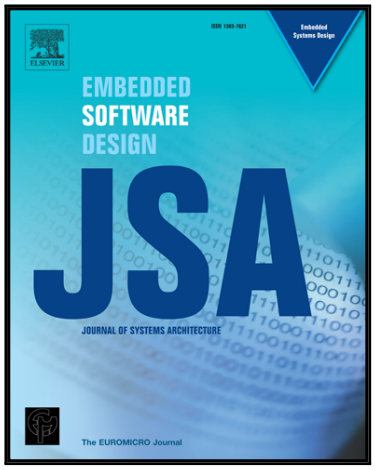
Journal Pre-proof



A Semi-autonomous Distributed Blockchain-based Framework for UAVs System

Chunpeng Ge, Xinshu Ma, Zhe Liu, Jinyue Xia

PII: S1383-7621(20)30022-9
DOI: https://doi.org/10.1016/j.sysarc.2020.101728
Reference: SYSARC 101728

To appear in: *Journal of Systems Architecture*

Received date: 10 September 2019
Revised date: 30 December 2019
Accepted date: 19 January 2020

Please cite this article as: Chunpeng Ge, Xinshu Ma, Zhe Liu, Jinyue Xia, A Semi-autonomous Distributed Blockchain-based Framework for UAVs System, *Journal of Systems Architecture* (2020), doi: https://doi.org/10.1016/j.sysarc.2020.101728

A Semi-autonomous Distributed Blockchain-based Framework for UAVs System

Chunpeng Ge, *Member, IEEE,* Xinshu Ma, Zhe Liu*, *Senior Member, IEEE,* and Jinyue Xia

***Abstract*—The impact of the Internet of Things (IoT) to our daily life has become bigger than ever, which can be witnessed from smart homes, smart transportation, and smart personal care. With widespread applications of UAVs in IoT contexts such as delivery and military, protecting communications between UAVs and ground control system is needed so as to resist potential vulnerabilities and optimize the coordination between distributed UAVs. In this work, to secure communications during data acquisition and transmission, as well as diminish the probability of attacking by malicious manipulated UAVs, we propose a distributed UAVs scheme harnessing blockchain technology whose network has similar topology to IoT along with cloud server. Instead of directly using the typical blockchain technique which requires expensive computation and high bandwidth overhead, we propose a novel, secure, and lightweight blockchain architecture which mitigates the computation and storage overhead while retaining its privacy and security benefits. Moreover, multiples types of transactions are defined to describe various data access and a novel reputation-based consensus protocol is designed to ensure the reliability of the decentralized network. Finally, performance evaluation demonstrates our blockchain-based distributed scheme is secure and efficient.**

***Index Terms*—Blockchain, UAV, Dos attack detection, IoT.**

I. Introduction

As a typical IoT scenario, the Unmanned Aerial Vehicles (UAVs) are becoming increasingly common as the rapid advancements of underlying technologies [1]. Owing to their low cost, low risk, light weight and easy to control, UAVs serve a broad range of applications from personal entertainment to critical missions. For example, as battery and fast charging technology develop, UAVs are able to monitor critical infrastructures [2], [3], such as power line detection [4]. Another application example is using UAVs to have a close monitor on the atmosphere from two to three kilometers above [5], which is difficult for satellites to track. The aggregated data including temperature, winds and turbulence, airspeed, etc., could help current weather forecasting models.

However, when using UAVs, akin to other smart devices of IoT, commands and data generally travel through an untrusted communication channel which may contain important security and privacy data, and therefore can be suffered from various cyber-attacks especially *Sybil attack*, *DoS/DDoS attack* and *GPS spoofing* which may lead to the destruction of data availability among the whole system. Therefore, device authorization and communication security would be a significant issue. Moreover, the system of UAVs, similar to many existing IoT systems, rely on a central server or cloud computing or fog computing to process and store data [6]. The problem is that once the server is attacked, the entire network will be disrupted which is also the inherent flaw of traditional centralized architecture, and cloud server could be manipulated to steal information or tamper data thus may compromise data integrity.

Besides, the trend of autonomy in the field of UAVs technology driven by the anticipated advancements in batteries, charging methods and embedded software concerning machine learning algorithms are becoming increasingly evident. As far as we know, the technique is being developed and tested while for now no authorized autonomous UAV systems are serviceable. Clearly, semi-autonomous UAVs indicate that a fleet of UAVs armed with advanced algorithms could deal with various human-defined missions and meet emerging challenges with a high level of coordination, merely requiring the interaction between UAVs and Ground Control Station (GCS). In fact, the concept of "a swarm of UAVs" has been existed in the field of military aircrafts for a long time and has penetrated into the civilian UAVs. Therefore, future UAVs demand a distributed security and privacy safeguard as well as a responsive and sustainable network system to build a trusted, integrated environment though it's extremely challenging to invent a satisfactory fully autonomous system which enables the UAVs to act like our human world.

Accordingly, the Blockchain (BC) technology is being considered as a powerful tool to be utilized in handling a large number of connected devices, enabling transaction processing and coordination between plentiful devices in the context of IoT, which is the rudimental technique of Bitcoin [7] along with other cryptocurrencies [8]. The reasons are threefold: (i) BC, de facto, is an immutable, replicated and tamper-evident log: data on BC cannot be deleted or modified, and anyone in the network can both read data from BC and verify its validity; (ii) the decentralized architecture of BC could prevent single-point failure [9], achieving a more resilient and stable ecosystem for IoT devices to run on; (iii) the underlying cryptographic algorithm employed by BC, including hash functions, symmetric encryption and digital signature, could protect the security and privacy of user data. So far, BC has been applied in numerous non-monetary scenarios [10], [11] for IoT protection, such as healthcare data [12], [13], government democracy and legal enforcement [14], smart home [15]–[17], smart toy with edge computation [18], and vehicle to infrastructure communication scheme [**?**], etc.

* Zhe Liu is the corresponding author.

Chunpeng Ge, Xinshu Ma and Zhe Liu are with College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics. E-mail: {gecp, xinshuma, zhe.liu}@nuaa.edu.cn.

Jinyue Xia is with the affiliation of IBM. E-mail: jinyue.xia@ibm.com.

Integrating blockchain with IoT is indirect and entails some key challenges including: (i) *high resource consumption* to solve PoW puzzles; (ii) *high delays* attributed to PoW and 6-confirmation rule aiming to hinder double spending attack which is extraordinarily significant for cryptocurrencies but not for IoT; (iii) *high memory overhead* to store the records of billions of transactions. Most research studying the combination of BC and UAVs only focuses on using BC technology as a decentralized database [11], [16], [19] where the full potential of BC technology was not fully explored.

With this in mind, in this paper, we propose a distributed, blockchain-based framework for UAVs system to address the aforementioned security and privacy problems as well as to achieve a high level of operational autonomy. The main contributions are summarized as follows:

- Due to the composition of small-memory, resource-constrained devices, we redesign the blockchain constitution to mitigate the pressure of storage and calculation imposed on each UAV, utilizing new transaction and block structure as well as lightweight cryptography technologies.
- A novel consensus protocol akin to Delegated Proof of Stake (DPoS) [20] combined with a reputation evaluation scheme is adopted to reach an agreement with the aggregated data between a fleet of trustless UAVs and allow for distributed decision making.
- We show that the presented blockchain-based decentralized framework for UAVs system is secure by analyzing its security with respect to the adversary model. We also implement experiments to verify the system self-defensive capability and ensure that the proposed architecture meets the general requirements of throughput for data communication between UAVs.

We organize the rest of paper as follows: Section II introduces background information related to UAVs networks and BC technology. Section III illustrates the system infrastructure needed for the proposed semi-autonomous BC-based UAVs framework which includes the structure of block and transaction. Section IV elaborates the working mechanism of our proposed UAVs framework. Section V gives the performance analysis including security analysis and efficiency evaluation. Ultimately, Section VI reviews the related works in the literature and Section VII concludes the paper.

II. Preliminary

This section introduces the background information of UAVs network and Blockchain technology.

A. UAVs Communication System and Threat Model

1) Typical UAVs Communication Scenario: As shown in Fig. 1, the typical UAV system consists of three component: an UAV or a fleet of UAVs, GCS and three kinds of communication data links including satellite link, UAV-UAV link and radio communication link [21]. Note that every kind of link carries different information: (i) satellite link transmits GPS and weather information between satellite and UAVs; (ii) UAV-UAV link transmits the interaction message between UAVs; (iii) radio communication link deliveries the commands sending from GCS, audio/video, and the other information between GCS and UAVs [22].

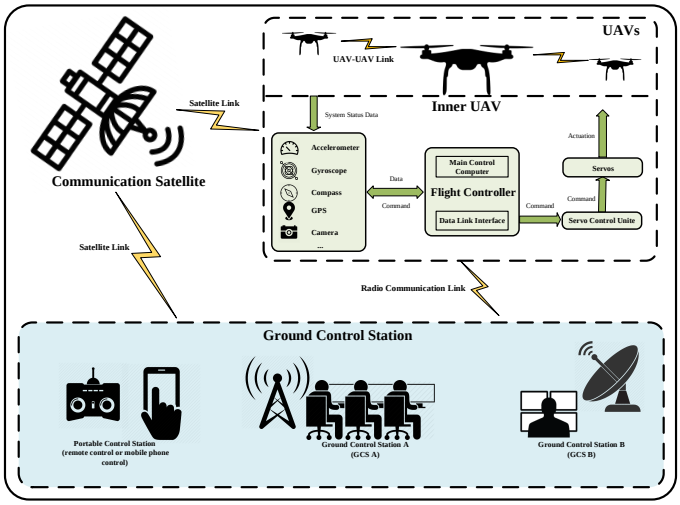


Fig. 1. High-level architecture of a typical UAV communication system.

Moreover, throughout the paper, we only concentrate on the building blocks that are related to our research and therefore consider the UAV that contains a flight controller, a cluster of sensors and a set of actuators. Here we briefly overview the inner operational mechanism of UAV. Basically, the UAV is controlled by the flight controller – the central processing unit, which reads and processes the data gathered by various sensors, and feed the servo control units with updated system status or relays this information to GCS depending on the type of control. Furthermore, commands from GCS are also managed by the flight controller and thus influence other acting actuators [23].

Numerous researches have demonstrated the practicability of using UAVs as an important tool for aerial photography, unmanned cargo transport, precision crop monitoring, building surveillance, tracking, aggregating dangerous conditions or supplying necessities for disaster services, etc [24]–[32]. To some degree the UAVs system is a representative application of an embedded system in the IoT scenario where a multi-scale technological ecosystem conglomerates several wireless access techniques and communication technologies — e.g., WiFi, Zigbee, 4G/5G cellular communications and Machine-to-Machine (M2M) communication — as well as subsidiary computational resources (such as cloud computing and edge computing platform). Nevertheless, current UAVs autopilot systems are vulnerable to various cyber-attacks, since cyber-security of the whole system was not a priority in the early-stage design process [33].

2) UAVs Threat Model: We briefly overview three malicious cyber attacks aiming to destroy the availability and security of the distributed UAVs autopilot system:

- **Sybil Attack.** It is an attack where an adversary creates

stolen or fabricated identities to serve as multiple distinct nodes in peer-to-peer (P2P) network. The adversary is capable of acquiring a disproportionate level of control and affecting the data integrity, resource utilization and overall network performance by various malicious behaviors such as packet dropping and packet selective forwarding [34].

- **DoS/DDoS Attack.** It aims to prevent some or all legitimate requests from being responded via sending superfluous requests to a target device in order to cause the machine or network resources unavailable [35]. It should be noted that either external machine or the individual device of the UAVs system might be manipulated to launch DoS/DDoS attack.
- **GPS Spoofing.** Basicly, military GPS signals are encrypted and hence cannot be tampered with viciously; whereas civilian GPS signals remain in no encryption and no authentication allowing the adversary to arbitrarily generate or falsify the original GPS signals [36]. Namely, the attacker is able to lead the UAV to a designated point deviating from the existing planned path, by using arbitrarily manipulated signals [37].

B. Blockchain Basics

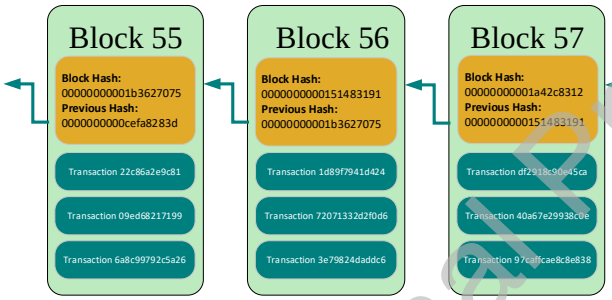


Fig. 2. An illustratioin of blockchain struction.

1) Blockchain Overview: Satoshi Nakamato [7] initiated the conception of blockchain in 2008 which has drawn much attention of developers and researchers during the last few years and generally been accepted as an emerging technology for distributed and decentralized data sharing [38]. Although blockchain was originally proposed for recording financial transactions where individual transactions will be encoded and stored by all users in the P2P network, the development tendency to blending blockchain technology and non-monetary scenarios is emerging. In general, blockchain technology demonstrates that a group of users are able to reach a consensus which could be recorded in a verifiable and secure mode without involving the third-party centralized controlling authority [39].

2) Blockchain Structure: From Fig. 2, we can see that the chain consists of a series of blocks connected by hash value of previous block. Each block includes a set of transactions recording the details of who sent how much money to whom, a reference to the preceding block, and the hash of current block which requires a target value (i.e., *nonce*) to a complex mathematical problem known as hash functions. Let us take Bitcoin as an example, the concept of "proof of work" was proposed to make block generation computationally "hard" based on conventional hash functions, thus preventing the adversaries from tampering blocks information in their favor. Only miners have the responsibility to create blocks and broadcast new-generated blocks back to the network. All the parties who received the new block should validate it as well as the transactions embedded in, and append it to blockchain once the new-generated block is valid.

III. System Architecture of the Distributed BC-based UAVs Framework

The system infrastructures of the distributed UAVs framework based on the blockchain technology is demonstrated in this section, and then we provide the reconfigured blockchain structure tailored for the UAVs communication systems.

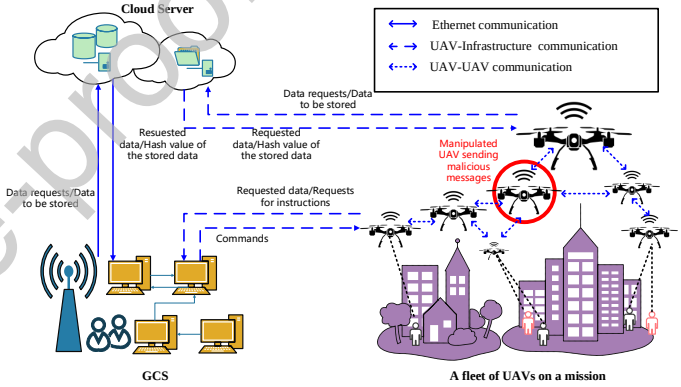


Fig. 3. Blockchain-based UAVs system model, composed of Ground Control Station (GCS), cloud server, and a fleet of UAVs serving on a mission (e.g., a swarm of police surveillance UAVs searching for missing people or fugitives).

A. System Overview

To detail the system model, we take a case of such scenario where a fleet of police surveillance UAVs are performing the task of searching for a fugitive in the sky over the city as shown in Fig. 3. This is based on the assumption that ordinarily each person walking outside in a controlled area could be observed by several surveillance UAVs and the UAVs are capable of recognizing the target person with the assistance of identification including face recognition.

A GCS is a land-based or sea-based mission control center that facilitates the management of UAVs and the processing of aggregated information [40], mainly in charge of the mission planning and payload data (the data collected via various of sensors) analysis. Besides, the function of cloud server is threefold: (1) *Storage Service:* Each UAVs status data, location information, mission details and data streams including sensor data and images/videos could be stored in the cloud. (2) *Computational Resources:* Diverse computation incentive tasks could be performed by the cloud since various excellent

computational tools are deployed. (3) *Internet Service:* This allows UAVs to acquire Internet services such as getting no-fly zone information. Note that, to protect data integrity, cloud server is required to send back the hash value of the data need storing to the requester (either GCS or UAVs) on the hypothesis that we have a semi-honest cloud server but a trusted GCS [41].

B. Reconstructed Blockchain Constitution

Considering the UAVs network is composed of lightweight and low-energy IoT devices, it is irrational to require these devices to possess equal computational power to the miners in Bitcoin network, which makes the task of supporting distributed storage and security quite challenging. Thus, in our proposed framework, a reconstructed blockchain architecture is illustrated to reduce the pressure of storage and calculation.

1) Block Detail: As shown in Fig. 4, the structure of the reformatory block, akin to Bitcoin, could be divided into two parts: block header and block body. Nevertheless, in difference from conventional block composition, our proposed block is tailored for the lightweight IoT devices as well as the communications between UAVs, via utilizing lightweight cryptography technologies Keccak [42], [43] (i.e. a low-cost alternative to the standard version which is selected as the winner of SHA-3 by NIST [44]) for example and redefining the functions of all transactions.

The block header, detailed in Table I, is composed of the current block header's hash, preceding block header's hash, root of the reputation tree, policy list, a timestamp, and root of the transaction tree. Here, unlike Bitcoin where the miners are required to find the solution to a hash puzzle so as to win the right of appending a block to the main chain, our solution relies on a voting mechanism combining with reputation evaluation scheme which is akin to the fundamental idea of *Delegated Proof of Stake* (DPoS) [20], to nominate a node to generate a new block. Thus, the item of reputation tree is added into the block and the root of tree is recorded by block header. In addition, the policy list is generated by the GCS administrator when adding new UAVs to the system during the initialization process and added into the first block. To update it, the administrator only need to modify the policy list in the latest block, and therefore each node in the network should refer to the latest policy to handle the transactions.

Accordingly, block body contains a reputation tree and a transactions tree. The reputation value of each UAV will be recalculated once the UAV acts in suspicious ways, such as querying privacy data against the access policy listed in block header, and creating or relaying the invalid blocks or transactions. And the details of reputation evaluation scheme are elaborated in Section IV-B. It should be noted that a cryptographically authenticated data structure—modified Merkle Patricia Trie (MPT) applied in Ethereum [45] is adopted to store the reputation value of each UAV as depicted in Fig.5, which could quickly and efficiently identify data that has changed without having to retrieve over all the data in order to make the comparison.

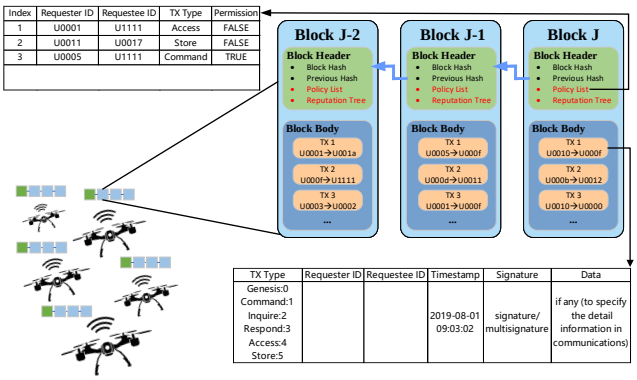


Fig. 4. Overview of the proposed UAVs blockchain architecture: the structure of transactions (see Section III-B2) and policy lists (see Section III-B1).

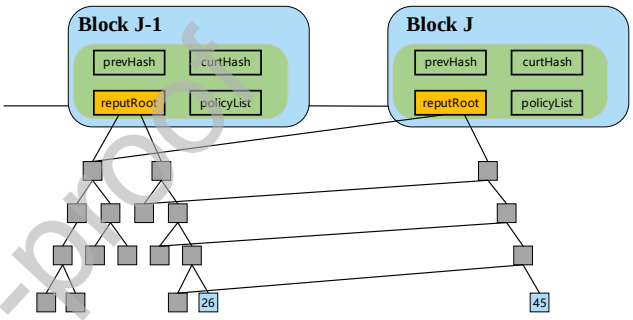


Fig. 5. Example of the modified Merkle Patricia Trie structure for recording the reputation values. Two blocks B_{J-1} and B_J containing two reputation trees, it is shown that the reputation value 26 was changed to 45 in the latter block B_J. Specifically, only the modified data would be stored in the new block and the unmodified data would be linked to the new root without duplication, efficiently reducing the request of memory compared to the original Merkle Tree that is adopted in Bitcoin [7].

2) Transaction Detail: As for defining transactions, inspired from [16], communications between GCS, UAVs and cloud server among the whole system are formatted as transactions. Owning to the constrained storage space in UAVs, a micro-size transaction structure is suggested as shown in TABLE II. The detail of a transaction contains the transaction type's IDs of the requester and requestee (similar to the addresses in the blockchain), the signature of the requester (i.e., sender) and the additional data if necessary. Note that we use shorter IDs to identify UAVs instead of the addresses as in blockchain, and the length of additional data is variable ranging from 0 to 1024 bits.

3) Transaction Handling: Here, we focus on how transactions are handled in semi-autonomous UAVs system based on the general topology of distributed BC-based architecture aforementioned as shown in Fig. 3.

Genesis We use *genesis* to define the process of adding new devices to the UAVs system before starting the mission, which should be created by the administrators of GCS after authentication, while an unique ID being assigned to each UAV and a pair of public key and private key of each new UAV are

TABLE I
COMPOSITION OF A BLOCK

Contents	Size(bit)	Description
BLOCK_HASH	80	Hash value of current block header
PREV_HASH	80	Hash value of previous block header
TIMESTAMP	24	Unix timestamp of the block
POLICY_LIST	$30 \times N$	Access rules of a fleet of N UAVs
REPUTATION_ROOT	80	Root of the reputation tree
TRANSACTION_ROOT	80	Root of the transaction tree

TABLE II
COMPOSITION OF A TRANSACTION

Contents	Size(bit)	Description
TX_TYPE	4	Transaction type
REQUESTER_ID	8	Device ID of the sender
REQUESTEE_ID	8	Device ID of the receiver
SIGNATURE	1024/2048	Signature/multi-signature
DATA	Maximum 1024	Additional information

distributed in order to allow it to sign transactions. Besides, in terms of the reputation value, each UAV would be initialized with $r = 70$ which indicates the credibility and the value of r changes according to the malicious actions the UAV has performed (cf. Section IV-B).

Command The *command* transaction could only be initiated by GCS for requiring data including status data and image data from UAV or sending control command to UAV devices. Namely, the status data could be airborne GPS information, flight status data (such as flight altitude, speed, acceleration, etc.), and the sensor data on UAVs; the image data represents the images and videos captured through the camera; and the concrete control order includes mission start, reboot, land, loiter unlimited, etc. It should be noted that *command* transaction is applied to the scenario where a swarm of UAVs are not far from GCS. Basically, GCS sends this transaction with the item DATA denoting the specific control order or the type of data collected first. After receiving *command* transactions, UAVs are required to execute the instruction after a time window (whose duration is denoted by w_g). Otherwise, GCS could disqualify the suspicious UAV via artificially capturing it, modifying the policy list to ban the communications with it, or setting the reputation value r much lower to notify other UAVs in the network.

Inquiry Based on the defined policy, UAVs might need data from other UAV devices for some purposes. As an example, some UAVs when adjusting the heading automatically sometimes need the information regarding the flight course of other UAVs to perform route planning more accurately. It should be noted that this type of transaction only could be started by UAVs. Due to the unstable connections between the UAVs swarm, in our strategy, the requester might have to resend the transaction less than RET_{max} within a time window w_u. Once receiving no response in the premise of legitimate $inquiry$ within w_u, the requester would initiate a *report* transaction broadcasting the suspicious activity of the certain UAV.

Respond If the *inquiry* violates the access policy list, the requestee should create a *report* transaction reporting the malicious information and broadcast it to penalize the suspicious UAV to some extent (cf. *Report* in this section). Instead, once the policy is satisfied, the requestee would respond with probability $\mathcal{P}$ deriving from the reputation value r according to eq. 1. The receiver would use generalized Diffie-Hellman shared key and share the response with the requester. The response is embedded in a *respond* transaction back to the requester with the shared key.

Access We use *access* transaction to describe the interactions between UAVs/GCS and cloud server. All the UAVs receiving the transactions should check the validity referring to the latest policy list and relay the valid transactions. When the transaction is illegal, it should be discarded and a *report* ought to be broadcast to penalize the requester of the *access* transaction.

Store The cloud server is responsible for providing storage service for UAVs and GCS. When receiving the *store* request, cloud server verifies the transaction on the premise of there existing available space in the cloud storage. Then, it proceeds to calculate the hash value of received data and compare it with received hash value. The data packets will be saved in the cloud once two hash values match. Next, the respective address is encrypted with a shared key generated by Diffle-Hellman algorithm, and sent back to the requester immediately.

Report We propose *report* transaction to enhance the abilities of self-supervision and semi-autonomy among the whole system. Each UAV and GCS have the right to report any malicious activity performed by any part which is regarded as the compromised device. Thus once the validity of *report* is confirmed, the suspicious device will be punished by decreasing the reputation value r (cf. Section IV-B).

Vote This transaction is designed for the distributed decision

making to ensure guaranteed convergence towards a common conclusion, especially in the cases of disagreement such as election of the committee to mine the blocks and accepting the *report* transaction or not. Taking the election process for example, it requests one node (usually the leader UAV) to initiate a *vote* transaction and all of the nodes respond via *respond* transaction including the ID of the candidates as well as its signature. After receiving the messages the receiver calculates the outcomes of voting and announce the new committee to the whole network. Note that the detailed information of election could be found in Section IV-C.b

Alert In order to defend the potential cyber attacks, each UAV and GCS could create a *alert* transaction to sound a warning once it finds itself under a certain kind of attack, which could greatly improve the self-defensive capabilities of the whole system and cut loss in the early stage of the attack. All UAVs in the network would perform corresponding actions towards different attacks.

4) Periodically Memory Release: With the continuous operation of UAVs system, there is no doubt that the blockchain distributed ledger would become increasingly larger. For instance, suppose that the size of the block header is 100 Bytes; the block body is 2000 bytes; and the generation rate of the blocks is 1 block every 2 minutes. Therefore, after 4 hours the size of the ledger would be $(2000+100)\times 60\times 8 \div 2 = 252$ KB. Considering the restricted memory space of UAVs, freeing up the UAV memory at a frequency of every 2 hours is sufficient for recycling the memory space. Namely, the distributed ledger of blockchain in the proposed framework needs to be backed up to cloud server and the physical memory of the UAV devices is released periodically.

IV. Working Mechanism of the Semi-autonomous BC-based UAVs Framework

In our framework, all communications information are eventually saved in a distributed ledger, which exits in each UAVs and GCS, in the form of connective blocks. Thus, to protect the data security, it is significant to guarantee the data accuracy in different procedures: message transmission, message verification through voting mechanism and mining process. In this section, we elaborate the working mechanism of our framework in detail including data process, reputation evaluation scheme, and the consensus algorithm.

A. Data Processing

1) Registration: Every device (i.e., UAV) has to register to join the network via *genesis* transaction (Section III-B3). Ahead of registration, each device creates a private key on the basis of its MAC address ∂_m, latest timestamp τ_C, and random salt hash value $hbar$. Moreover, each node will be preloaded a policy that indicates the actions to communications.

2) Data Hashing and Signing: Note that the basic information stored in each node is composed of the public keys of all nodes, its own private key and the consecutive blocks. All devices need to execute cryptography algorithms like hash function and digital signature before sending messages. It is worth noting that Keccak [46], [47], a high-performance hash function in both code size and cycle count [43], [48] compared to other lightweight hash functions (such as Quark [49], PHOTON [50], and SPONGENT [51]), is adopted to generate a *message digest*. To reduce memory usage, the 160-bit output is truncated to 80-bit which saves a mount of space due to the heavy use of hash functions, e.g., block hash, previous hash, reputation root, transaction root, and the *message digest* of each transaction.

3) Data Verification: When a node receives a transaction in the peer to peer network, it verifies: (i) data integrity and consistency via checking if two *digests* match with each other; (ii) the validity of the transaction via checking the request whether satisfy the policy list. The transaction is relayed to the neighbors if validation passes, otherwise, the received transaction is considered as false and not transmitted if it lacks data integrity while the *report* transaction is generated by the receiver to inform other UAVs in the network and the reputation value of the certain UAV decreased if the received transaction against policy list. Analogously, the receiver who report the malicious action successfully is rewarded with an increase of the reputation value.

In our protocol, it should be noted that each issue of *report* transaction would induce a voting process based on an *ID-based distributed voting mechanism* (cf. IV-B2), namely, each node would vote on its verification result as well as the reputation value of the suspicious UAV.

B. Reputation Evaluation Scheme

1) Evaluating Reputation Value: We use distributed reputation evaluation scheme to ensure the received blocks to be valid and decrease the overhead of block verification compared to the conventional blockchain community. In the proposed framework, the reputation value r of all the nodes are stored in block header in the form of Merkle Patricia Trie [52]. All UAVs are managed in groups, and each group consists of a head UAV and general UAVs. The system maintains a trust rating for each node based on activities it has performed harnessing the reputation evaluation.

Generally, each UAV is initialized with a fixed reputation value 70 which could be decreased for performing malicious actions or increased for successfully report a suspicious UAV. More importantly, each UAV in the network choose to accept a request or relaying the transactions with probability $\mathcal{P}$ educed from the reputation value r according to the following equations:

$$\mathcal{P}_i = \begin{cases} 1 & \mathrm{r} \geq 100 \\ \frac{\rho_1 \cdot r}{\sum_{j=1}^{N} r_j \cdot C_i} & \mathrm{r} \geq 60 \\ \frac{\rho_2 \cdot r}{\sum_{j=1}^{N} r_j \cdot C_i} & \mathrm{r} < 60 \end{cases} \tag{1}$$

where $\mathcal{P}_i$ represents the probability to accept the request of UAV U_i; r_i represents the reputation value of U_i; C_i denotes the number of suspicious actions the U_i has performed; ρ_1 and ρ_2 are the coefficient applied to the UAVs with $r \geq 60$ and $r < 60$ respectively. Therefore, a high reputation value

favors of getting its messages accepted and trusted and vise versa. Besides, it should be noted that, once the reputation value of the requester is lower than 30, the neighbor UAVs will refuse to relay almost all of the transactions initiated by it. Thus the probability of malicious or manipulated UAVs attacking the whole system via sending plenty of spam messages or malicious messages would be lessened. Note that, in our scheme, we adopt the method of reputation computation method in [53], [54]. In [53], a node leverages the quality of service to compute the reputation of a connected node. However, in our scheme, we introduce coefficients ρ_1 and ρ_1 to weight the importance of connections.

2) ID-based distributed voting mechanism: The functions of the proposed *ID-based distributed voting mechanism* is threefold: (1) *Election of Miners Committee*: as mentioned before, a distributed consensus protocol akin to DPoS is proposed to reach an agreement with the collected data. Therefore, we utilize the voting mechanism to elect the committee in which the block is generated in turn; (2) *Handling Report Transactions*: as we all know, *report* transaction is created to inform against the malicious UAVs acting suspiciously. However, the compromised UAV might harm the availability of the whole system via fabricating *report* transaction to frame the compliant UAVs thus other UAVs losing trust on it. Hence, the validity of each *report* transaction should be evaluated by the voting mechanism. (3) *Handling Other Disagreements*: to provide the ability of distributed decision making and semi-autonomy, we utilize the voting process to deal with various situations with divergence. For example, when one UAV finds itself in/close to the no-fly zone suddenly with no expectation, it has the reason to suspect of being attacked by *GPS spoofing* and generates a *vote* transaction immediately to compare its GPS with other nodes. Once they don't match with each other, it is highly possible that the UAV is under the attack of *GPS spoofing* and the UAV should initiate a alert transaction to inform the neighbors to mitigate risks by taking preventive measures.

To detail the voting mechanism, considering a network consisting of N UAVs, each UAV node votes on the contingency of its verification results and its own decision. The number of votes are denoted by K where $K \leq N$, and the voting is accepted only the following condition is met:

$$\frac{K}{N} \geq \epsilon, \tag{2}$$

where ϵ denotes the threshold whose value ought to be greater than 50% to guarantee the accepted result is in consensus with the majority of nodes among the whole system. Consequently, the verified data comes into effect of which the miner of the committee operating on the basis.

C. Consensus Protocol

The consensus algorithm, designed to attain trust and reliability in the network involving multiple devices, is important in distributed and multi-agent systems like UAVs system. The working mechanism, which is automatically executed by each node, is illustrated in this section, including the rules of committee selection block generation.

1) Committee Selection: To relieve the burden of the resource constrained processor of the UAVs, it is sensible to abandon the Proof of Work algorithm which needs to solve a complex mathematical challenge and we adopt the core idea of DPoS requiring to elect the committee where the block should be generated in turn. Considering the actual situation of UAVs system, we propose the following two schemes to select miners.

Strategy 1: GCS as the Miner, this strategy is suitable for the environment where the distance between GCS and UAVs is close allowing for the good quality of the communications among the whole system. Based on the premise that GCS is trusted, it is rational to assign GCS to act as the miner responsible for collecting all the transactions, verifying the validity of each transaction, and managing the changes of reputation values in the block header, which mitigates the computation load of the UAVs in the network.

Strategy 2: Voted Nodes as Miners, in contrast, this strategy is appropriate for the scenario where the UAVs swarm need to autonomously coordinate with each other on a mission without uninterrupted connections to GCS. Intuitively, at the embryonic period of the system, a pre-designated committee should be organized by the administrator of GCS based on the role assignment of UAVs, and the number of members of committee depends on the total number of UAVs. Formally, the re-election of the committee is triggered by any omitting of block generation or forks in the blockchain ledger. In that case, the members of committee are selected by their reputation value r and, namely, only top 15% of the nodes could become the candidates. A *vote* transaction will be created by the leader UAV after which each node could vote for $3/5$ of the candidates and the final committee will consist of the top $3/5$ of candidates. The result of the vote will be broadcast on the whole network.

2) Block Generation: If the rate of block generation is slow, the size of block will be quite large due to the accumulative transactions over time, which could cause the communication delay or slow down the transmission rate among the network. Otherwise, extremely frequent mining could become the computation burden for the each node in the blockchain system. Consequently, the suitable block generation rate is significant for the proposed framework and we propose the method of generating blocks by fixed time.

In detail, each block is created at a fixed time slot which requires the mining task to be rotated at the same frequency. The next new round of mining process starts instantly after the generation of the previous block. It is adjustable that the stipulating of the time period between two rounds of block generation owing to the diverse communication requirements of different tasks. For an N-UAVs network, let α denote the time interval of mining process, β denote the average size of the generated block, t_0 represent the time period that periodically releases the memory (cf. Section III-B4), and Δ represent the average allocated size of storage space in UAVs.

We have the following constraint:

$$\beta \cdot floor(\frac{t_0}{\alpha}) < \Delta, \tag{3}$$

where $floor(\cdot)$ represents rounding down to the nearest integer. Clearly, Eq. 3 ensures that all collected data in the blockchain could be well stored in each devices before next round of memory release.

V. Performance Analysis of the Semi-autonomous Distributed BC-based UAVs Framework

A. Security Analysis and Potential Disadvantages

1) Protection against Sybil Attack: In our proposed framework, we keep malicious requests aways from the devices to increase the availability by restricting the access rights of each participants in the network by policy list, to those entities contains some critical information of the system. Before forwarding them on to the neighbors, transactions received from the other UAVs are authorized by each devices, which could also mitigate the pressure of message transforming.

2) DoS/DDoS Mitigation: In our system, the reputation evaluation scheme allows to reduce the probability of being undermined by DoS/DDoS attack due to that the junk information won't be relayed by the network nodes when the reputation value of sender is less than a threshold value. Moreover, GCS could supervise the packet flows among the UAVs therefore GCS could reset the policy list to ban all the access permissions to decrease the effect of manipulated UAV.

3) GPS Spoofing Resistance: Our system could resist GPS spoofing to some extent due to the *vote* transaction could gathering other UAVs GPS. Basically, it is quite impossible for the attackers to compromise all of the UAVs simultaneously. Namely, once a UAV finds it is in or close to a none-fly zone, it will send a *vote* transaction to claim the GPS information itself. This would call a *vote* function allowing each participant to send a *True/False* message back to the requester. Thus the requester could check if it has the valid GPS information.

4) Security of the consensus protocol: Since the proposed UAV systems is built on top of the blockchain system, the security of the underlying blockchain consensus protocol is critical for the proposed blockchain-based UAV system. In [55], Natoli et al. conducted a summary of the security of consensus protocols in different attack model including the mining power attack, the strategic mining attack, the communication attack, the hybrid of strategic mining and communication attack, and the stake attack. Our scheme consensus is based on the reputation, and can resistant to the mining power attack and the strategic mining attack. However, our scheme cannot resistant to the communication attack, the hybrid of strategic mining and communication attack, and the stake attack.

B. Efficiency Evaluation

We evaluate our distributed BC-based architecture utilizing UB-ANC Emulator [56], an emulator for multi-agent UAVs networks based on the technique of ns-3, and the detailed experiment configuration is shown in TABLE III. To compare the overheads of our proposed architecture, we simulated another scenario where the transactions are processed without the techniques of digital signature, hashing, and blockchain technology which is referred to as the base scheme. It is worth mentioning that, due to the constraints of the simulator, the average delay of the communication is omitted in our experiment. The simulation experiments results can be see from Fig.6-8.

TABLE III
Simulation environment

Operating Platform	64-bit Ubuntu 16.04
CPU	3.1 GHz Intel Core i5
Network Simulation Tool	ns-3.27
Ground Control Station Tool	QGroundControl

Intuitively, our solution would increase computational and communication overhead on the original UAVs networks due to the additional encryption and hashing operations, while improves the security and privacy of the drone system. As shown in Fig. 6, time overhead of different kinds of transactions is depicted, where *Store*, *Inquiry* are the most time-consuming part. It is evident that most transactions in the proposed scheme cost more or equal time compared to base scheme. Particularly, since UAVs in our framework could choose more creditable object to aggregate information which saves a mass of time waiting for valuable responses, *Inquiry* transaction consumes less time in our solution.

Fig. 7 shows the fluctuation of the malicious node's reputation value over the time. Note that, in the base scheme without the reputation evaluation scheme, the reputation value of the malicious node could be regarded as linearly increasing by the time since the other compliant nodes cannot detect any vicious activity. However, in our solution, the reputation value of the compromised node decreases below the threshold value (r=60) rapidly because of the proposed reputation-based system. From the figure, we can see that a malicious node's reputation grows down with the time. When the reputation of the malicious node is lower than a threshold, this node will be not trusted by other nodes. Thus, the security of the distributed independent decision of the UAVs swarm could be guaranteed.

TABLE IV
Evaluation of the Packet Flow

Packet Flow	Base (Bytes)	Ours (Bytes)
From UAV to GCS	20	35
From UAV to UAV	15	25
From GCS to Cloud	60	62
From UAV to Cloud	20	35

As shown in Fig. 8, the average throughput of the proposed BC-based framework increases as the number of UAVs among the entire network increases. Finally, TABLE IV illustrates the simulation outcomes in terms of the average packet overhead. Utilizing the Cryptography technology including digital sig-

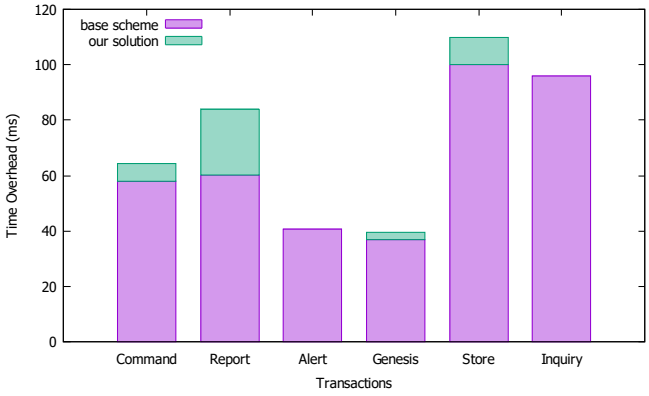


Fig. 6. Evaluation of time overhead.

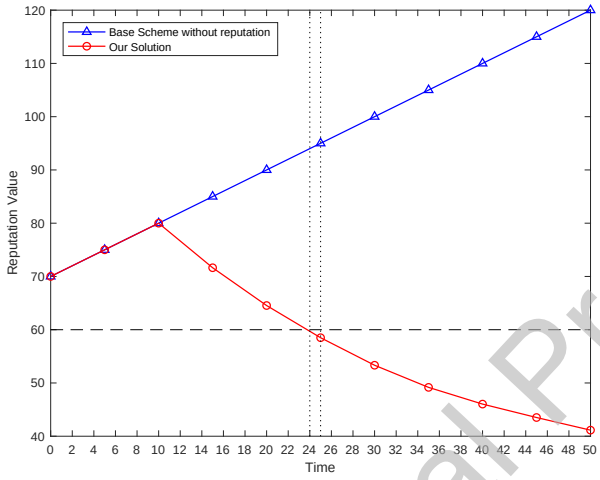


Fig. 7. The reputation value of a malicious node.

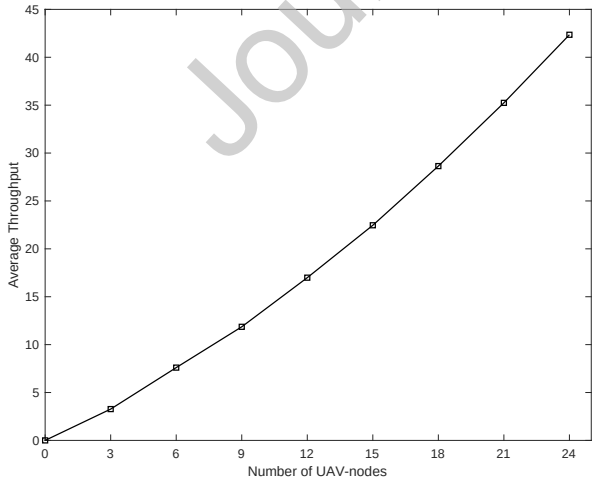


Fig. 8. Average throughput of our solution.

nature, encryption and hash functions increases the size of the transmitted payload.

VI. Related Work

A. IoT security

While the number of smart devices significantly increases in IoT, it is important to secure the devices in the network because the devices are vulnerable to cyber attacks such as buffer-over-flow attack [57]–[59]. If the device is comprised, it may cause data breach and expose the server to the attacks as well. To solve this problem, researchers utilize PUFs and the technique of hardware security primitives. However, such an approach requires a high computation capacity from the devices. Moreover, the work didn't address the data integration problem. A recent study [60], [61] describes some off-the-shelf IoT devices didn't carefully consider the security requirements, so they could lead to massive cyber attacks.

Many efforts related to the security analysis of UAV communication networks are being conducted for enhancing secrecy performance. Rudinskas [62] analyzed the radio communication system of the SMONIT project, discussing radio-related problems, malicious threats and possible solutions for data transformation between various entities. This study concentrated on cryptography techniques while overlooking the resource restraint of UAVs. Moreover, the work by [21] and [63] presented the clear and comprehensive security threat model of UAVs system with possible mitigation techniques to help researchers and users to understand the threat profile of the system. As UAVs system is designed to based on GPS position system, many UAV-related research focused on resisting GPS spoofing and jamming attacks. [64] performed a concrete analysis of various GPS spoofing and jamming attacks and proposed a taxonomy of cyberattacks for UAV as well as the research trend in the future. [65] studied the anatomy, design, and impact of GPS spoofing attack, proposed a novel GPS spoofing detection and mitigation technique, and simulated using the most promising test platform. Javaid et al [65] pointed out that the lack of encryption of GPS information was the culprit of spoofing.

Regarding the network layer security, Randu et al [66] proposed a multi-path routing protocol (named MP-OLSR) for FANET network to aggregate dynamic data with high mobility specifically in emergency situations. Although the scheme performs well in the simulation platform, the scenario with malicious nodes in the network is not discussed. Furthermore, Hooper et al designed a multi-layer security framework for WiFi-based UAVs system [67] and illustrated how the proposed scheme mitigate three adversarial attacks: Buffer-Overflow attack, DoS attack and ARP cache poison attack. On the other hand, Zhang et al discussed the problem of eavesdropping in both the UAV-to-ground (U2G) and ground-to-UAV (G2U) communications and observed that the legitimate link can be established much more stronger than the eavesdropping link by adjusting the location of UAV [68]. Motivated by this, the authors designed joint trajectory and

optimizing transmit power solution to improve physical layer security.

B. Blockchain for IoT Security

Blockchain has brought attentions into numerous researchers due to its immutable and distributed ledger. However, many challenges [69] involving with IoT devices came out for Blockchain industry. For example, the consensus protocols in Blockchain is a major problem which could potentially lead a delay for proof of work consensus. Recently, an optimized lightweight blockchain structure has been proposed for smart home by mixing the private and public ledgers in local networks [15]–[17] . Unfortunately, the integrity is not guaranteed. Yang et al studied smart toy with edge computation [18], and vehicle to infrastructure communication scheme [70].

As blockchain can bring many benefits to multiple IoT scenarios, many researches has been conducted to explore the success of integrating blockchain technique with UAVs system in various aspects. Li et al proposed a mutual-healing group key distribution scheme with a private blockchain to guarantee the distribution and storage of group keys as well as manage the dynamic list of network membership [70]. Scarlato et al discussed the difficulty in rescuing a crashed UAV in case of accidents and designed a permissioned side chain with Proof-of-Authority consensus recording GPS coordinates and height flight for the collision avoidance and recovery of the crashed UAVs [71]. Zhu et al considered trading and storage management issues in air-to-ground IoT network, and to optimize the resource consumption and enable trading process, the authors proposed a novel consensus algorithm utilizing Nash equilibrium [72]. Kuzmin and Znak proposed a new structure for autonomously operating UAVs network based on blockchain with a novel Proof-of-Graph consensus algorithm while overlooking the constrained computational resources of UAVs [73]. Youssef et al designed a distributed payment system between an UAV cloud and a sensor cloud where the blockchain is adopted as a distributed and public ledger to secure the data integrity, traceability and unforgeablity [74]. Rana et al focused on improving the data security when there are sending and receiving information between UAVs and cloud, where GPS information is required to be added in the block [75]. Alsam and Shin designed a blockchain-based data acquisition scheme for UAVs swarm where a memory-efficient data structure – π-hash bloom filter is utilized to validate user's authentication and filter malicious devices efficiently [76].

VII. Conclusion

UAV has a capability to sense and deliver in a wide range of locations, so it could offer the benefits to IoT applications. In this work, we present a BC-based IoT architecture that mitigates most security and privacy threats of the UAV system. The architecture considers the limitations of IoT devices and enables UAV-based applications to receive sensor data which is controlled in a trusted and autonomous way. In our proposed system, we make sure the real-time data collection meets the requirement of integrity, confidentiality, as well as availability. Lastly, we developed a prototype for our proposed UAV system and conducted an experiment that demonstrates a relative good performance from our prototype.

Acknowledgment

This work was supported by the supported by the Fundamental Research Funds for the Central Universities, NO.YAH18040.

We would like to thank the anonymous reviewers for very insightful comments to an earlier version of this paper.

References

[1] Z. Liu, Z. Li, B. Liu, X. Fu, I. Raptis, and K. Ren, "Rise of mini-drones: Applications and issues," in *Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing*. ACM, 2015, pp. 7–12.

[2] Y. Ham, K. K. Han, J. J. Lin, and M. Golparvar-Fard, "Visual monitoring of civil infrastructure systems via camera-equipped unmanned aerial vehicles (uavs): a review of related works," *Visualization in Engineering*, vol. 4, no. 1, p. 1, 2016.

[3] S. Sankarasrinivasan, E. Balasubramanian, K. Karthik, U. Chandrasekar, and R. Gupta, "Health monitoring of civil structures with integrated uav and image processing system," *Procedia Computer Science*, vol. 54, pp. 508–515, 2015.

[4] C. Deng, S. Wang, Z. Huang, Z. Tan, and J. Liu, "Unmanned aerial vehicles for power line inspection: A cooperative way in platforms and communications," *J. Commun*, vol. 9, no. 9, pp. 687–692, 2014.

[5] W. Khawaja, O. Ozdemir, and I. Guvenc, "Uav air-to-ground channel characterization for mmwave systems," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2017, pp. 1–5.

[6] M. Chiang and T. Zhang, "Fog and iot: An overview of research opportunities," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 854–864, 2016.

[7] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[8] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*. IEEE, 2015, pp. 104–121.

[9] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[10] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.

[11] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for internet of things security: a position paper," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018.

[12] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of internet of things infrastructure for secure and smart healthcare," *arXiv preprint arXiv:1805.11011*, 2018.

[13] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. IEEE, 2017, pp. 772–777.

[14] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," *Available at SSRN 2580664*, 2015.

[15] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: challenges and solutions," *arXiv preprint arXiv:1608.05187*, 2016.

[16] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, 2017, pp. 618–623.

[17] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *Proceedings of the second international conference on Internet-of-Things design and implementation*. ACM, 2017, pp. 173–178.

[18] J. Yang, Z. Lu, and J. Wu, "Smart-toy-edge-computing-oriented data exchange based on blockchain," *Journal of Systems Architecture*, vol. 87, pp. 36–48, 2018.

[19] H.-K. Moon, W. Lee, S. Kim, J. Park, J. Lee, and I. Joe, "An adaptive security approach according to the reliability level of drones using blockchain," in *International Conference on Mobile and Wireless Technology*. Springer, 2018, pp. 51–57.

[20] "Dpos description on bitshares." [Online]. Available: http://docs.bitshares.org/bitshares/dpos.html

[21] A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam, "Cyber security threat analysis and modeling of an unmanned aerial vehicle system," in *2012 IEEE Conference on Technologies for Homeland Security (HST)*. IEEE, 2012, pp. 585–590.

[22] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on uavs for wireless networks: Applications, challenges, and open problems," *IEEE Communications Surveys & Tutorials*, 2019.

[23] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, p. 7, 2017.

[24] D. R. Jacques, "Unmanned aerial vehicles: modeling considerations for wide area search munition effectiveness analysis," in *Proceedings of the 34th conference on Winter simulation: exploring new frontiers*. Winter Simulation Conference, 2002, pp. 878–886.

[25] K. D. Mullens, E. B. Pacis, S. B. Stancliff, A. B. Burmeister, and T. A. Denewiler, "An automated uav mission system," SPACE AND NAVAL WARFARE SYSTEMS COMMANDSAN DIEGO CA, Tech. Rep., 2003.

[26] L. Merino, F. Caballero, J. R. Martínez-de Dios, J. Ferruz, and A. Ollero, "A cooperative perception system for multiple uavs: Application to automatic detection of forest fires," *Journal of Field Robotics*, vol. 23, no. 3-4, pp. 165–184, 2006.

[27] J. L. Drury, L. Riek, and N. Rackliffe, "A decomposition of uav-related situation awareness," in *Proceedings of the 1st ACM SIGCHI/SIGART conference on Human-robot interaction*. ACM, 2006, pp. 88–94.

[28] J. Cooper and M. A. Goodrich, "Towards combining uav and sensor operator roles in uav-enabled visual search," in *Proceedings of the 3rd ACM/IEEE international conference on Human robot interaction*. ACM, 2008, pp. 351–358.

[29] R. R. Pitre, X. R. Li, and D. DelBalzo, "A new performance metric for search and track missions 2: Design and application to uav search," in *2009 12th International Conference on Information Fusion*. IEEE, 2009, pp. 1108–1114.

[30] I. Maza, K. Kondak, M. Bernard, and A. Ollero, "Multi-uav cooperation and control for load transportation and deployment," in *Selected papers from the 2nd International Symposium on UAVs, Reno, Nevada, USA June 8–10, 2009*. Springer, 2009, pp. 417–449.

[31] E. A. Marconato, M. Rodrigues, R. d. M. Pires, D. F. Pigatto, C. Q. Luiz Filho, A. R. Pinto, and K. R. Branco, "Avens-a novel flying ad hoc network simulator with automatic code generation for unmanned aircraft system," 2017.

[32] A. B. Colturato, A. B. Gomes, D. F. Pigatto, D. B. Colturato, A. S. R. Pinto, L. H. C. Branco, E. L. Furtado, and K. R. L. J. C. Branco, "Pattern recognition in thermal images of plants pine using artificial neural networks," in *International Conference on Engineering Applications of Neural Networks*. Springer, 2013, pp. 406–413.

[33] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, "Cyber attack vulnerabilities analysis for unmanned aerial vehicles," in *Infotech@ Aerospace 2012*, 2012, p. 2438.

[34] A. Rajan, J. Jithish, and S. Sankaran, "Sybil attack in iot: Modelling and defenses," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2017, pp. 2323–2327.

[35] J. Chen, Z. Feng, J.-Y. Wen, B. Liu, and L. Sha, "A container-based dos attack-resilient control framework for real-time uav systems," in *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2019, pp. 1222–1227.

[36] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing," *University of Texas at Austin (July 18, 2012)*, pp. 1–16, 2012.

[37] S.-H. Seo, B.-H. Lee, S.-H. Im, and G.-I. Jee, "Effect of spoofing on unmanned aerial vehicle using counterfeited gps signal," *Journal of Positioning, Navigation, and Timing*, vol. 4, no. 2, pp. 57–65, 2015.

[38] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[39] E. C. Ferrer, "The blockchain: a new framework for robotic swarm systems," in *Proceedings of the Future Technologies Conference*. Springer, 2018, pp. 1037–1058.

[40] G. Natarajan, "Ground control stations for unmanned air vehicles," *Defence Science Journal*, vol. 51, no. 3, pp. 229–237, 2001.

[41] B. Qureshi, A. Koubaa, M.-F. Sriti, Y. Javed, and M. Alajlan, "Poster: Dronemap-a cloud-based architecture for the internet-of-drones." in *EWSN*, 2016, pp. 255–256.

[42] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Keccak," in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2013, pp. 313–314.

[43] J. Balasch, B. Ege, T. Eisenbarth, B. Gérard, Z. Gong, T. Güneysu, S. Heyse, S. Kerckhof, F. Koeune, T. Plos *et al.*, "Compact implementation and performance evaluation of hash functions in attiny devices," in *International Conference on Smart Card Research and Advanced Applications*. Springer, 2012, pp. 158–172.

[44] P. Hernandz, "Nist releases sha-3 cryptographic hash standard," *Dostopno na: https://www. nist. gov/news-events/news/2015/08/nistreleases-sha-3-cryptographic-hash-standard*, 2015.

[45] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[46] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Keccak specifications," *Submission to nist (round 2)*, pp. 320–337, 2009.

[47] ——, "Keccak sponge function family main document," *Submission to NIST (Round 2)*, vol. 3, no. 30, 2009.

[48] T. Meuser, L. Schmidt, and A. Wiesmaier, "Comparing lightweight hash functions–photon & quark."

[49] J.-P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia, "Quark: A lightweight hash," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2010, pp. 1–15.

[50] J. Guo, T. Peyrin, and A. Poschmann, "The photon family of lightweight hash functions," in *Annual Cryptology Conference*. Springer, 2011, pp. 222–239.

[51] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varıcı, and I. Verbauwhede, "Spongent: A lightweight hash function," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2011, pp. 312–325.

[52] D. Vujičić, D. Jagodić, and S. Randić, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*. IEEE, 2018, pp. 1–6.

[53] B. Yu, J. Liu, S. Nepal, J. Yu, and P. Rimba, "Proof-of-qos: Qos based blockchain consensus protocol," *Computers & Security*, p. 101580, 2019.

[54] J. Yu, D. Kozhaya, J. Decouchant, and P. Verissimo, "Repucoin: Your reputation is your power," *IEEE Transactions on Computers*, 2019.

[55] C. Natoli, J. Yu, V. Gramoli, and P. Esteves-Verissimo, "Deconstructing blockchains: A comprehensive survey on consensus, membership and structure," *arXiv preprint arXiv:1908.08316*, 2019.

[56] J. Modares, N. Mastronarde, and K. Dantu, "Ub-anc emulator: An emulation framework for multi-agent drone networks," in *2016 IEEE International Conference on Simulation, Modeling, and Programming for Autonomous Robots (SIMPAR)*. IEEE, 2016, pp. 252–258.

[57] A. Kanuparthi, R. Karri, and S. Addepalli, "Hardware and embedded security in the context of internet of things," in *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*. ACM, 2013, pp. 61–64.

[58] J. Zhou, X. S. Hu, Y. Ma, J. Sun, T. Wei, and S. Hu, "Improving availability of multicore real-time systems suffering both permanent and transient faults," *IEEE Transactions on Computers*, vol. 68, no. 12, pp. 1785–1801, 2019.

[59] J. Zhou, J. Sun, X. Zhou, T. Wei, M. Chen, S. Hu, and X. S. Hu, "Resource management for improving soft-error and lifetime reliability of real-time mpsocs," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2018.

[60] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena, and M. S. Obaidat, "A learning automata based solution for preventing distributed denial of service in internet of things," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. IEEE, 2011, pp. 114–122.

[61] K. Cao, J. Zhou, T. Wei, M. Chen, S. Hu, and K. Li, "A survey of optimization techniques for thermal-aware 3d processors," *Journal of Systems Architecture*, 2019.

[62] D. Rudinskas, Z. Goraj, and J. Stankūnas, "Security analysis of uav radio communication system," *Aviation*, vol. 13, no. 4, pp. 116–121, 2009.

[63] V. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defences," in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2016, pp. 164–170.

[64] C. L. Krishna and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*. IEEE, 2017, pp. 194–199.

[65] A. Y. Javaid, F. Jahan, and W. Sun, "Analysis of global positioning system-based attacks and a novel global positioning system spoofing detection/mitigation algorithm for unmanned aerial vehicle simulation," *Simulation*, vol. 93, no. 5, pp. 427–441, 2017.

[66] D. Radu, A. Cretu, B. Parrein, J. Yi, C. Avram, and A. Aştilean, "Flying ad hoc network for emergency applications connected to a fog system," in *International conference on emerging internetworking, data & web technologies*. Springer, 2018, pp. 675–686.

[67] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson, and W. Alexis, "Securing commercial wifi-based uavs from common security attacks," in *MILCOM 2016-2016 IEEE Military Communications Conference*. IEEE, 2016, pp. 1213–1218.

[68] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing uav communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1376–1389, 2019.

[69] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*. IEEE Press, 2017, pp. 458–467.

[70] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11 309–11 322, 2019.

[71] M. Scarlato, C. Perra, M. Y. Jabarulla, G. Jung, and H. N. Lee, "A blockchain for the collision avoidance and the recovery of crashed uavs," *Korean Institute of Electronics Engineers Conference, pages=463–467, year=2019*.

[72] Y. Zhu, G. Zheng, and K.-k. Wong, "Blockchain empowered decentralized storage in air-to-ground industrial networks," *IEEE Transactions on Industrial Informatics*, 2019.

[73] A. Kuzmin and E. Znak, "Blockchain-base structures for a secure and operate network of semi-autonomous unmanned aerial vehicles," in *2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*. IEEE, 2018, pp. 32–37.

[74] S. B. H. Youssef, S. Rekhis, and N. Boudriga, "A blockchain based secure iot solution for the dam surveillance," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2019, pp. 1–6.

[75] T. Rana, A. Shankar, M. K. Sultan, R. Patan, and B. Balusamy, "An intelligent approach for uav and drone privacy security using blockchain methodology," in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 2019, pp. 162–167.

[76] A. Islam and S. Y. Shin, "Bus: A blockchain-enabled data acquisition scheme with the assistance of uav swarm in internet of things," *IEEE Access*, vol. 7, pp. 103 231–103 249, 2019.

Chunpeng Ge received the Ph.D degree in Computer Science from Nanjing University of Aeronautics and Astronautics in 2016. He is now a research fellow of University of Wollongong, Australia. Prior to that, he was a research fellow of Singapore University of Technology and Design, Singapore. His current research interests include cryptography, information security and privacy preserving for blockchain. His recent work has focused on the topics of public key encryption with keyword search, proxy re-encryption, identity-based encryption, and techniques for resistance to CCA attacks.

Xinshu Ma received her B.S. degrees in Computer Science from Nanjing University of Aeronautics and Astronautics. His current research interests include cryptography, information security and privacy preserving for blockchain. His recent work has focused on the topics of reliable systems, blockchain for IoT and IoT security systems.

Zhe Liu is a full professor in college of computer science and technology, Nanjing University of Aeronautics and Astronautics (NUAA), and also a research associate in SnT, University of Luxembourg, Luxembourg. He received his Ph.D degree Laboratory of Algorithms, Cryptology and Security (LACS), University of Luxembourg, Luxembourg. His Ph.D. thesis has received the prestigious FNR Awards 2016 - Outstanding PhD Thesis Award for his contributions in cryptographic engineering on IoT devices. His research interests include computer arithmetic and information security. He has co-authored more than 70 research peer-reviewed journal and conference papers.

Jinyue Xia received the Ph.D degree in Computer Science from University of North Carolina at Charlotte, USA in 2017. His current research interests include data security, cryptography and information security. His recent work has focused on the topics of public key encryption with proxy re-encryption and identity-based encryption.

Dear Editor,

We would like to submit the enclosed manuscript entitled "A Semi-autonomous Distributed Blockchain-based Framework for UAVs System", which we wish to be considered for publication in Journal of Systems Architecture.

In this work, we proposed a distributed scheme by utilizing the blockchain technology where the network has similar topology to IoT along with the cloud server. Instead of harnessing the typical blockchain that requires expensive computation and high bandwidth overhead, we propose a new secure, private and lightweight blockchain architecture that eliminates the overhead of blockchain while maintaining most of its security and privacy benefits.

I hereby declare that the authors have no conflicts of interest to this work. I declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

Sincerely yours!
Zhe Liu