Leveraging Blockchain for Secure Drone to Everything Communications

Gagangeet Singh Aujla*, *Senior Member, IEEE,* Sahil Vashisht†, *Member, IEEE,*
Sahil Garg‡, *Member, IEEE,* Neeraj Kumar§¶, *Senior Member, IEEE*, Georges Kaddoum¶, *Member, IEEE*
*Department of Computer Science, Durham University, Durham, United Kingdom
† Dept. of Computer Science & Engineering, Shree Guru Gobind Singh Tricentenary University, India
‡¶École de Technologie Supérieure, Université du Québec, Montréal, Canada
§Computer Science & Engineering Department, Thapar Institute of Engineering and Technology, India
¶School of Computer Science, University of Petroleum and Energy Studies, Dehradun, Uttarakhand., India
(E-mail: gagi_aujla82@yahoo.com, sahilvashist90@gmail.com, sahil.garg@ieee.org,
neeraj.kumar@thapar.edu, georges.kaddoum@etsmtl.ca)

Abstract

The popularity of drones has increased its deployment in a wide range of applications like commercial delivery, industrial systems, monitoring, surveillance, and surveys. The facility of fast deployment and cost-effectiveness make drones a potential choice for an aerial base station to serve User Equipment (UEs) in a defined area. Drones are equipped with night-vision cameras, advanced sensors and GPS receivers which make them capable to capture the data and either analyze it to discover new patterns or transmit it to the remote cloud for storage and processing. Even more, the drones data relaying system helps to extend the service coverage area to provide reliable communication connection to the isolated UEs. However, the deployment of drones at remote location rely only on GPS and these systems are prone to various attacks and can lead to signal blockage. The data integrity and privacy are some of the important issues which must be addressed before the deployment of drones in commercial sectors. Therefore, in this paper, we propose a blockchain-based security approach for drone-to-everything communications wherein the location of drones is tracked based on the segment division of area under deployment. Moreover, we design a miner node selection algorithm which uses computational resources, battery status and time of flight of a drone as parameters to select the miner node. The security evaluation of the proposed framework clearly shows its viability of blockchain in drone deployments across remote sites.

Index Terms

Permissioned Blockchain, Data Integrity, Drones-to-Everything, Internet of Drones, Miner Node, Privacy Preservation, Security.

1 Introduction

Nowadays, the deployment of unmanned aerial vehicles (UAVs) or drones as the aerial base stations (ABS) and wireless relays (WRs) has gained a significant consideration due to the inherent characteristics like agility and mobility. The quick and efficient deployment of drones can enhance the uplink and downlink communication for ground user equipment (UE) and provide support to the overloaded cellular networks. They can also be utilized as the flying WRs, to boost the wireless coverage in a certain region temporarily. The key requirement for the robust service provisioning relies on the Line of Sight (LoS) communication link establishment by these drones with ground UEs. The mobility and altitude adjustment by the drones help to establish a reliable connection with the ground users with a minimum transmit power. Additionally, it helps to overcome the traditional challenges such as–signal blockage and shadowing. In this way, drones can provide energy-efficient and cost-effective wireless data relaying and communication to serve the numerous ground users with a minimum investment of terrestrial infrastructure. Even. the next-generation networks like 5G also utilize drones as movable ABS to reduce the infrastructure costs [1]. With the increasing popularity of drones, they are expected to play an essential role in providing *connectivity* and *emergency* services in the smart cities.

Drones can handle diverse consumer applications such as as-personal WiFi hot-spot, delivery services (goods and healthcare products), and follow-me-UAV (to provide light to pedestrian). Drones can connect and communicate with different devices, machines, sensors, vehicles and many more, thereby forming a drone to everything (D2X) communication environment. The drone can act as enablers for providing fast and reliable data relaying services for the Internet of Things (IoT) environment in the smart cities. Moreover, drones play the role of ABS to collect data from the sensors and then forward it to the destination processing nodes like cloud, or edge. Although the drones provide manifold benefits, the emergence of autonomous drones can also pose many security implications and challenges related to public safety. Drones are capable to carry explosives, chemical weapons and atomic bombs and an attacker can

control the drones to target important infrastructures (oil and gas pipeline and atomic plants) and public establishments (public events, and residential societies). Even more, drones are also prone to the various cyber attack, signal blockage, GPS spoofing and data theft and many more security issues.

1.1 Attack vectors for D2X Communications

Generally, drones rely on the WiFi for data transmission and the transfer of the control messages. Due to the weight limitations and computational power constraints, the use of on-board encryption mechanism is not prevalent in the drones. Exploiting the varying distance between the drones, an attacker tries to inject the false information in D2X environment using various prevalent attacks like GPS spoofing, false information injection or man-in-middle attacks. Even more, the attackers try to limit the availability or exhaust the resources using Denial of Service (DoS) attacks [2]. Fig. 1 shows different attack vectors for drone communications.

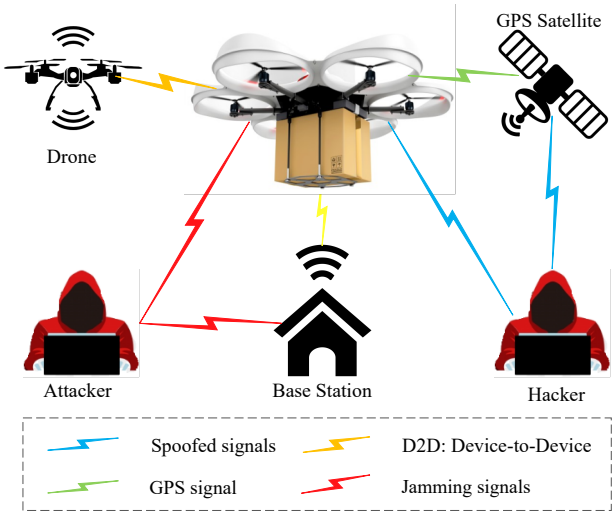

Fig. 1: Attack vectors in drone communications.

Some of the prevalent attack vectors in D2X environment are listed as below.

GPS Spoofing: In general, a drone receives the GPS signals from the satellite to obtain coordinates for its movement and notification of the presence of other drones in its vicinity. The several on-demand drone-assisted services like product delivery and Internet provisioning require the location coordinates of the drones. Thus, by spoofing the GPS signals, an attacker can change the position and direction of drones as per its desired choice. In 2011, the Iranian hackers spoofed the GPS signal of a US drone and grounded it by providing false coordinates [2].

WiFi de-authentication attack: WiFi is the major platform for data transfer and communications in D2X environment. An attacker can disable the WiFi module on the drones to hinder the communication. Although the WiFi is protected using either wired equivalent privacy (WEP) or Wi-Fi protected access (WAP), these protections can be compromised by the air-cracking technique. In this technique, an attacker generates unauthenticated frames to disrupt the communication systems. In such a case, the drones are not provided with the updated information and directions from the ground base stations (GBS) and thereby misleading the drone's flight to perform any suspicious activity [3].

False data injection attack: An effected drone can broadcast false information (leakage in the gas pipeline, false traffic update, and environmental conditions) to its GBS and the neighbouring drones. Such attacks are performed using automatic dependent surveillance-broadcast (ADS-B) component which is installed on a drone to avoid collisions by updating the position information from time to time [4].

DoS attacks: The major goal of these attacks is to exhaust the resources or limit the availability of the services to disturb the performance of a network. Such attacks are performed by either jamming the channel or flooding the messages to the drones over the network.

1.2 Motivation: A Pathway to Blockchain for Security

All these attacks related to D2X communications raise the concerns to the design of secure and dependable D2X communication environment. Being an integration of heterogeneous networks, the security challenges are not restricted to the inherent issues brought by sensor networks, mobile and cellular communications, and the Internet, but it also involves issues related to the privacy protection and data integrity. Hence, the drones have to prepare themselves to embed advanced security concepts like authentication, authorization, information integrity, confidentiality, and access control, apart from cyber-attack protection and prevention mechanisms. In D2X communications, as any device can communicate with the drones, then prior precautions are essential as the damages can be drastic at later stages.

Drones are being deployed for the product delivery in residential and commercial locations and therefore carry sensitive or confidential consumer data (address, contact number, payment mode, and many more). Often, an attacker can compromise security loopholes and access the identity of such consumers and then use the same for false intention's. Moreover, the use of cryptographic primitives is essential as the data in the D2X communication system travels over an insecure channel. Furthermore, the drone data is generally stored in plain text which can be easily accessed by an intruder. Therefore, it is essential to embed some cryptographic mechanisms to protect the data related to drone communications. However, deploying the heavy cryptographic primitives in drones is a tough challenge due to computational and power limitations. Even more, in collaborative drone application, the group of drones communicate and coordinate to collect and share vital information. In such a scenario, it is quite challenging to maintain the integrity of the data being shared. Here, the role of central coordinating authority remains vital, but if this central coordinator is compromised, then the entire systems may collapse or can be misused.

After analysis of the aforementioned challenges, it is pertinent to say that *blockchain* can be a possible solution for providing secure and autonomous functionality in D2X communications. Blockchain allows the peer-to-peer (P2P) decentralized communication wherein any changes in data can be easily tracked [5], [6]. Moreover, it prevents inauthentic drones or users to participate in the network. In

drones, the transactional data (data related to the movement of drones like, 'who deploy where' and transaction recorded by networks agents) can be stored in 'blocks. Such blocks consist of the definite number of transactions which are interlinked to each other to build a blockchain. Moreover, with the help of the cryptographic primitives and hash functions in blockchain, the group of network agents can sign an agreement on a defined state of affairs and every node in the network follows it without the need of any controlling authority [7]. Also, the record keeping and sharing of blocks among drones in vicinity help to avoid collision and cater to the need for path selection in a dynamic environment.

2 Blockchain and Drones: The Current State-of-the-art

Recently, blockchain has been very popular technology to provide security solutions in the diverse environments. Although the state-of-the-art is still limited but certainly, some solutions exist which take along the amalgamation of blockchain and drones as illustrated in Table 1. The current state-of-the-art and there limitations are described below.

BUS: A Blockchain-Enabled Data Acquisition Scheme [8] utilizes the blockchain-based technology to provide security for data acquisition from IoT devices using UAVs. In *BUS*, the UAVs shares the shared key with the IoT devices to initiate the communication process. Using the shared key, IoT devices encrypt the information at their end before transmitting it to the UAVs. Additionally, the UAVs uses π-hash bloom filter and digital signature algorithm along with encryption to secure UAV-to-server data forwarding. After approval from the validator's, the data can be stored in the blockchain. However, this scheme is applicable for only data acquisition from IoT devices and do not consider drone-to-drone (D2D) communications.

Lightweight permissioned blockchain system [9] has been deployed over named data networking for UAV ad-hoc network to develop a scalable and adaptive delegate-based consensus algorithm. The proposed system helps to mitigate the content poisoning, when it is integrated with the interest-key-content binding, and forwarding strategy. In this mechanism, the content is classified into static and dynamic contents. Moreover, to detect internal attackers, a feedback phase is included in the proposed mechanism, wherein blockchain maintains a secure ledger in a distributed manner. Although this work proposed a new adaptive consensus algorithm but its applicability in diverse D2X scenarios is not clearly validated and is limited for named data networking. Moreover, it deploys a permissioned blockchain architecture where only trusted parties are involved unlike the public blockchain architecture.

In [10], the authors utilizes the principles of the blockchain to secure the UAVs network. In proposed technique, likewise the blockchain, the UAVs has blocks of information of other operating UAVs in vicinity. If a hijacked UAV tries to alter the blockchain by injecting false information, this information would be discarded by other UAVs as per the P2P principle of blockchain. To validate the approach *ABS-SecurityUAV* agent based simulator is utilize for achieving efficient simulations. However, this work also considers a permissioned blockchain architecture where it all the validators or miners are assumed to be trusted nodes.

Proof-of-Graph (POG) consensus mechanism [11] has been designed to overcome the number of limitations in existing consensus mechanisms to secure the blockchain-based UAV systems. In the proposed approach, the UAVs acts as the node for blockchain network which can read and write transactions. Even, the stochastic blocks are created for the partitioning of the network in equal groups. Further, these groups work as blockchain participants. This approach used a dynamic partitioning schme for selecting validators based on role swapping but it do not consider the computational and energy resources (both being most essential for drones) while selecting drones as validators.

In [12], a short survey has been presented to understand the security in the swarm of UAVs which is one of the six frameworks developed under Hyperledger project. This framework helps to design a permissioned and private architecture for the UAVs network. Moreover, the capability of this framework includes, efficient processing, modular design, identity management, chain code functionality, privacy and confidentiality in a UAV network. This work is a generic review of different blockchain architectures and hyperledger model but it do not explicitly say which model fits best in D2X scenario.

Aviation Easements Rights and Ownership (AERO) Network [13] is expected to provide a peer-to-blockchain temporary agreement between drone service providers and private property owner. This network can enable the qualified drone service providers to access low altitude airspace over the owner's property thereby creating superhighways. *AERO Token* is an ethereum-based blockchain technology which allows the property owners to grant temporary right-to-way permissions to use the air space above their properties in exchange for some incentives. This will work as a repository of navigable airspace to serve commercial drones which would be the future chain of connectivity.

In summary, the above discussed state-of-the-art related to the blockchain application for drone communications are mostly considering trusted nodes as validator irrespective of their resource (computational and energy) and historic credentials. If in a case, the drone considered as miner do not have enough computational resources or sufficient energy supply then it may not participate in the validation process of blockchain. This can create severe implications for security and even the blockchain validation process if the scenario is under an attack.

2.1 Contributions

Due to the above reasons, in this paper, a blockchain-based security approach for D2X communication is designed which includes the following phases.

- A miner node selection mechanism is designed which is based on the drones state of energy, computing resources, time to hover, service record, and validation time.
- A block creation and validation scheme are designed using the proof of work consensus mechanism for secure and traceable D2X communication.

TABLE 1: Comparison of the state-of-the-art for blockchain and drones

Technique	*BUS: A Blockchain-Enabled Data Acquisition Scheme* [8]	*Lightweight permissioned blockchain system* [9]	*Peer-to-peer principle of blockchain [10]*	*Proof-of-Graph (POG) consensus mechanism* [11]	*Blockchain model based on Hyperledger fabric* [12]	Blockchain-based healthcare scheme [14]	Proposed Scheme
Securing U2U Communication	No	Yes	Yes	Yes	Partial	No	Yes
Securing U2I Communication	Yes	No	No	Yes	Partial	No	Yes
Interference Management	No	No	Yes	No	Partial	No	Yes
Type of blockchain	Consortium	Permissioned	Permissioned	Public	Review of different type of blockchain	Consortium	Hybrid (Public)
Consensus algorithm	Proof of Authority (PoA)	Scalable adaptive delegate consensus algorithm	Proof of Work (PoW)	PoG	Review of different of consensus algorithms	PoA	Proof of Work
Miner nodes/validators	Only trusted nodes	All delegates	All trusted nodes	Role swapping	-	Mobile edge servers, Ground control station and Private cloud	Selective
Miner node/validator selection	Based on majority voting	Delegate consensus process	Based on central authority	Dynamic partitioning	-	Based on majority voting	Computational power, historic record and energy based selection
Energy as a parameter for miner selection	No	No	No	No	-	No	Yes
Measure	Data acquisition scheme for IoT using UAVs	Named data networking with blockchain	Secure communication and prevention of UAVs from hijacking	Intrusion detection and prevention for false data injection	Different blockchain schemes and overview of Hyperledger Fabric.	UAV based secure communication with body sensors hives via a token	Miner node selection scheme for D2X communications
Key Tasks	Data encryption and two phase validation using π-hash bloom filter and digital signature	Interest-key-content binding (IKCB), forwarding strategy, and on-demand verification	Asymmetric encryption	Stochastic blocks	Survey on various permissioned architecture	Blockchain based security system is utilized to store the health data from UAVs	Miner node selection, Block creation and validation
Localization	No	No	Yes	No	Yes	Yes	Yes
Fault Tolerant	No	No	Yes	No	No	No	Yes (through multiple miners)
Latency	27ms	158ms	NA	NA	NA	25ms	35ms

3 Blockchain Consortium for Secure Communication in D2X Environment

The proposed blockchain consortium for secure communication in the D2X environment is elaborated below.

3.1 Secure D2X Communication Model

The system model of the proposed scheme comprises of a dual-plane architecture having physical and blockchain/control planes. The physical plane consists of i interconnected drones with GBS. These UAVs provides on-demand services (Internet facility, data relaying and product delivery) to the users. To provide these services securely and transparently, a hybrid (public) blockchain-based system model has been designed for highly mobile D2X network. The entire process of the blockchain and control mechanism is performed at the blockchain or control plane. The information among the drones is transfer using the blockchain which helps to maintain security, data integrity and confidentially. The blocks contain the drone service and communication-related data along with the location coordinate of all drones in a vicinity. This information is synced with the other drones to avoid the collisions and provide reliable paths. Also, the proposed model checks and prevent the misuse of drones for any unauthentic or unethical use and warns the GBS about any minor change in its system configuration. Fig. 2 shows a blockchain-based

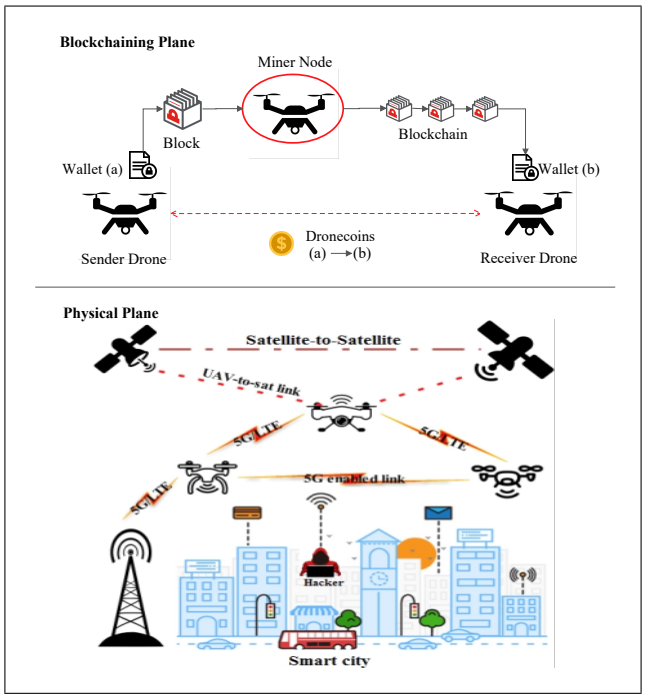

Fig. 2: System Model

system model for D2X communications.

3.2 Blockchain-based Security Framework for D2X Communications

Blockchain is a distributed public ledger which stores the information which can be accessed by all nodes connected in a P2P manner without the intervention of any trusted third party. The blockchain comprises of a growing list of blocks or records, which are interconnected to each other using cryptographic primitives. Each block includes the cryptographic hash of the previous block, transaction data, a time stamp, and proof of work. Blockchain is considered as an open and a distributed ledger which is resistant to any modification or altercation of the data. This ledger can record the transactions happening between two parties, i.e., drone, in an efficient, verifiable and traceable manner. The data in a blockchain cannot be altered retroactively without the consent of the majority of the blocks [15].

In the proposed scheme, the drones forward a service request to the aviation authority (AA) which acts as a central controller. On receiving the request, the block creation process is initiated using proof of work (PoW) or digital signatures of the participating drones. After this, a miner node is selected to validate the transactional process. Once a miner node is selected, the ongoing transactions between drones are validated using these miner nodes. Miner node performs an independent validation of blocks for the successful exchange of data between transacting drones. In the final process, the validated blocks are added to the blockchain and thereby the entire blockchain is updated and synchronized at each drone node. Now, this blockchain can only be accessed by the participating drones and any attempt by an attacker to access the data is failed. Here, *drone coins* are used to reward the miner node for every successful transaction validation. The proposed scheme is divided into *two* parts, 1) miner selection algorithm, and 2) block creation and validation process. These parts are comprehensively elaborated as below.

3.2.1 Miner node selection

The selection of miner node plays an important role in the blockchain-based secure communications. Fig. 3 shows the miner selection process. The AA selects the miner node among the available drones, which is then used to validate the requests from the drone nodes. The foremost requirement of the miner node includes the computational power as it has to compute or solve a cryptographic puzzle. In this algorithm, the AA checks the resource required (R_i^{REQ}) to process any data transaction and then compares it with the threshold level of resources (R_i^{TH}) with each drone. If R_i^{REQ} is greater than the R_i^{TH}, then all such drones are added to shortlisted drone list (SDL). Now, for these j shortlisted drones (j < i) added in the SDL_1, the AA checks the state of energy (SoE_j^{PRS}) available at that instance and compares it with the threshold value, i.e., SoE_j^{TH}. If the SoE_j^{PRS} is less than the SoE_j^{TH}, then they are added to SDL_2. After this, the available SoE, i.e., SoE_j^{AVL} is computed for each drone in SDL_2. Thereafter, the energy available (E_j^{TH}) with all these drones is also computed based on the rated energy of drones battery (E_j^{RT}).

After the battery levels and computational power for each drone are verified, the next step involves the computation of expected time required to validate the transaction initiated in the blockchain. For this purpose, the size of the block (D_{BLK}) and the level of difficulty (d) are major factors. The time required to validate a block by the miner is given as:

$$ToV_j = \frac{D_{BLK}}{R_j^{REQ} \times d} \tag{1}$$

Now, the time available for each drone to hover (ToH_j) is computed as:

$$ToH_j = \frac{T_{CHR}^{RT}}{E_j^{RT}} \times E_j^{REQ} \tag{2}$$

where T_{CHR}^{RT} is the time taken to charge drones battery to its rated capacity and E_j^{REQ} is the energy required to hover.

An service index (SI) is used to record the service track of each drone after completing its flight. A positive flight or successful service adds to this index and unsuccessful or negative user feedback leads to the reduction of this index. Using this index, a miner index (MI) is calculated to select the miner node from all the available drones as below.

$$MI = (ToH_j - ToV_j) \times SI \tag{3}$$

The value of MI for each drone is arranged in the descending order. The drones with the MI above a certain threshold (can be adjusted by AA) are selected as a miner nodes and all the remaining nodes act as ordinary nodes. This process is adopted to ensure that the nodes with sufficient computational resources, energy and positive track record of historic transactions are facilitated as miners. This ensures a strong blockchain security.

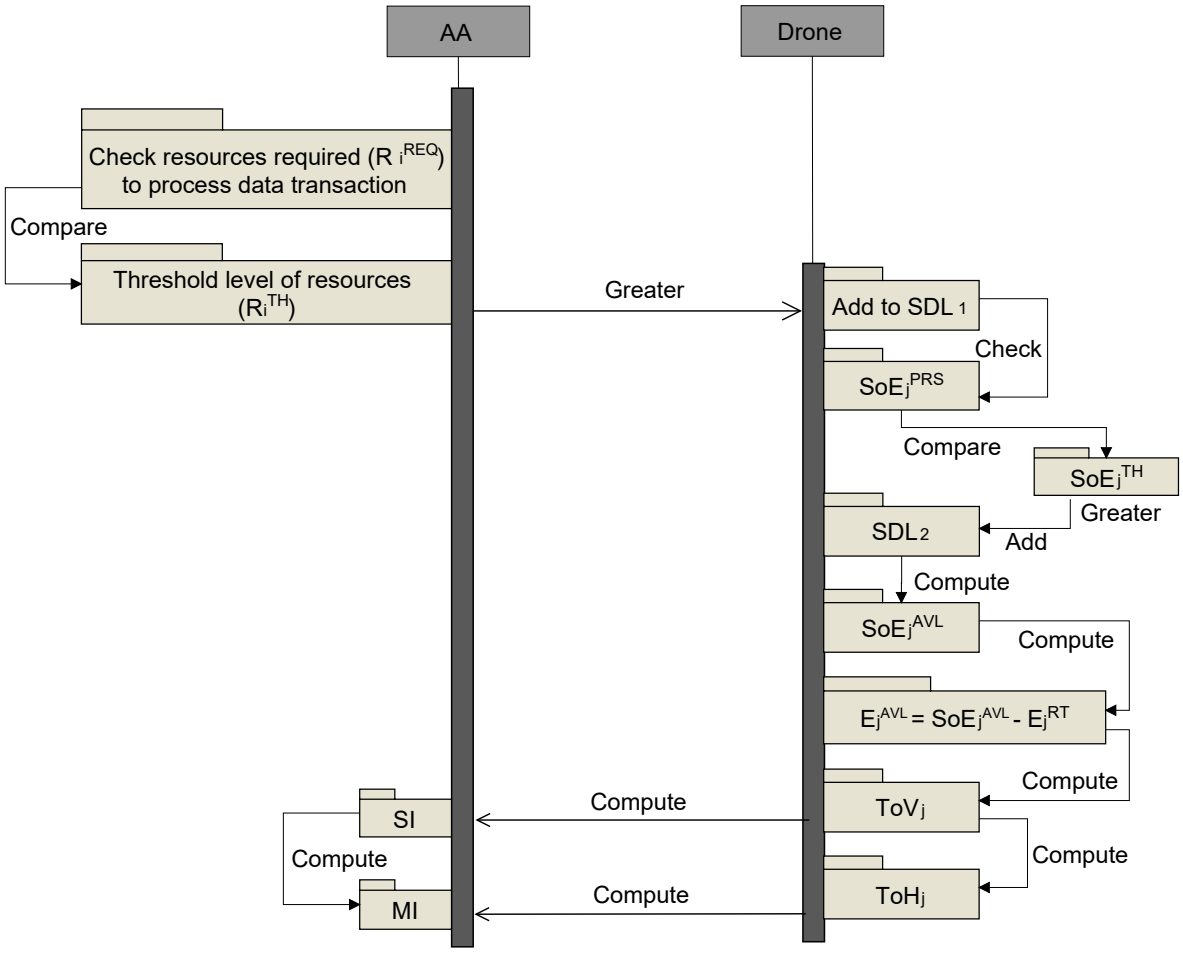

Fig. 3: Miner node selection process

3.2.2 Block Creation and Validation

The requesting drone generates an encrypted block and broadcasts it to the other drones in the network. Then, the AA stores the blocks into a micro cloud and forward them to the miner nodes for validation. The storage of these blocks at the micro cloud helps in future synchronization if required. Here, during the process of validation, different activities like, sensing, performing computations, and storing the data, are performed by the selected miner node. If a block is authenticated by the miner node, then the blockchain is updated. However, it is invalidated if found to be inauthentic. In a case, where the request is validated, then only a drone can commence the transactions as it has proved to be authentic.

The sequence of activities for blockchain-based secure communication between two drones is depicted in Fig. 4. In step 1, the transaction set is created for the requesting drone (a), which comprises of Wallet details, previous transaction record, transaction number, order, receiver public address and digital signature. Using the transaction set details, the block header is generated in step 2 which consists of sender and destination drone addresses along with the action preformed status module. In step 3, the block is created using a block header, previous block hash, encrypted transaction set, timestamp and Proof of Work consensus. Now, the block header and payload is presented for validation in step 4 to the miner node using Proof of Work consensus mechanism. In this step, the miner node is selected based on the scheme discussed in the previous section. If the block is validated, it is added to the blockchain. In the final step, the receiver drone (b) can access the details of the block as per the granted access rights. The above-discussed activities involve a communication dialogue between drones (i), AA, and miner node (j). This communication dialogue is presented in Fig. 5 and discussed as below.

1) In the first step, drone (i) generates a request $\mathbb{R}$ and sends it to AA using a secure channel, i.e., SSL/TLS connection. $\mathbb{R}$ contains the details like, drones identity $(\mathbb{ID}_i)$, location coordinates of drone (l_x, l_y, l_z) from the point of origin, drones rotation angle (r_θ), scale (s), and skewness of the drone from its origin (γ).

2) In second step, AA (j) computes the unique wallet address $(W_{\mathbb{ID}_i})$ on basis of $\mathbb{R}$ and a 32-bit salt value $(\mathbb{S}_i)$ is added to it. $\mathbb{S}_i$ is added to increase the complexity so that an attacker cant break it with ease. Now, a valid certificate (C_i) is generated and appended with the $(W_{\mathbb{ID}_i})$ and sent to the requesting drone.

3) When the requesting drone receives $(W_{\mathbb{ID}_i})$ and the valid certificate (C_i), it use Merkle hash tree to generate the

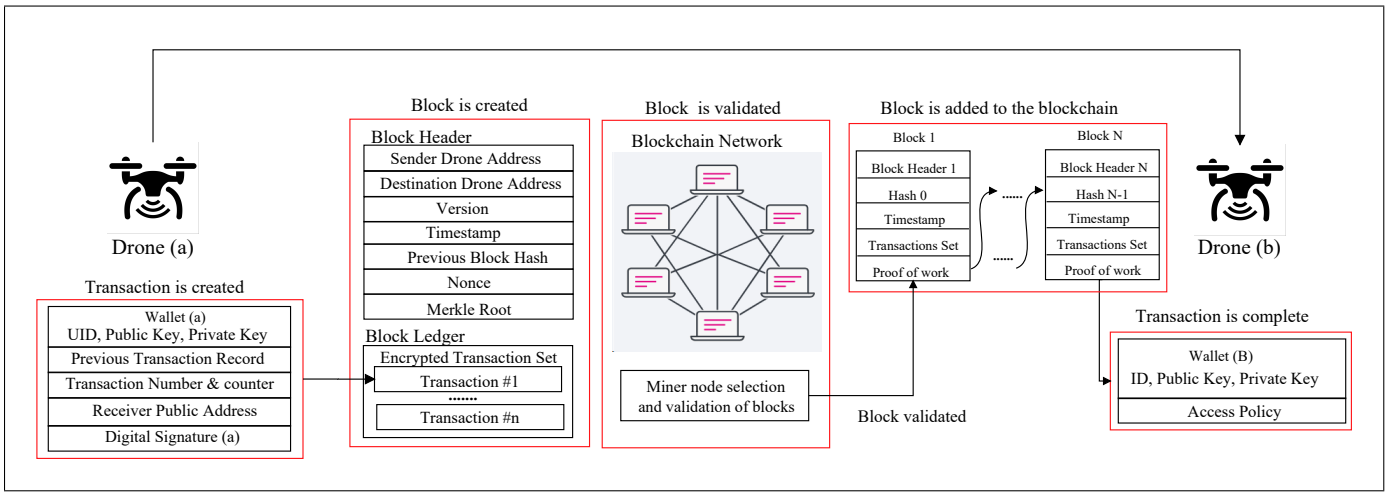

Fig. 4: Blockchain process

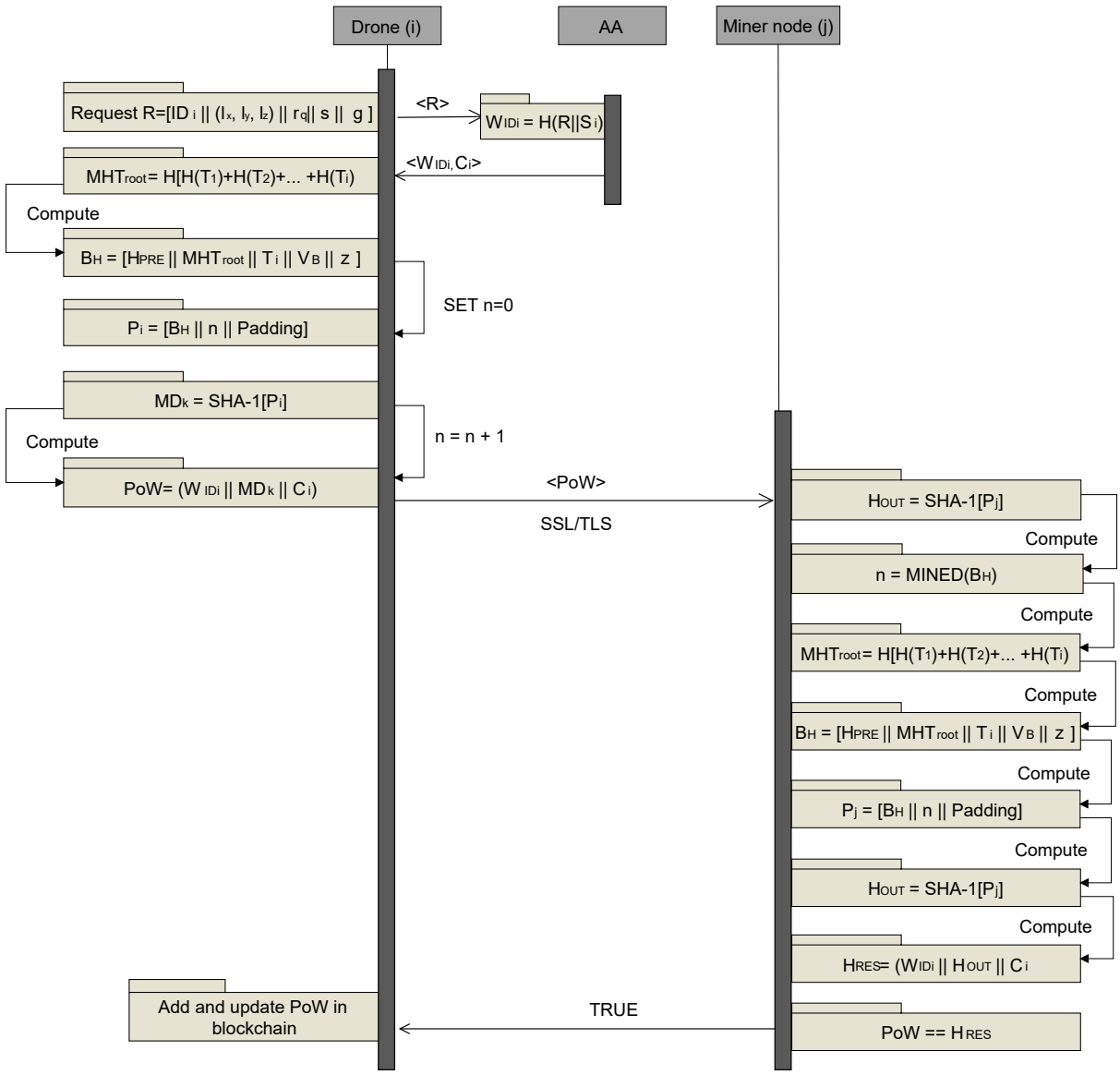

Fig. 5: Communication Dialog for Blockchain

combined hash address ($\mathbb{MHT}_{root}$) for all the transactions. This ($\mathbb{MHT}_{root}$) is computed by the hashing individual transaction like $\mathbf{H}(\mathbf{T}_1)$ and thereafter a hash code is generated by combining the left and right hash indexes of the child. After this process, the drone computes a random block header ($\mathbb{B}_{\mathbf{H}}$) to provide some stochastic nature by adding the hash index of the previous block ($\mathbf{H}_{PRE}$), ($\mathbb{MHT}_{root}$), the time stamp (T_i), the current version of the block $\mathbb{V}_{\mathbb{B}}$ along with a random difficult number (ζ). This random difficulty number is chosen from a range (0) to the 2^{32}. Now, to create a message of determined size, a nonce and the padding bits are added with the ($\mathbb{B}_{\mathbf{H}}$). Starting from n = 0, the value of nonce is incremented after each successful iteration. Here, a message digest ($\mathbb{MD}_k$) is computed for the input block using SHA-1 which generates a 160 bits hash output. Now, the block value is repeatedly hashed to create a complex hash index based on different nonce values. Finally, the **PoW** is generated as a digital acknowledgment for the requesting drone by combining $\mathbb{W}_{\mathbb{ID}_i}$, $\mathbb{MD}_j$, and $\mathbb{C}_i$. This **PoW** is forwarded to the miner node for validation using the secure channel.

4) The miner node (j) get the initial inputs like, ($\mathbf{H}_{PRE}, \mathbb{V}_{\mathbb{B}}, d$) and then mines the $\mathbb{B}_{\mathbf{H}}$ and extracts the nonce from it. Afterwards, it calculates an alike $\mathbb{B}_{\mathbf{H}}$ and utilize the same to calculate the hash output ($\mathbf{H}_{OUT}$) using SHA-1 on $\mathbb{B}_{\mathbf{H}}$ and the payload ($\mathbb{P}_j$). Finally, it generates the hash result ($\mathbf{H}_{RES}$) using the $\mathbb{W}_{\mathbb{ID}_i}$, $\mathbf{H}_{OUT}$ and $\mathbb{C}_i$. Now, if ($\mathbf{PoW} = \mathbf{H}_{RES}$), then the transaction is validated otherwise it is rejected. After validated, the block is added and the blockchain is updated.

4 Security Evaluation

The security evaluation of the proposed scheme concerning computation time and communication cost is given below.

4.1 Communication cost

In the proposed scheme, a 128 bits key is used for generating $\mathbb{ID}_i$ of a drone. This identity produces an SHA-1 based 160 bits message digest or hash output. These two values become the basis for the computation of the communication cost in the proposed scheme. The computed cost is shown as below.

- **Drone (i)**: The drones location is computed using (128+8+8+8+8) = 160 bits; where $[(l_x, l_y, l_z), r_\theta, s, \gamma$ are of 8 bits each. In the first phase, 416 bits are processed for $\mathbb{B}_{\mathbf{H}}$, which includes, 160 bit $\mathbf{H}_{PRE}$ and $\mathbb{MHT}_{root}$, respectively and 32 bit $\mathbf{T}_i$, $\mathbb{V}_{\mathbb{B}}$, and ζ, respectively. A 32 bit nonce and a 64 bit padding is amalgamated with the $\mathbb{B}_{\mathbf{H}}$ to generate a 512 bit $\mathbf{P}_i$. Now, a 160 bit out put is returned using SHA-1 to generate $\mathbb{MD}_k$.
- **AA**: At this level, a 160 bit $\mathbb{W}_{\mathbb{ID}_i}$ is generated including the 32 bit salt and 128 bit $\mathbb{C}_i$.
- **Miner node (j)**:The **PoW** is processed for validation purpose and the output or 480 bits is received in the form of 1 bit valid (1) or invalid (0) result.

Combining the above computed values, the communication cost comes out to be (160 + 192 + 128 + 480 + 1) = 481 bits.

4.2 Computation time

In the proposed scheme, different operation (addition, one-way hashing function and append) are used to crate and validate the block. The standard time used for addition (ADD), one-way hashing (H) and append (APP) operations is 1 ms, 2.7 ms and 0.3 ms. Based on these values, the time incurred for the computations in the proposed scheme is discussed below.

- The computation time incurred at drone level includes 12 APP, 2 H, 2 ADD operations which totals out to be 16 ms.
- The computational time incurred at AA includes 1 H and 1 APP operations resulting in 3 ms time.
- At miner node, the computation time $\mathbf{T}_k$ = 16 ms.

Combining the above computed values, the computation time comes out to be (16 + 3 + 16) = 35 ms.

5 Issue and Future Research Challenges

- **Tracking and Positioning**: In IoD ecosystem, the drone have to rely on GPS signals (often prone to errors) for their positioning. To further supplemented the positioning technologies, the on-board vision and sensing devices are used but this ends up in an increased computational cost.
- **Resource Exhaustion**: As we are aware that drones have limited computational and non-computational (battery power) resources, so sustaining the drones computations to a minimal level is always a challenge.
- **Communication Security**: The wireless networks are backbone for the entire communication process in the IoD. But, these networks are inherently prone to several security vulnerabilities, making it necessary to protect them from security flaws.
- **Scalability**: The number of UAV participating in a network is decided according to the requirement of the application. Even entry of a single UAV into blockchain is a difficult task as all the transactions are verified at every single node.
- **Storage capacity**: This is also one of the key factors in the blockchain. When the chain grows, it stores copies of data at each node in the network, the storage requirement becomes significant. The drones have limited resources so as the chain grows, the capacity needs to be a tough challenge as the oversized chain has diverse impact on the performance.
- **Over-sized chain**: As the chain grows, the size of the chain also grows. This often results in an oversized chain which limits the performance. Moreover, the synchronization of such oversized chain is a challenging task due to computational overhead and complexity.
- **Energy consumption**: The use of blockchain technology in UAVs increases a load of computations via proof-of-work or other consensus methods. These methods are highly energy consuming, whereas UAVs battery has limited power capacities.
- **Leaving a blockchain**: If in a case, any UAV wants to leave from the blockchain serving the entire group,

but, it has all the information on the ledger about the location and functioning of other UAVs. The hacker can easily target the other UAVs and can hinder the functioning of UAVs.

6 Conclusion

A blockchain-based security framework has been designed in this paper to provide secure communications in D2X environment. This framework considers the miner node selection mechanism based on multiple factors like computational power, battery state of energy, segment-based area division, and time to hover. These factors are used to compute a service index and thereafter a miner index using which a suitable miner node is elected. The block creation and validation process in D2X environment depend completely on the selected miner node. Finally, the security evaluation for the proposed framework is presented. The lightweight validation shows a minimal communication cost and computation time incurred during the block creation and validation phases. Further, the challenges and future directions pertaining to resource exhaustion, scalability, storage capacity, oversized chain, energy and many other factors have been identified.

Acknowledgement

This work is partially supported through Startup Fund (090614) provided by the Durham University, UK.

References

[1] S. Vashisht, S. Jain, and G. S. Aujla, "Mac protocols for unmanned aerial vehicle ecosystems: Review and challenges," *Computer Communications*, 2020.

[2] E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya, and S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2016, pp. 216–221.

[3] D. He, S. Chan, and M. Guizani, "Drone-assisted public safety networks: The security aspect," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 218–223, 2017.

[4] A. Abbaspour, K. K. Yen, S. Noei, and A. Sargolzaei, "Detection of fault data injection attack on uav using adaptive neural network," *Procedia computer science*, vol. 95, pp. 193–200, 2016.

[5] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *Journal of Network and Computer Applications*, vol. 144, pp. 13–48, Oct 2019.

[6] M. Singh, G. S. Aujla, and R. S. Bali, "Odob: One drone one block-based lightweight blockchain architecture for internet of drones," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2020, pp. 249–254.

[7] G. S. Aujla, M. Singh, A. Bose, N. Kumar, G. Han, and R. Buyya, "Blocksdn: Blockchain-as-a-service for software defined networking in smart city applications," *IEEE Network*, vol. 34, no. 2, pp. 83–91, 2020.

[8] 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.

[9] K. Lei, Q. Zhang, J. Lou, B. Bai, and K. Xu, "Securing icn-based uav ad hoc networks with blockchain," *IEEE Communications Magazine*, vol. 57, no. 6, pp. 26–32, 2019.

[10] I. García-Magariño, R. Lacuesta, M. Rajarajan, and J. Lloret, "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain," *Ad Hoc Networks*, vol. 86, pp. 72–82, 2019.

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

[12] I. J. Jensen, D. F. Selvaraj, and P. Ranganathan, "Blockchain technology for networked swarms of unmanned aerial vehicles (uavs)," in *IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, 2019, pp. 1–7.

[13] C. D. Perkins, E. J. Wroble, and H. A. Halpin, *Aero Token-Creating a Drone Superhighway Using the Blockchain*, 2017. [Online]. Available: https://icosbull.com/whitepapers/3110/AERO_Token_whitepaper.pdf

[14] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in internet of things," *Computers & Electrical Engineering*, vol. 84, p. 106627, 2020.

[15] G. Singh, A. Singh, M. Singh, S. Sharma, N. Kumar, and K.-K. R. Choo, "Blocked: Blockchain-based secure data processing framework in edge envisioned v2x environment," *IEEE Transactions on Vehicular Technology*, 2020.