Computing and Informatics, Vol. 40, 2021, 428–445, doi: 10.31577/cai_2021_2_428

VERIFICATION OF LOCALIZATION VIA BLOCKCHAIN TECHNOLOGY ON UNMANNED AERIAL VEHICLE SWARM

Mustafa Cosar, Harun Emre Kiran

Department of Computer Engineering
Hitit University
North Campus
19030, Corum, Turkey
e-mail: {mustafacosar, harunemrekiran}@hitit.edu.tr

Abstract. Verification of the geographic location of a moving device is vital. This verification is important in terms of ensuring that the flying systems moving in the swarm are in orbit and that they are able to task completion and manage their energy efficiency. Cyber-attacks on unmanned aerial vehicles (UAV) in a swarm can affect their position and cause various damages. In order to avoid this challenge, it is necessary to share with each other the positions of UAV in the swarm and to increase their accuracy. In this study, it is aimed to increase position accuracy and data integrity of UAV by using blockchain technology in swarm. Experiments were conducted on a virtual UAV network (UAVNet). Successful results were obtained from this proposed study.

Keywords: Distributed network, UAVNet, localization, blockchain, Merkle algorithm, energy efficiency

1 INTRODUCTION

In recent years, the concept of blockchain in information technologies has started to come to the fore in areas such as finance, wireless sensor networks [1], medical applications [2], unmanned aerial vehicles [3], cyber security [4] and finance [5]. It is obvious that the majority of these areas focus on communication security. The starting point of the research is based on taking measures in order to increase the coefficient of confidence during the communication of the devices used and to establish a healthier communication.

While blockchain is used in various fields such as cryptocurrencies, supply chain management and e-voting systems, it is also used to provide secure communication in autonomous systems. UAV Swarm Robot autonomy, decentralized control, collective decision making ability, high fault tolerance etc. It has some features such as Blockchain, a decentralized ledger managed by a peer-to-peer network with cryptographic algorithms, provides a platform for the secure execution of different transactions [6]. The decentralized nature of swarm robotics pushes it to think together with blockchain technology. It also allows it to implement different decentralized decision making, behavior differentiation and other business models. Blockchain technology has become an increasingly popular technology in recent years to provide decentralized trust and security in many digital systems, following its success with Bitcoin. Blockchain is used in many areas, which are listed below, as it eliminates the need for a trusted third party.

- Access management [7],
- Digital content distribution [8],
- Applied in areas such as supply chain management [9],
- Smart contracts in the Internet of Things (IoT) field [10, 11],
- Distribution and verification of sensitive business documents [12],
- Increasing privacy in healthcare [13, 14],
- Firmware update of embedded devices [15],
- Security of military autonomous systems [16],
- Swarm management, organization [11].

UAV uses many sensors such as Inertial Measurement Units (IMU), Laser, Global Positioning System (GPS) and Cameras to solve the positioning problem [17]. The UAV is only equipped with GPS equipment for location information due to various constraints such as cost, weight and range. The GPS signal can be easily affected by external interference, noise, receiving equipment failure [18] and cyber attacks. In real experiments for UAVs equipped with GPS only, it has been observed that some may temporarily lose their GPS connection for an extended period of time. In such a case, UAVs that lose their GPS connection have to be downloaded and their missions are canceled due to security concerns. To solve this problem, UAVs need location verification from within the swarm.

The addition of location information to the blockchain as described above provides control of the pre-recorded position evidence with distributed architecture. In this way, it can be stored and protected against attack. Furthermore, the blockchain as a distributed control and security system scenario, can provide the autonomy of UAV when communication channels from other components of UAVNet are lost [19].

Data packets are encrypted using cryptology to ensure secure data transmission in network technologies. However, in some cases, cryptology may be insufficient when a group of network nodes communicate among themselves. In the transmission between nodes, security measures are taken from the center according to the traditional architecture. In these centralized security methods, some major problems arise when there is no communication with the center at the time of the attack. As a solution to these problems, a new technology called blockchain is suggested when it is required to communicate securely between complex nodes.

The use of UAV for civil and military purposes is increasing day by day [20]. These vehicles have some disadvantages. For example, battery life, energy consumption values, physical and cyber-attacks [21]. There are many types of cyber-attacks on UAV networks. Examples of these cyber-attacks include disrupting communication broadcast, DoS / DDoS, buffer overflow, flooding can be shown as attacks [22]. Such attacks cause of UAVs to remain out of service, to fail the task, and even to crash. Another attack on UAV swarms is GPS attacks to change and disrupt their location information [23]. While the GPS signals of the UAVs used for military purposes are kept in an encrypted manner, this information of the civilian UAVs is transmitted directly in an unencrypted form [24].

The process of protecting the connection of devices in UAVNet is largely provided manually. This protection, which is done by encryption methods, is deprived of operational agility and transparency once applied. In the future, a kind of cryptographic infrastructure architecture should be simplified to distribute key data to the desired operating positions against the Man-In-The-Middle attack. In addition, some improvements in transmission methods should ensure that the network is protected against intrusion or interference, while the key information must be able to verify operational changes and users on the route, minimizing the burden on each UAV [19].

In this study, blockchain technology was applied in order to increase the accuracy and data integrity of geographic location information of different numbers of UAV swarms. In this way, against the attacks on the GPS position was tried to provide protection against the swarms. In addition, the energy consumption data of the UAVs were measured as a result of the application and another advantage of this technology was revealed.

In the next part of the study we provided the literature research, and in Section 3 the basic information was given. Section 4 introduces the proposed method and the results are given in Section 5. Conclusions are summarized in Section 6.

2 RELATED WORK

When the blockchain distributes directly to each UAV, it can significantly prevent the implementation of integrity and usability threats. Since each UAV has a copy of a blockchain, it can autonomously complete its course regardless of other elements of UAVNet. Knowing the location of neighbouring UAVs will prevent air collision [19].

Nowadays, the increased exposure of UAVs to cyber-attack due to their communication with wireless technologies leads to an increase in their work on their security [22]. In these studies, attentions are focused to position accuracy. In the literature, there are many studies on location accuracy of UAVs. The authors in [25] analyze the behaviour of the GPS deception attack targeting the GPS coordinates of the UAVs from the satellite. This study, although the author says that only the distribution of signal strength requires monitoring, does not give much detail on how to determine it. In [26], the author aimed at taking a precaution against GPS attack by means of multiple antennas. The solution made with this multi-antenna is an effective solution to the deterioration when used with the physical security function. This solution, however, is not cryptographic, and brings more weight and cost to the buyer. In many studies similar to these studies, a centralist security approach is recommended.

Since the blockchain is still a new technology, there are very few studies in the UAVNet area. In this area, there are studies such as data collection with data chain, protocol architecture [3] and data transfer [27]. A UAV that wants to ensure the position accuracy can verify the location via its short distance technology with the help of the UAVs in its neighbouring area [28]. In addition to neighbouring verification, we also recommend that the current location of the requesting UAV should not be changed with the previous location records thanks to the blockchain records.

As the use of blockchain technology increases in different areas, it is possible to use it in networks where devices such as UAVNet need to make geo-location accuracy. The fact that this kind of practice is not included in the literature has been evaluated as a motivation for this study. In this study, a model proposal has been made to verify the geographical location information of UAVs. In this model, it is based on a safe publication of adjacent UAVs by adding blockchain switch in a data packet for the location of a selected node of the selected UAVs.

Blockchain is a structure in which transactions and messages are electronically stored in blocks. It is also known that these messages and transactions are recorded by sending them to the entire network. If the messages pass the authentication test, one more block is added to the chain. Verifying any message on the blockchain is extremely simple and only requires a single hashing. In literature, numerous methods have been proposed in the literature to filter false reports from networks. All these schemes are based on collaborative report approval and hop-by-hop report verification [29].

3 CONCEPTUAL FRAMEWORK

The UAV requesting location verification from neighbouring UAVs in blockchain technology is protected against attack because they have signed the information in the data packets they use with their private keys. However, due to GPS attacks, the UAV cannot determine its correct position. Thanks to the close distance technology [28] used in this study, it can determine its actual position with evidence from neighbouring GPSs. However, if the neighbouring UAVs are also attacked after the control center publishes these packages:

- If the UAV which requests location verification, has position information already registered in the blockchain, the maximum distance that this UAV can go with the old records is calculated. If the new location info is greater than the maximum destination, this package is not used in the blockchain. In such a case, if the attacker wants to accept the package, he either has to change the blockchain or must capture more than 50 % of the system. The capture of such a system is almost impossible [28].
- If the UAVs requesting proof of location have two or more different location proofs in their neighbour UAVs, the high number of approved proof packages will be approved.

The addition of location information to the blockchain as described above provides control of the pre-recorded position evidence with distributed architecture. In this way, it can be stored and protected against attack. Furthermore, the blockchain as a distributed control and security system scenario, can provide the autonomy of UAV when communication channels from other components of UAVNet are lost [19].

3.1 Distributed Consensus

The concept of blockchain was first in the economy sector with the crypto currency called bitcoin [5]. The blockchain consists of each block and all blocks are connected to each other. Each block is created according to the consensus mechanism [30].

Consensus mechanisms allow nodes in the network to trust others. The four most popular consensus mechanisms, according to [31], are Proof of Work (PoW) [32], Proof of Stake (PoS) [33], Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof of Stake (DPoS), with other significant approaches including Proof of Authority (PoA), Proof of Elapsed Time (PoET) or Proof of Bandwidth (PoB). Of these PoW is considered to be a disadvantage because of the resource requirements of the systems that will produce the block [34].

The model we propose in this study is closer to the PoS algorithm in terms of block creation process. In UAVNet, as in this algorithm, it will be tasked to create a block to one of the UAVs whose neighbours receive the highest approval over the limit value. The UAVs exceeding the maximum limit shall have the right to be elected in proportion to the number of approved UAVs. Any of these UAVs will be randomly selected. This UAV is assigned by the control center to be selected in a random time and the task of creating new blocks. The first task of the UAV that has taken the task of creating a block is to summarize the location evidence packages of the UAVs with the current blockchain summary and combine it with the Merkle algorithm [35].

Then, to add new blocks to this UAV; it creates a data packet by adding the credential, location records, summary of the previous block, summary of the candidate block, and block creation time. Finally, it signs it with its own private key and transmits this package to other UAVs through the control center. If the majority of UAVs accepts the request to create this new block, the data packet is added to the blockchain, as shown in Figure 1.

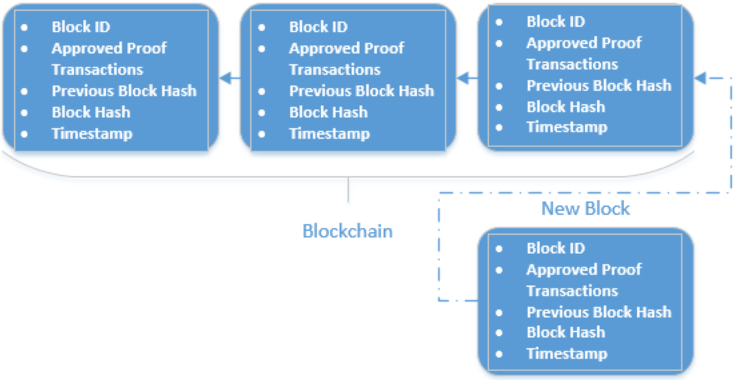


Figure 1. Data package for adding new block to blockchain

3.2 Merkle Tree

A Merkle Tree is a binary tree, a way of iteratively repeating to combine the two hashes in each transaction of a block, then hashing the two hashed transactions again and concatenating them two by one until they become one. The Summary Syntax Tree is a way to bind each function until all of the program's dependencies have been matched. A general structure of the Merkle Tree is shown in Figure 2. A Merkle tree is a secure and efficient [36] chain structure used to verify the consistency of a large set of data records. This structure improves transaction validation performance on blocks.

Each parent node derives its hash value from the value of its children that are recursively dependent on all values in its subtree. Figure 2 shows an example of a Merkle tree, each leaf (H1–H4) gets its value by calculating the imported value (D1–D4) and parents (H5–H6) get values from their children (H1–H4) and finally the root. The value of this Merkle tree (H7) corresponding to each value in the

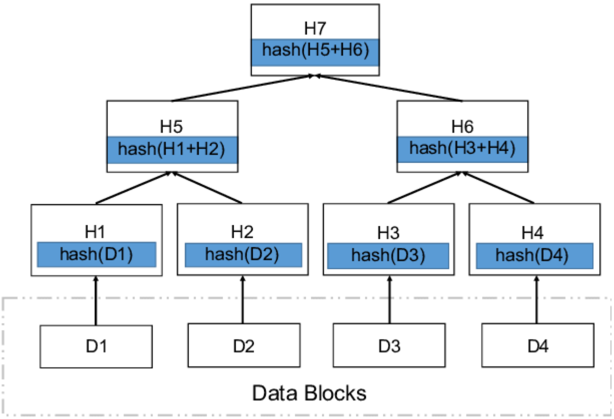


Figure 2. A general structure of the Merkle Tree [37]

tree is obtained. For example, H4 and H5 are needed to verify if H3 is in the tree. A root (H8) can be calculated using H3, H4, and H5. By comparing H7 and H8 we can confirm that H3 is in the tree if the two roots are the same, or that H3 is not in the tree if the two roots are different [37]. The top node named Top Hash [38] represents the Merkle root. All child nodes are leaf nodes and intermediate hash nodes are branches. The leaf nodes of the Merkle tree calculate hashes of numbers proportional to the logarithm, while the number of proportional leaf nodes has lists of hashes.

In the blockchain, a public key is used as the identity of the user and a private key is used to authenticate the data [39]. Also, the blockchain uses a Merkle tree in 1 blocks. In a Merkle tree, changing a value also changes the hash of the entire tree. However, before adding data to the blockchain, each miner must reach an agreement on the validity of the data [40]. Once accepted by everyone, the data is included in the blockchain. After adding data to the blockchain, no changes can be made. If someone tries to make a change to the block, the hash of the block also changes and breaks the blockchain. All validators must agree on this change to reconfigure the chain. Thus, the data on the blockchain remains secure. These blockchain features can be a potential solution to the above mentioned security threats (i.e. cyber attacks, data integrity issue).

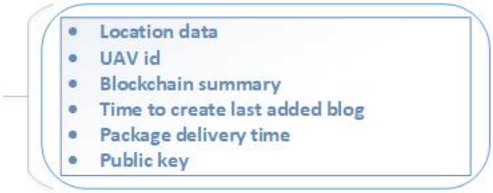
3.3 UAV and Swarm Organization

Although UAVs were originally designed for military purposes, they are also preferred in civilian applications due to their promising functions such as ease of deployment, low maintenance cost and usability [41, 42]. Also, a drone swarm can power IoTs by acting as a relay to transmit data. The use of autonomous systems such as unmanned aerial vehicles has greatly facilitated military operations and is successful in collecting sensitive data and transmitting it to the command center. However, due to the hardware and software components it contains, it has become the target of cyber attacks. Examples of these attacks are manipulating the content of critical messages used in the decision-making of autonomous systems, changing the flight path and changing the current location information. To ensure the successful operation of autonomous military systems [15], it is necessary to develop mechanisms that will strictly protect the integrity of data and messages collected/exchanged, and to provide an immutable record of each message.

Particle swarm optimization and ant colony optimization are the two main techniques in the swarm intelligence family. In particle swarm optimization (PSO), a swarm of particles is placed in a hypothetical solution space with multiple constraints to be met. The particle's global best position and velocity guide the swarm to reach the optimum position and velocity. PSO is a population-based technique and can be effectively used for route optimization problem [43].

3.4 Location Verification Process of a UAV

1. A UAV wanting to verify location, as shown in Figure 3, signs its own identity, the current location information, the summary of the blockchain, the creation time of the last block added to the chain, the time to create the package and the public key in a package and sign it with its private key. Then, the UAV issues this signed data package with the original package to the neighbour nodes and waits for a while. This UAV makes a publication covering the locations of neighbouring UAVs close to it, taking into account the energy consumption when broadcasting the package. If a certain number of neighbouring UAVs have not received approval during this period, they will repeat the broadcast by increasing the area to send the package. This process continues in the form of iterations until the confirmation of the determined number of neighbours is received.

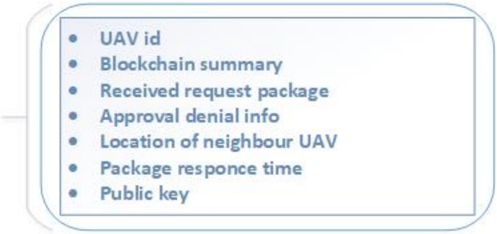


- Location data
- UAV id
- Blockchain summary
- Time to create last added blog
- Package delivery time
- Public key

Figure 3. The contents of the location verification in data package that the UAV sends to neighbouring UAVs

2. Neighbouring UAVs compare the contents of the data packet from the UAV that wants to verify its position with a summary of the current blockchain available in them. Because of the comparison, if the summaries of the blockchains are equalized, the neighbouring UAV approves its position information in the chain.

Then, comparing the requesting UAV's position information with the information in its chain, it summarizes its answer with its own private key, including the information in Figure 4, adds it to the data package and sends it to the control center.



- UAV id
- Blockchain summary
- Received request package
- Approval denial info
- Location of neighbour UAV
- Package responce time
- Public key

Figure 4. Content of the data package prepared by the neighbouring UAV for the UAV that wants to verify its position

3. The control center broadcasts this package to the other UAVs without making any changes. In fact, the neighbouring UAVs proving the accuracy of the location can broadcast this package directly to all UAVs. However, this publication is made by the center because the UAVs in the swarm may be scattered over a wide area and their battery capacity may have decreased.

3.5 Security

Information security is a concept that has been studied since the beginning of computing. Also, some specialized fields such as cryptography have been explored earlier than this. The main objectives of security requirements are: confidentiality, authentication, availability, integrity, and non-repudiation [42]. Cyber security comes to the fore when computers are connected to each other.

Wireless sensor networks are an easy target for report generation attacks where compromised sensor nodes can be used by an attacker to flood the network with fake/false reports. Pathway filtering is a mechanism where intermediate forwarding nodes identify and drop false reports as they are routed to the pool. Current path-through filtering schemes have either high storage overhead or low filtering efficiency [44]. As it is known, DoS, DDoS, MITM ataks, non-repudiation, content poisoning [45] are cyber attacks on UAVs. In addition, attackers UAVs can launch alteration attack to inject, delete or modify any message. Therefore, they may maliciously respond with data packets modified to meet the consumer interests, resulting in cache poisoning.

4 METHOD

The communication architecture with the neighbours for the location verification of a UAV within the UAV swarm is shown in Figure 4. The most remarkable innovation in this model is the use of blockchain technology. When a communication started, it was hashed into the code sent by a block and then broadcast to each node. Since thousands of transaction records can be processed in each node's block, the blockchain uses the Merkle Tree function to generate a final hash, which is the Merkle tree root.

The reason we included the Merkle Tree method in the formation of the blockchain is that it leads to a decrease in the block propagation speed between points. In [36], performing an application with the blockchain and Merkle tree simulator, showed that block transactions have a high effect of reducing the verification time by up to 30 times, with no effect on the block propagation delay. This latest hash value will be saved in the block header (the hash of the current block), thus greatly reducing data transmission and system resources using the Merkle Tree function.

As shown in Figure 5, UAV, which is orange in its background, transmits a broadcast to the neighbour UAVs to ensure location verification. The vector position deviation that occurs during the attack of the selected UAV is planned to be equal to the position deviations of the neighbouring UAVs.

The location verification process we have tried to summarize in 3 items above in Section 3, we experimented with a lot of 100 UAVs in the simulation environment. In this study, 10 different flight plans from 500 meters to 5 000 meters were conducted with UAVs. The energy consumption and position verification information of the swarm which is distributed randomly is tried to be calculated. Experiments were repeated 10 000 times in order not to be affected by different parameters, then an average value was calculated.

The information obtained using GPS trajectory data is becoming more comprehensive, detailed and accurate [46]. UAVs need accurate location information for a variety of purposes, including route planning, operations, control and mission completion [17]. Most UAVs use location information; global positioning system (GPS), inertial navigation system, or a combination of both [47].

5 RESULTS

5.1 Location Verification During Attack

During the location verification process, a simulation was made with 100 UAVs in the 5 000 m × 5 000 m area. In order to determine how the location verification of the UAVs was affected during the attack, one of the UAVs with randomly selected at least 6 neighbours was attacked with GPS Spoofing. The resulting position deviation of the attacked UAV was applied to the neighbours UAVs as the position deviation vector of the same value. This experiment was repeated 10 000 times in order to minimize the effects of the parameters that could not be taken into account.

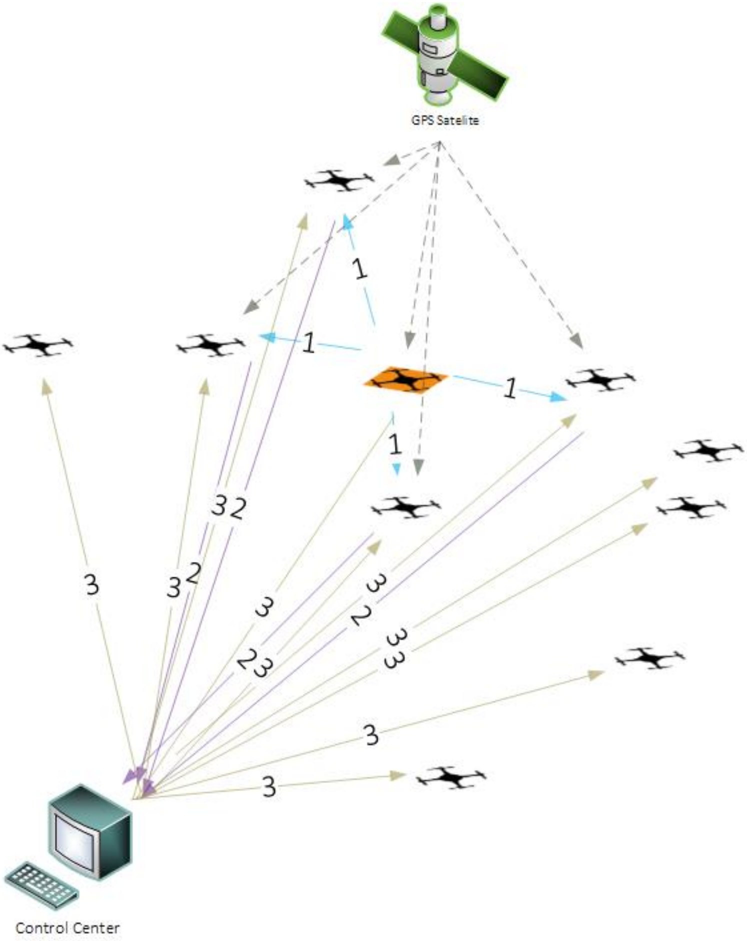


Figure 5. Location verification model among neighbours with blockchain technology in UAV swarm

As shown in Table 1, the number of attacked neighbouring UAVs increased as a result of a decrease in the position verification performance of UAVs. However, even with a decrease in performance rate, even if the attack rate is the highest, it is determined that the UAVs in the network, such as 84 %, have a high position accuracy.

When GPS is the Spoofing attack, a certain period of time is expected as the UAVs cannot be contacted immediately. In this study, since the UAVs are assumed to be attacked as soon as they start flying, the initial position information is not added to the blockchain. If the instant location information can be added to the blockchain in the first time interval, it is thought that these performance rates will

Number of attacked UAVs	**Position verification performance of UAVs [%]**
0	99.9
20	99.7
40	98.5
60	92.2
80	87.4
100	84.3

Table 1. Position accuracy performance of UAV, which will make position verification, based on the increase in the number of attacked UAVs

increase to close to 100 %. Because, even if an attack occurs, the positions stored in the blockchain will not be affected and the UAVs will be able to broadcast the correct position information.

5.2 Energy Consumption

As a result of the experiments, the second calculated value was energy consumption data. This value was calculated by taking the average of all experiments. It is known that the energy consumption values of UAVs increase as the flight range increases. As shown in Figure 6, it was determined that the UAVs communicating via the control center consumed more energy than the UAVs that communicated directly among them.

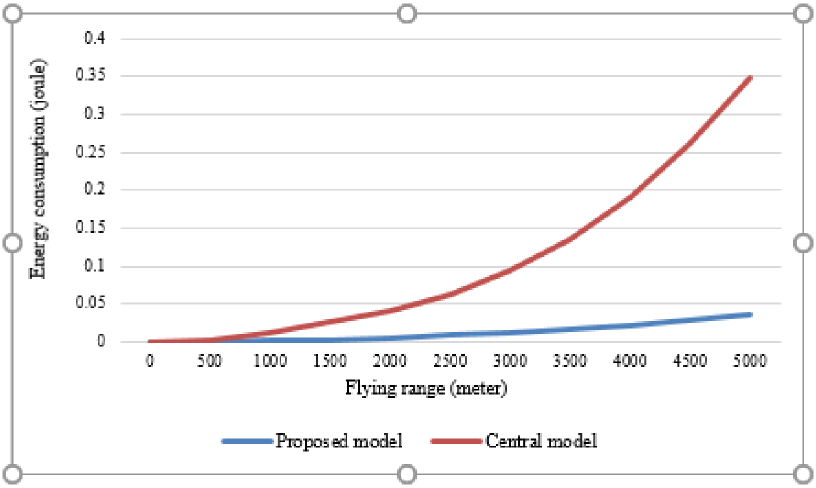


Figure 6. Energy consumption between models

6 CONCLUSIONS

In the proposed model, a hybrid method was used by combining UAV-Neighboring communication and UAV-Control center communication. In particular, in the position verification phase, UAV-Neighbour communication was made according to the possibility of attack of the control center. Blockchain technology was used to increase the reliability coefficient of this communication. Evidence validation was performed with special key in the chain formed by the merkle algorithm. With this model, a UAV deviating from orbit at the time of an attack may request verification from its neighbours. In addition, it is thought that performing location verification by block broadcasting between neighbors will increase energy efficiency, with the thought that broadcasting new locations to the entire swarm by the control center at the end of the location verification process of UAVs will increase energy consumption. Since the control center is included in the chain here, the new location information will also reach it. It can be said that it is unnecessary to verify by contacting the control center again.

In this study, it is aimed to increase the coefficient of trust by the blockchain technology of the location verification process of the UAV flock under attack. During CPS-attack in a UAV swarm, a UAV can verify a position information added to the blockchain, at a rate close to 100 % when from neighboring UAVs require verification. Even if the number of attacked UAVs increased, the verification rate did not fall below 80 %. When the energy consumption values with our model are examined, it is seen that there is a decrease in the rate of 8 times.

An attacker could compromise multiple sensor nodes to inject false reports into the network. These false reports claim events that do not exist at random locations on the network, causing the pool to make incorrect decisions. Therefore, such attacks can cause mission-critical networks to fail. Thanks to this blockchain developed for UAVs,

- Avoiding excessive signature verification for each Data packet,
- Refrain from passing on Interests to potential attackers, provided.

These advantages ensured energy efficiency. Blockchain technology is recommended against some attacks such as content poisoning. However, the method of moving block data to the cache may have a degrading effect on system performance.

REFERENCES

[1] Dorri, A.—Kanhere, S. S.—Jurdak, R.—Gauravaram, P.: Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 618–623, doi: 10.1109/PERCOMW.2017.7917634.

[2] Azaria, A.—Ekblaw, A.—Vieira, T.—Lippman, A.: MedRec: Using Blockchain for Medical Data Access and Permission Management. 2016 2$^{\text{nd}}$ In-

ternational Conference on Open and Big Data (OBD), 2016, pp. 25–30, doi: 10.1109/obd.2016.11.

[3] Kapitonov, A.—Lonshakov, S.—Krupenkin, A.—Berman, I.: Blockchain-Based Protocol of Autonomous Business Activity for Multi-Agent Systems Consisting of UAVs. 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), 2017, pp. 84–89, doi: 10.1109/red-uas.2017.8101648.

[4] Liang, G.—Weller, S. R.—Luo, F.—Zhao, J.—Dong, Z. Y.: Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks. IEEE Transactions on Smart Grid, Vol. 10, May 2019, No. 3, pp. 3162–3173, doi: 10.1109/TSG.2018.2819663.

[5] Nguyen T. T.—Hatua, A.—Sung A. H.: Blockchain Approach to Solve Collective Decision Making Problems for Swarm Robotics. In: Prieto, J., Das, A., Ferretti, S., Pinto, A., Corchado, J. (Eds.): Blockchain and Applications (BLOCKCHAIN 2019). Springer, Cham, Advances in Intelligent Systems and Computing, Vol. 1010, 2020, pp. 118–125, doi: 10.1007/978-3-030-23813-1_15.

[6] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. Self-Publication, available at: `https://bitcoin.org/bitcoin.pdf`, 2009.

[7] Di Pietro, R.—Salleras, X.—Signorini, M.—Waisbard, E.: A Blockchain-Based Trust System for the Internet of Things. Proceedings of the 23rd ACM on Symposium on Access Control Models and Technologies (SACMAT '18), 2018, pp. 77–83, doi: 10.1145/3205977.3205993.

[8] Kishigami, J.—Fujimura, S.—Watanabe, H.—Nakadaira, A.—Akutsu, A.: The Blockchain-Based Digital Content Distribution System. 2015 IEEE 5th International Conference on Big Data and Cloud Computing, Dalian, China, 2015, pp. 187–190, doi: 10.1109/BDCloud.2015.60.

[9] Hofmann, E.—Johnson, M.: Supply Chain Finance – Some Conceptual Thoughts Reloaded. International Journal of Physical Distribution and Logistics Management, Vol. 46, 2016, No. 4, pp. 1–8, doi: 10.1108/IJPDLM-01-2016-0025.

[10] Christidis, K.—Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things. IEEE Access, Vol. 4, 2016, pp. 2292–2303, doi: 10.1109/ACCESS.2016.2566339.

[11] Islam, A.—Shin, S. Y.: BUS: A Blockchain-Enabled Data Acquisition Scheme with the Assistance of UAV Swarm in Internet of Things. IEEE Access, Vol. 7, 2019, pp. 103231–103249, doi: 10.1109/ACCESS.2019.2930774.

[12] Aitzhan, N. Z.—Svetinovic, D.: Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. IEEE Transactions on Dependable and Secure Computing, Vol. 15, 2018, No. 5, pp. 840–852, doi: 10.1109/TDSC.2016.2616861.

[13] Aydar, M.—Çetin, S.: Blockchain for Health Information Systems. European Journal of Science and Technology, 2020, No. 19, pp. 533–538, doi: 10.31590/ejosat.735052 (in Turkish).

[14] Yue, X.—Wang, H.—Jin, D.—Li, M.—Jiang, W.: Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. Jour-

nal of Medical Systems, Vol. 40, 2016, No. 10, Art. No. 218, doi: 10.1007/s10916-016-0574-6.

[15] Lee, B.—Lee, J. H.: Blockchain-Based Secure Firmware Update for Embedded Devices in an Internet of Things Environment. The Journal of Supercomputing, Vol. 73, 2017, No. 3, pp. 1152–1167, doi: 10.1007/s11227-016-1870-0.

[16] Angin, P.: Blockchain-Based Data Security in Military Autonomous Systems. European Journal of Science and Technology, Special Issue, 2020, pp. 362–368, doi: 10.31590/ejosat.824196.

[17] Abdelkrim, N.—Aouf, N.—Tsourdos, A.—White, B.: Robust Nonlinear Filtering for INS/GPS UAV Localization. 2008 16th Mediterranean Conference on Control and Automation, 2008, pp. 695–702, doi: 10.1109/MED.2008.4602149.

[18] Mao, G.—Drake, S.—Anderson, B. D. O.: Design of an Extended Kalman Filter for UAV Localization. Information, Decision and Control, Adelaide, SA, Australia, 2007, pp. 224–229, doi: 10.1109/IDC.2007.374554.

[19] Kuzmin, A.—Znak, E.: Blockchain-Base Structures for a Secure and Operate Network of Semi-Autonomous Unmanned Aerial Vehicles. 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), 2018, pp. 32–37, doi: 10.1109/SOLI.2018.8476785.

[20] Goh, G. D.—Agarwala, S.—Goh, G. L.—Dikshit, V.—Sing, S. L.—Yeong, W. Y.: Additive Manufacturing in Unmanned Aerial Vehicles (UAVs): Challenges and Potential. Aerospace Science and Technology, Vol. 63, 2017, pp. 140–151, doi: 10.1016/j.ast.2016.12.019.

[21] Mansfield, K.—Eveleigh, T.—Holzer, T. H.—Sarkani, S.: Unmanned Aerial Vehicle Smart Device Ground Control Station Cyber Security Threat Model. 2013 IEEE International Conference on Technologies for Homeland Security (HST), 2013, pp. 722–728, doi: 10.1109/THS.2013.6699093.

[22] Javaid, A. Y.—Sun, W.—Devabhaktuni, V. K.—Alam, M.: Cyber Security Threat Analysis and Modeling of an Unmanned Aerial Vehicle System. 2012 IEEE Conference on Technologies for Homeland Security (HST), 2012, pp. 585–590, doi: 10.1109/ths.2012.6459914.

[23] He, L.—Li, W.—Guo, C.—Niu, R.: Civilian Unmanned Aerial Vehicle Vulnerability to GPS Spoofing Attacks. 2014 Seventh International Symposium on Computational Intelligence and Design, 2014, pp. 212–215, doi: 10.1109/iscid.2014.131.

[24] He, D.—Chan, S.—Guizani, M.: Communication Security of Unmanned Aerial Vehicles. IEEE Wireless Communications, Vol. 24, 2017, No. 4, pp. 134–139, doi: 10.1109/mwc.2016.1600073wc.

[25] Shepard, D. P—Bhatti, J. A.—Humphreys, T. E.—Fansler, A. A.: Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. ION GNSS Conference, Nashville, TN, 2012.

[26] Magiera, J.—Katulski, R.: Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. Journal of Applied Research and Technology, Vol. 13, 2015, No. 1, pp. 45–57, doi: 10.1016/S1665-6423(15)30004-3.

[27] Liang, X.—Zhao, J.—Shetty, S.—Li, D.: Towards Data Assurance and Resilience in IoT Using Blockchain. 2017 IEEE Military Communications Conference (MILCOM), 2017, pp. 261–266, doi: 10.1109/MILCOM.2017.8170858.

[28] Zhu, Z.—Cao, G.: Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System. IEEE Transactions on Mobile Computing, Vol. 12, 2013, No. 1, pp. 51–64, doi: 10.1109/tmc.2011.237.

[29] Kumar, A.—Pais, A. R.: Blockchain Based En-Route Filtering of False Data in Wireless Sensor Networks. 2019 11th International Conference on Communication Systems and Networks (COMSNETS), 2019, pp. 1–6, doi: 10.1109/COMSNETS.2019.8711352.

[30] Dey, S.: A Proof of Work: Securing Majority-Attack in Blockchain Using Machine Learning and Algorithmic Game Theory. International Journal of Wireless and Microwave Technologies, Vol. 8, 2018, No. 5, pp. 1–9, doi: 10.5815/ijwmt.2018.05.01.

[31] Vasin, P.—Co, B.: BlackCoin's Proof-of-Stake Protocol v2. Self-Publication, available at: `http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf`, 2014.

[32] Queralta, J. P.—Westerlund, T.: Blockchain-Powered Collaboration in Heterogeneous Swarms of Robots. 2019 Symposium on Blockchain for Robotics and AI Systems, 16 pp., 2020, arXiv: arXiv:1912.01711v3.

[33] Conoscenti, M.—Vetrò, A.—De Martin, J. C.: Blockchain for the Internet of Things: A Systematic Literature Review. IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016, pp. 1–6, doi: 10.1109/AICCSA.2016.7945805.

[34] Dorri, A.—Kanhere, S. S.—Jurdak, R.: Towards an Optimized BlockChain for IoT. 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), 2017, pp. 173–178.

[35] King, S.—Nadal, S.: PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Self-Publication, available at: `https://archive.org/details/PPCoinPaper`, 2012.

[36] Fattahi, S. M.—Makanju, A.—Milani Fard, A.: SIMBA: An Efficient Simulator for Blockchain Applications. 2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S), 2020, pp. 51–52, doi: 10.1109/DSN-S50200.2020.00028.

[37] Huang, H.—Lin, J.—Zheng, B.—Zheng, Z.—Bian, J.: When Blockchain Meets Distributed File Systems: An Overview, Challenges, and Open Issues. IEEE Access, Vol. 8, 2020, pp. 50574–50586, doi: 10.1109/ACCESS.2020.2979881.

[38] Bosamia, M.—Patel, D.: Current Trends and Future Implementation Possibilities of the Merkle Tree. International Journal of Computer Sciences and Engineering, Vol. 6, Aug 2018, No. 8, pp. 294–301, doi: 10.26438/ijcse/v6i8.294301.

[39] Islam, A.—Uddin, M. B.—Kader, M. F.—Shin, S. Y.: Blockchain Based Secure Data Handover Scheme in Non-Orthogonal Multiple Access. Proceedings of the 4th International Conference on Wireless Telematics (ICWT), 2018, pp. 1–5, doi: 10.1109/ICWT.2018.8527732.

[40] Dinh, T. T. A.—Liu, R.—Zhang, M.—Chen, G.—Ooi, B. C.—Wang, J.: Untangling Blockchain: A Data Processing View of Blockchain Systems. IEEE Transactions on Knowledge and Data Engineering, Vol. 30, 2018, No. 7, pp. 1366–1385, doi: 10.1109/TKDE.2017.2781227.

[41] Merkle, R. C.: Protocols for Public Key Cryptosystems. IEEE Symposium on Security and Privacy, 1980, pp. 122–134, doi: 10.1109/sp.1980.10006.

[42] Hayat, S.—Yanmaz, E.—Muzaffar, R.: Survey on Unmanned Aerial Vehicle Networks for Civil Applications: A Communications Viewpoint. IEEE Communications Surveys and Tutorials, Vol. 18, 2016, No. 4, pp. 2624–2661, doi: 10.1109/COMST.2016.2560343.

[43] Gupta, L.—Jain, R.—Vaszkun, G.: Survey of Important Issues in UAV Communication Networks. IEEE Communications Surveys and Tutorials, Vol. 18, 2016, No. 2, pp. 1123–1152, doi: 10.1109/COMST.2015.2495297.

[44] Cizmar, A.—Papaj, J.—Dobos, L.: Security and QoS Integration Model for MANETs. Computing and Informatics, Vol. 31, 2012, No. 5, pp. 1025–1044, retrieved from `http://www.cai.sk/ojs/index.php/cai/article/view/1187`.

[45] Lei, K.—Zhang, Q.—Lou, J.—Bai, B.—Xu, K.: Securing ICN-Based UAV Ad Hoc Networks with Blockchain. IEEE Communications Magazine, Vol. 57, 2019, No. 6, pp. 26–32, doi: 10.1109/MCOM.2019.1800722.

[46] Zhu, S.—Sun, H.—Duan, Y.—Dai, X.—Saha, S.: Travel Mode Recognition from GPS Data Based on LSTM. Computing and Informatics, Vol. 39, 2020, No. 1-2, pp. 298–317, doi: 10.31577/cai_2020_1-2_298.

[47] Sasiadek, J. Z.—Hartana, P.: Sensor Fusion for Navigation of an Autonomous Unmanned Aerial Vehicle. IEEE International Conference on Robotics and Automation (ICRA '04), Vol. 4, 2004, pp. 4029–4034, doi: 10.1109/robot.2004.1308901.

Mustafa Cosar received his B.Sc. degree in computer science from the Karadeniz Technical University. He received his Ph.D. degree in computer education from Gazi University, Ankara, Turkey, in 2013. Since 2013, he has been Assistant Professor with the Computer Engineering Department, Hitit University. At the same time, he worked as an IT manager at Hitit University between 2007 and 2017. He is the author of more than 10 articles, and more than 45 conference papers. His research interests include computer networks and cybersecurity, localization, computer forensics and IDS/IPS architecture.

Harun Emre Kiran received his B.Sc. in computer engineering from the Kırıkkale University, Kırıkkale, Turkey. Also, he received his M.Sc. degree in computer engineering from Karadeniz Technical University in 2019. He is currently pursuing the Ph.D. degree in the Deparment of Computer Engineering, Gazi University, Ankara, Turkey. His research interests are mainly in the areas of wireless sensor network and network security.