belief of the drone in the GBS increases if the drone thinks that the map service is high-quality in the case with a stable communication link (i.e., a positive statement without uncertainty) and vice versa. In this article, each drone generates a credit opinion for a specific miner candidate by taking direct historical interactions and indirect credit opinions into consideration [5]. All the credit opinions are recorded and updated in the drone blockchain, where the permissioned blockchain works as a credit layer of PEGDONs to securely manage the decentralized credit opinions, as shown in Fig. 1.

Subjective Logic Model for Credit Assessment

A drone may communicate and interact with a GBS for communication or information services, such as remote sensing or map navigation in B5G drone networks. If the drone believes that the services provided by the GBS are useful and reliable, the drone will treat this as a positive interaction and generate a positive rating as its direct credit opinion for the GBS. In general, the rating of a drone to a GBS is formally expressed as a direct credit opinion vector with three elements: belief degree, distrust degree, and uncertainty degree. The sum of these elements is one. Without loss of generality, all the drones utilize the same evaluation criteria to generate their direct credit opinions.

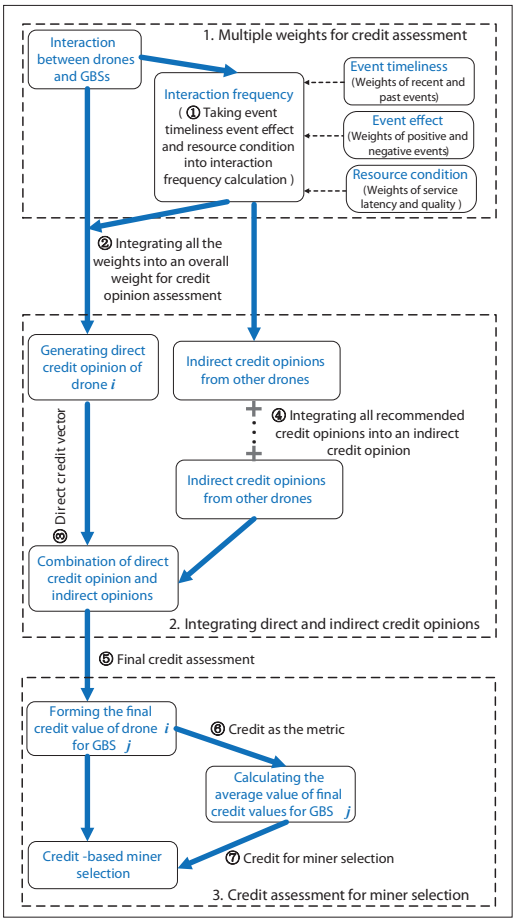

FIGURE 2. Four-weight subjective logic model for secure miner selection [13].

According to [5], the uncertainty degree depends on the successful transmission probability of data packets (i.e., the quality of a communication link between the drone and the GBS), which is affected by the wireless communication ability of the GBS. The belief degree depends on the positive interaction percentage of all the interactions in the condition of good communication quality. Similarly, the distrust degree is determined by the percentage of negative interaction, for example, the GBS intentionally ignores navigation service requests from the drone or drops packets of sharing records. According to the direct credit opinion vector, the credit value represents the drone's expected belief that the GBS is reliable and provides high-quality services during the communication and information service process or behaves honestly during the consensus process. The credit value is depended on both the belief degree and the uncertainty degree [5].

Four-Weight Subjective Logic Model for Credit Opinions

When taking different factors into consideration for the credit opinions, traditional subjective logic models can evolve toward multi-weight subjective logic models to obtain more accurate and reliable credit values. As shown in Fig. 2, without loss of

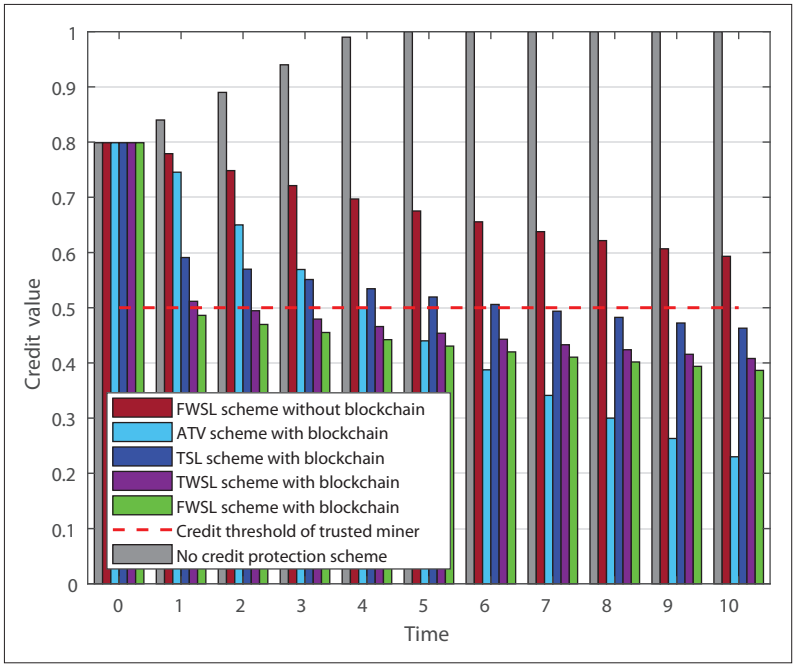

FIGURE 3. The credit of a malicious miner candidate.

generality, we consider four factors as weights to formulate the credit opinions [5]. For other B5G drone networks, we can also consider more specific weights, which can be straightforwardly extended to more sophisticated B5G drone networks.

Interaction Timeliness: GBSs are not always trustworthy and reliable because of the openness and decentralization of wireless networks. GBSs without adequate security protection are susceptible to attack. Thus, the trust level and direct credit of a drone to a GBS change over time. We use a timescale to identify the recent and past interactions (e.g., four days). The recent interactions have a higher weight on the drone's credit opinion of the GBS [5].

Interaction Effects: Negative interactions decrease the credit of GBSs and vice versa. Negative interactions have a lower weight than positive interactions on the drone's credit opinions.

Interaction Frequency: Note that a higher interaction frequency indicates that a drone has more prior knowledge about its interacting GBS. The interaction frequency between the drone and a GBS is defined as the ratio of the number of times that the drone interacts with the GBS to the average times that the drone interacts with other GBSs during a time window. The higher interaction frequency leads to a better direct credit opinion of the GBS [5, 13].

Resource Availability: A GBS with better resource availability (i.e., more available computation and storage resources) can provide higher-quality communication and information services. For miner selection, the better resource availability can decrease the delay of blockchain generation and mining. The interaction events with higher-quality services between the drone and the GBS indicate that the GBS has better resource availability. Therefore, these interaction events with higher-quality services have larger weight on the drone's direct credit opinions on the GBS [12].

Considering the weights of interaction timeliness, interaction effect, and resource availability, the interaction frequency is updated and calculated by the above weight factors and the average number of times that the drone interacts with other GBSs during a time window (① in Fig. 2). Thus, we utilize the updated interaction frequency to generate an overall weight for calculating the direct credit opinions and indirect credit opinions (② and ③ in Fig. 2).

Indirect Credit Opinions from Other Drones

For a drone, other drones' credit opinions act as indirect credit opinions (i.e., recommended credit opinions). The indirect credit opinions are combined into an integrated indirect credit opinion with recommended belief degree, distrust degree, and uncertainty degree. These degrees can be obtained through weighted arithmetic mean of all the belief degrees, distrust degrees, and uncertainty degrees from recommender drones [13], respectively. In other words, a combined credit opinion called the indirect credit opinion is generated by integrating the subjective opinions with different weights from different recommenders (④ in Fig. 2).

Combining Direct Credit Opinions with Indirect Credit Opinions

After obtaining the integrated indirect credit opinion, the drone still considers its own direct credit opinion to avoid cheating while calculating the final credit opinion (as shown in ⑤ of Fig. 2). The final credit opinion of the drone of the GBS is formed as a final credit opinion vector consisting of three elements, which is similar to that in the direct credit opinion. Therefore, the final credit value of the drone of the GBS depends on both the final belief degree and the final uncertainty degree. More details about the final credit value calculation can be found in [5]. This final credit value can be used as a metric to select high-quality miner candidates with high credit as the miners for permissioned blockchains (⑥ and ⑦ in Fig. 2). These high-credit miners will have good behavior and verify block data honestly to further improve their credit values for earning more mining rewards from the systems. Thus, the credit-based miner selection scheme can efficiently detect and remove unreliable and untrusted miner candidates, thus defending against block verification collusion attacks and ensuring secure block verification. Moreover, the credit is mainly affected by weight factors including attributes of interaction events and also the resource condition of the GBS. These factors are commonly available in most B5G drone networks. Therefore, the credit assessment scheme based on these weights is common and universal, and is easy to extend and apply in various B5G drone networks.

Security Analysis for Credit Assessment

Defending against Malicious Drones: With the help of the open access and tamper-resistant drone blockchain, it is easy to identify suspicious drones that continuously upload fake credit opinions (i.e., significantly higher or lower than the average value of indirect credit opinions from other drones) to the drone blockchain over a period of time. These suspicious drones will be

put into a blacklist to decrease the negative effect from malicious drones on the credit assessment. In the proposed subjective logic model, drones can set a low weight value for the recommended opinions from the suspicious drones during calculating the integrated indirect credit opinions. Moreover, similar to [12], we consider that the majority of drones are benign and reliable in the PEGDONs. Therefore, the low-weight credit opinions from a limited number of malicious drones have very limited influence on credit assessment.

Defending against Malicious GBSs: In drone blockchain, the consensus among miners (i.e., GBSs) can run properly even if a small number of malicious GBSs modify their received credit opinions. The reason is that all the credit opinions from drones are uploaded to the pre-selected miners with the drones' digital signatures. These digitally signed credit opinions ensure that no malicious miners can pose as drones to corrupt the drone blockchain through modifying or forging credit opinions received from the drones. Only the drone can generate a credit opinion signed with its own digital signature. Modified or forged credit opinions are more easily identified during block verification by other honest miners. Moreover, credit opinions on the drone blockchain are open access for both miners and drones. The drones can check and compare the credit opinions uploaded by themselves with those on the drone blockchain. The malicious miners will be identified and added to the blacklist, and thus be held accountable by the system [12].}

Numerical Results

In the simulation, we consider a remote sensing scenario with 100 drones flying in an urban area, and set 51 uniformly deployed GBSs as miner candidates. During credit assessment, there are 90 honest drones and 10 compromised drones with fake credit opinions. The interaction frequency between drones and GBSs ranges from 20 to 70 times each week. The probability of successful data packet transmission varies from 60 to 100 percent. Similar to [5], the weight parameters of positive, negative, recent, and past interactions, and good and bad resource availability in the Four-Weight Subjective Logic (FWSL) scheme are 0.6, 0.4, 0.6, 0.4, 0.6, and 0.4, respectively. The timescale of past and recent interactions is three days. More parameters for the simulation are adopted from [5].

Figure 3 shows credit variation of a randomly chosen compromised miner candidate under six cases:

- Without any subjective logic model scheme
- FWSL scheme with the drone blockchain
- FWSL scheme without the drone blockchain
- Three-weight subjective logic (TWSL) scheme in [5] with the drone blockchain
- Traditional subjective logic (TSL) scheme from [5] with the drone blockchain
- Aggregated trust value (ATV) scheme from [12] with the drone blockchain

In the ATV scheme, a credit value for an entity is obtained by aggregating trust value offsets with different weights from the drones. The trust value offset is calculated by the ratio of the difference between positive events and negative events to the total number of events [12, 13]. Each compromised miner candidate pretends to behave well in order to obtain positive credit values during a certain period of time. After that, the candidates randomly misbehave with 50 honest drones with probability of 80 percent.

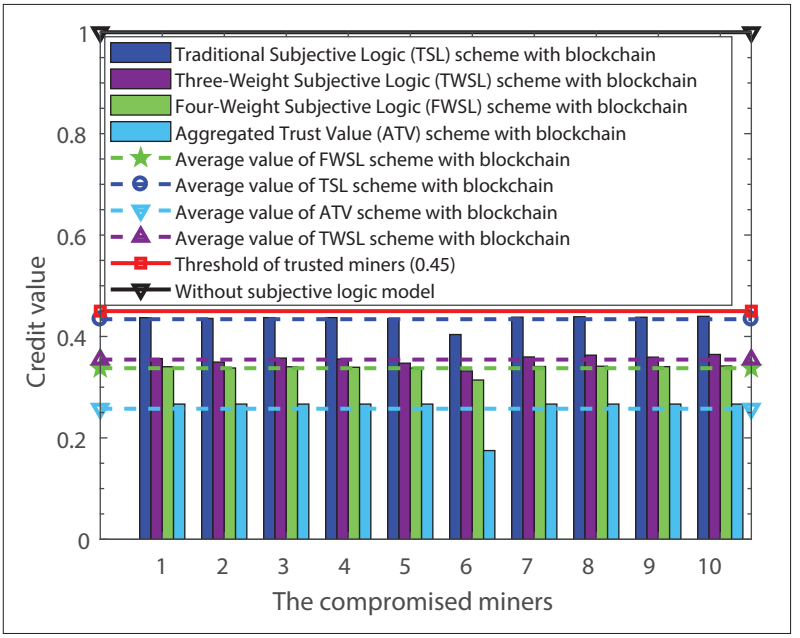

FIGURE 4. The credit of the malicious miner candidates.

For the scheme without subjective logic model, when a malicious candidate misbehaves, the credit of the candidate calculated by a drone linearly increases since the candidate's misbehavior for other drones cannot be directly detected by this drone. However, for the other four cases with the drone blockchain, the candidate's credit values quickly drop because of the consideration and incorporation of indirect credit opinions from other drones. The credit value decreasing below a credit threshold of trusted miners in the FWSL scheme is the fastest caused by the considered weight factors. Here, the credit threshold of a trusted miner means that the miner candidates with a credit value higher than the threshold are treated as trustworthy candidates. The credit in the ATV scheme declines faster than that of the FWSL scheme over time. This is because the ATV scheme is sensitive to the latest negative events but does not consider unintentional mistakes of good candidates with good behavior histories. This may cause false positive errors and partial credit assessment to decrease the participating willingness of the miner candidates [13]. The FWSL scheme is slightly better than the TWSL scheme due to considering one more weight (i.e., resource availability). Moreover, FWSL with the drone blockchain has higher accuracy and reliability than that without the drone blockchain. The reason is that the drone blockchain with the advantages of decentralization and tramper resistance, which can defend against miner collusion attacks. Therefore, the FWSL scheme with the drone blockchain ensures a more secure and fair miner selection through a more accurate credit assessment.

We observe 10 malicious miner candidates and observe their credit variations during 90

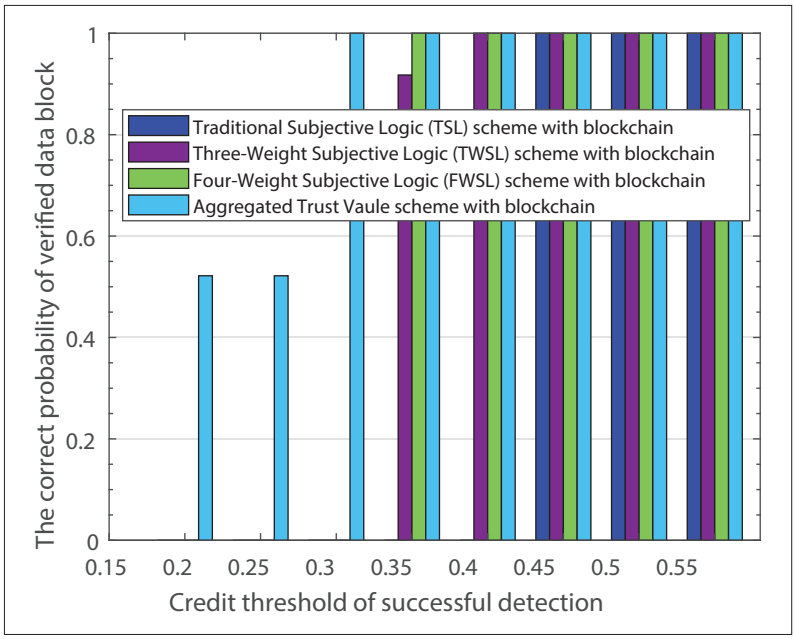

FIGURE 5. Correct probability of data block verification.

minutes, as shown in Fig. 4. For the cases with the drone blockchain, the average credit value of the malicious candidates in the TWSL, FWSL, and ATV schemes are 21.2, 25, and 38.9 percent lower than that in the TSL scheme, respectively. We also observe the probability of data block being correctly verified (i.e., correct probability) during 90 minutes. A metric named credit threshold of successful detection is defined as the credit of adverse miners below the threshold that can be successfully detected. Figure 5 shows the correct probability under different credit thresholds of successful detection. For all the schemes with the drone blockchain, a malicious miner can perform block verification collusion attacks and thus produce manipulated verification results in the cases of a relatively low credit threshold (e.g., below 0.2) [11]. The correct probability of the FWSL scheme with the drone blockchain can achieve 100 percent when the credit threshold is not lower than 0.35. The correct probability of the FWSL scheme is 9 percent larger than that of the TWSL scheme when the credit threshold of successful detection is 0.35. The collusion attacks cannot be discovered in the TSL scheme until the credit threshold is larger than 0.4 5. This indicates that FWSL with the drone blockchain can achieve secure block verification with a high correct probability through defending against block verification collusion attacks [13].

Conclusion and Future Studies

In this article, we have introduced permissioned blockchains for securing data sharing in B5G drone networks. We have outlined the challenges of applying permissioned blockchain in B5G drone networks and analyzed an intractable attack named block verification collusion attack. To defend against this attack, we have proposed a credit-based miner selection scheme developed based on the permissioned blockchain. A four-weight subjective logic model was used to calculate the credit of miner candidates. The numerical results show that the proposed secure miner selection scheme is effective to defend against the block verification attack.

The following interesting directions are worth further study.

Deployment Optimization for Ground Base Stations: For blockchain-based B5G drone networks, the ground base stations play a significant role (i.e., miner) in the blockchain systems. To further improve communication reliability and reduce communication delay between moving drones and miners, it is challenging to design optimal GBS deployment schemes in the scenarios with limited numbers of GBSs or heterogeneous B5G networks.

Machine Learning for Efficient Miner Selection: Inspired by the great potential of machine learning in solving complicated decision making problems of wireless networks, it is a promising direction to utilize machine-learning-based approaches, for example, deep reinforcement learning (DRL) [15], to design efficient and secure miner selection schemes. We can explore efficient and low-complexity DRL approaches for ground base station deployment in large-scale B5G drone networks with high-speed moving drones as well.

Acknowledgments

This research is supported by the National Research Foundation (NRF), Singapore, under Singapore Energy Market Authority (EMA), Energy Resilience, NRF2017EWT-EP003-041, Singapore NRF2015-NRF-ISF001-2277, Singapore NRF National Satellite of Excellence, Design Science and Technology for Secure Critical Infrastructure NSoE DeST-SCI2019-0007, A*STAR-NTU-SUTD Joint Research Grant on Artificial Intelligence for the Future of Manufacturing RGANS1906, Wallenberg AI, Autonomous Systems and Software Program and Nanyang Technological University (WASP/NTU) under grant M4082187 (4080), and NTU-WeBank JRI (NWJ-2020-004), and also the National Research Foundation of Korea (NRF) Grant funded by the Korean Government (MSIT) under Grant 2014R1A5A1011478, and National Nature Science Foundation of China (NSFC) under grant No. 61973087 and U1911401.

References

[1] M. Mozaffari *et al.*, "Beyond 5G With UAVs: Foundations of a 3D Wireless Cellular Network," *IEEE Trans. Wireless Commun.*, vol. 18, no. 1, 2018, pp. 357–72.
[2] S. Garg *et al.*, "UAV-Empowered Edge Computing Environment for Cyber-Threat Detection in Smart Vehicles," *IEEE Network*, vol. 32, no. 3, May/June 2018, pp. 42–51.
[3] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain Envisioned Uav Networks: Challenges, Solutions, and Comparisons," *Computer Commun.*, vol. 151, 2020, pp. 518–38.
[4] T. Dasu, Y. Kanza, and D. Srivastava, "Geofences in the Sky: Herding Drones With Blockchains and 5G," *Proc. 26th ACM SIGSPATIAL Int'l. Conf. Advances in Geographic Info. Systems*, 2018, pp. 73–76.
[5] J. Kang *et al.*, "Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory," *IEEE Trans. Vehic. Tech.*, vol. 68, Mar. 2019, pp. 2906–20.
[6] H. Chao *et al.*, "UAV Traffic Information Exchange Network," *2018 Aviation Technology, Integration, and Operations Conf.*, 2018, p. 3347; http://dx.doi.org/10.2514/6.2018-3347.
[7] X. Liang *et al.*, "Towards Data Assurance and Resilience in Iot Using Blockchain," *Proc. IEEE MILCOM 2017*, 2017, pp. 261–66.
[8] T. Alladi *et al.*, "Applications of Blockchain in Unmanned Aerial Vehicles: A Review," *Vehic. Commun.*, 2020, p. 100,249.

[9] W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, 2019, pp. 22,328–70.
[10] J. Qiu *et al.*, "Blockchain-Based Secure Spectrum Trading for Unmanned-Aerial-Vehicle-Assisted Cellular Networks: An Operator's Perspective," *IEEE Internet of Things J.*, vol. 7, no. 1, 2019, pp. 451–66.
[11] O. Dib *et al.*, "Consortium Blockchains: Overview, Applications and Challenges," *Int'l. J. Advances in Telecommun.*, vol. 11, no. 1, 2018, pp. 1–6.
[12] Z. Yang *et al.*, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," *IEEE Internet of Things J.*, vol. 6, Apr. 2019, pp. 1495–1505.
[13] J. Kang *et al.*, "Reliable Federated Learning for Mobile Networks," *IEEE Wireless Commun.*, 2020.
[14] Z. Lu *et al.*, "A Privacy-Preserving Trust Model Based on Blockchain for Vanets," *IEEE Access*, vol. 6, 2018, pp. 45,655–64.
[15] Z. Xiong *et al.*, "Deep Reinforcement Learning for Mobile 5g and Beyond: Fundamentals, Applications, and Challenges," *IEEE Vehic. Tech. Mag.*, vol. 14, June 2019, pp. 44–52.

Biographies

Jiawen Kang (kavinkang@ntu.edu.sg) received his M.S. degree from Guangdong University of Technology, China, in 2015, and his Ph.D. degree from the same school in 2018. He is currently a postdoctoral researcher at Nanyang Technological University, Singapore. His research interests mainly focus on blockchain, security, and privacy protection in wireless communications and networking.

Zehui Xiong [S' 17,M' 20] (zehui.xiong@ieee.org) is an assistant professor in the Pillar of Information Systems Technology and Design, Singapore University of Technology and Design. Prior to that, he was a researcher with Alibaba-NTU Joint Research Institute, Singapore. He received his Ph.D. degree from Nanyang Technological University, Singapore. He was a visiting scholar at Princeton University and the University of Waterloo. His research interests include wireless communications, network games and economics, blockchain, and edge intelligence. He has published more than 90 research papers in leading journals and flagship conferences, and 4 of them are ESI Highly Cited Papers. He has won five Best Paper Awards in international conferences and technical committees. He is now serving as an Editor or Guest Editor for many leading journals including IEEE Transactions. He is the recipient of the Chinese Government Award for Outstanding Students Abroad in 2019 and the NTU SCSE Best PhD Thesis Runner-Up Award in 2020.

Dusit Niyato [M'09, SM'15, F'17] (dniyato@ntu.edu.sg) is currently a professor in the School of Computer Science and Engineering, Nanyang Technological University. He received his B.Eng. from King Mongkut's Institute of Technology Ladkrabang, Thailand, in 1999 and his Ph.D. in electrical and computer engineering from the University of Manitoba, Canada, in 2008. His research interests are in the area of energy harvesting for wireless communication, the Internet of Things, and sensor networks.

Shengli Xie [M'01, SM'02, F'19] (shlxie@gdut.edu.cn) received his M.S. degree in mathematics from Central China Normal University, Wuhan, China, in 1992, and his Ph.D. degree in control theory and applications from South China University of Technology, Guangzhou, in 1997. He is currently a full professor and the head of the Institute of Intelligent Information Processing, Guangdong University of Technology, Guangzhou. He has authored or coauthored two books and over 150 scientific papers in journals and conference proceedings. His research interests include wireless networks, automatic control, and blind signal processing. He was a recipient of the Second Prize in China's State Natural Science Award in 2009 for his research on blind source separation and identification.

Dong In Kim [M'91, SM'02, F'19] (dikim@skku.ac.kr) received his Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1990. He was a tenured professor with the School of Engineering Science, Simon Fraser University, Burnaby, British Columbia, Canada. Since 2007, he has been an SKKU-Fellowship Professor with the College of Information and Communication Engineering, Sungkyunkwan University, Suwon, South Korea. He was a recipient of the 2019 IEEE Communications Society Joseph LoCicero Award for Exemplary Service to Publications. He was the first recipient of the NRF of Korea Engineering Research Center in Wireless Communications for RF Energy Harvesting in 2014. From 2001 to 2019, he served as an Editor and an Editor-at-Large of Wireless Communication I for the IEEE Trans. Communications. From 2002 to 2011, he also served as an Editor and a Founding Area Editor of Cross-Layer Design and Optimization for *IEEE Transactions on Wireless Communications*. From 2008 to 2011, he was the Co-Editor-in-Chief of the *IEEE/KICS Journal of Communications and Networks*. He served as the Founding Editor-in-Chief of *IEEE Wireless Communications Letters* from 2012 to 2015. He is an Executive Chair of IEEE ICC 2022, Seoul, Korea. He is a Fellow of the Korean Academy of Science and Technology and a member of the National Academy of Engineering of Korea.