Alexandria Engineering Journal 113 (2025) 451–460

Contents lists available at ScienceDirect

Alexandria Engineering Journal

journal homepage: www.elsevier.com/locate/aej

Original article

A blockchain-based secure path planning in UAVs communication network

Shubhani Aggarwal [a], Ishan Budhiraja [b], Sahil Garg [c,d], Georges Kaddoum [c,e], Bong Jun Choi [f,*], M. Shamim Hossain [g]

[a] *Amity School of Engineering and Technology, Amity University Punjab, Mohali, India*
[b] *School of Computer Science Engineering and Technology, Bennett University, Greater Noida, Uttar Pradesh, India*
[c] *Electrical Engineering Department, École de Technologie Supérieure, Montreal, QC H3C1K3, Canada*
[d] *Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, 140401, Punjab, India*
[e] *Artificial Intelligence & Cyber Systems Research Center, Lebanese American University, Beirut, Lebanon*
[f] *School of Computer Science and Engineering, Soongsil University, Seoul, Republic of Korea*
[g] *Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 12372, Saudi Arabia*

ARTICLE INFO

Keywords:
Blockchain
Unmanned aerial vehicles
Path planning
Genetic algorithm
Travelling salesman problem
Security and privacy

ABSTRACT

Unmanned aerial vehicles (UAVs) are one of the most popular and effective systems in various industrial applications such as surveillance, security, and infrastructure inspection. It is gradually becoming an essential part of navigation as a consequence of high progress in military and civilian missions. Path planning of UAVs in military and civilian missions or in unknown and restricted environments is one of the biggest problems facing the operation of UAVs. This problem is not only searching for a path from an initial point to the final but also linked to find an optimal among all possible paths and provides collision avoidance. By examining the best path for UAVs, there is a need for the consideration of various other issues such as security and privacy, turning angle, overtake speed of obstacle, *etc.* The fundamental problem of UAVs is finding an optimal and secure route in a challenging environment. To overcome these challenges, many researchers have used optimization techniques such as ant colony, particle swarm, artificial bee colony, *etc.* with planning and coordination. In this paper, a blockchain-based solution is used to secure and authenticate UAVs. Hence, we propose a blockchain-based method that uses a genetic algorithm, which solves both constrained and unconstrained optimization problems. The purpose of this technique is to locate the best possible flight path for the UAVs in a three-dimensional setting. In a genetic algorithm, each iteration is designed to surpass the previous one in terms of improvement. To achieve an ideal route, solving the travelling salesman problem is a crucial step in the proposed approach. Consequently, the blockchain technology offers a reliable wireless communication and a dependable network for UAVs path planning, guaranteeing efficient service. Simulation results demonstrate the impact of the proposed scheme. They show that a genetic algorithm is suitable for optimal path planning for UAVs.

1. Introduction

In recent years, unmanned Aerial Vehicles (UAVs) have been gaining popularity for their use in various applications and their contribution to market growth. They find utility in military operations for tasks like surveillance, as well as in civilian settings like smart cities. Additionally, UAVs play a crucial role in monitoring public spaces and enforcing social distancing measures during the Covid-19 pandemic. To facilitate their operations, UAVs are connected to a network of Internet-based intelligent devices that handle data aggregation, pre-processing, and distribution. This necessitates the establishment of wireless communication channels between the UAVs, the infrastructure, and the ground controller [1].

The rapid and extensive advancements of UAVs within a short period of time, along with their impressive speed in acquiring new capabilities, demonstrate that UAVs will play a significant role in aviation in the future. Numerous researchers have explored and showcased the practical applications of UAVs in various fields, including aerial photography, healthcare, agriculture, surveillance, tracking, and supply chain management, *etc.* [2,3]. They have delved into the specifications of UAVs, such as sensors,turning angle, version, vision cameras rotation

* Corresponding author at: School of Computer Science and Engineering, Soongsil University, Seoul, Republic of Korea .
E-mail addresses: saggarwal@pb.amity.edu (S. Aggarwal), ishan.budhiraja@bennett.edu.in (I. Budhiraja), sahil.garg@ieee.org (S. Garg), georges.kaddoum@etsmtl.ca (G. Kaddoum), davidchoi@soongsil.ac.kr (B.J. Choi), mshossain@ksu.edu.sa (M.S. Hossain).

https://doi.org/10.1016/j.aej.2024.10.078
Received 19 June 2024; Received in revised form 17 September 2024; Accepted 19 October 2024
Available online 24 November 2024

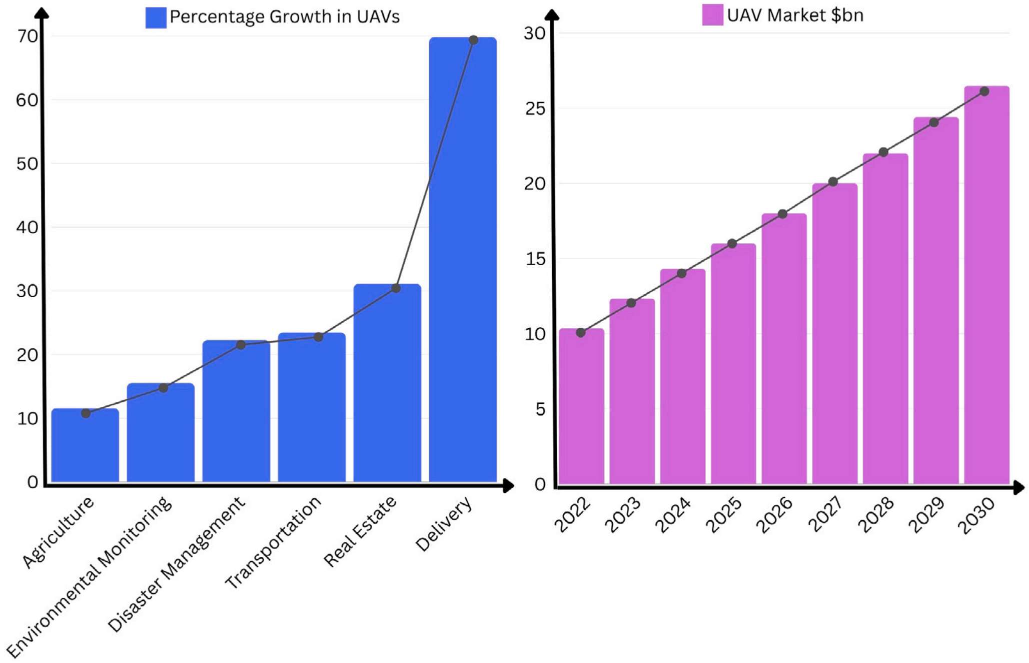

Fig. 1. (a) Percentage growth in various uses of UAVs by 2025. (b) The UAV market in $ billions of dollars by 2025.

angle, and tolerance power. However, only a few researchers have addressed the crucial aspect of UAVs path planning. Path planning is considered one of the most critical factors in the autonomous control of UAVs. After thoroughly reviewing the literature, we, as authors, have come to realize that finding an optimal route for UAVs in autonomous control is a challenging task [4–6]. In these scenarios, the online or offline method can be used to determine the routes for the flight, respectively. As a result, the process of planning the path for UAVs becomes challenging due to various factors such as control points, radar coverage areas, physical obstacles, and more. Several proposals have been made to determine a feasible path for UAVs path planning [7,8]. For example, Wang et al. [9] focused on optimizing the route planning of UAVs using a novel algorithm inspired by the collective behaviour of tuna swarms. UAVs path planning involves determining optimal routes that account for obstacle avoidance, energy efficiency, and mission-specific constraints. The proposed algorithm enhances the basic tuna swarm optimization by introducing modifications that improve its performance, such as better exploration of the search space and faster convergence on optimal solutions. Also, Castro et al. [10] explored the use of Q-learning, a reinforcement learning algorithm, to optimize path planning for swarms of UAVs operating in environments with obstacles. Q-learning enables UAVs to learn optimal actions through trial and error, using a reward-based system to improve decision-making over time. Considering the communication network of UAVs, it is crucial for the communication between UAVs to be secure and protected against attacks like spoofing, eavesdropping, distributed denial-of-service (DDoS), and others.

Moreover, the route for UAVs path planning should also be safeguarded against adversaries, security attacks, and obstacles. To address the challenges associated with path planning in communication networks for UAVs, there is a requirement for the development of a secure and effective communication platform that offers authentication and ensures secure data tracking. This platform would also mitigate the risks of potential attacks, such as the insertion of false data and successful impersonation. In order to enhance security and privacy among UAVs, the implementation of blockchain technology can be considered. Recent endeavours have been made to integrate blockchain with UAV-based communication networks [11–13]. For instance, Gai et al. [14] proposed a blockchain-based technique that enables multi-party authentication to facilitate reliable point-to-point communication among UAVs. Similarly, Garcia et al. [15] put forth a technique to ensure security in UAV networks within the framework of surveillance. They utilized the principles of blockchain, employing asymmetric encryption, and identified compromised UAVs based on trust policies.

From the aforementioned literature, it is evident that the existing proposals have not thoroughly examined the advantages of path planning techniques in the context of UAV communication. The identification of a secure and optimal route in UAV path planning holds significant potential for real-world applications such as agricultural systems, environmental monitoring, disaster planning, transportation systems, inspection systems, and delivery systems. Consequently, emerging technologies such as edge computing, big data, and blockchain are being extensively utilized for the advancement and implementation of UAVs in diverse domains including navigation, localization, mapping, and search operations. According to the report by 2025, the use of UAVs for target missions is expected to grow across a range of applications, as illustrated in Fig. 1(a). Additionally, according to the report presented by Interact Analysis (EV), the market for UAVs is projected to experience a substantial growth, reaching a value of $25 billion by the year 2030, as depicted in Fig. 1(b). Consequently, our proposal revolves around a blockchain-based approach that employs the travelling salesman method in conjunction with a genetic algorithm. This combined methodology aims to identify the most efficient route for secure path planning within the UAVs communication network. The utilization of blockchain in this study ensures the presence of security, transparency, traceability, and authentication features in relation to UAVs. Simultaneously, the integration of the travelling salesman problem with a genetic algorithm allows for the identification of an optimal path for UAVs during their path planning phase.

1.1. Motivation

Traditional centralized control systems are vulnerable to cyberattacks, data tampering, and single points of failure, which can compromise the safety and effectiveness of UAV operations. By integrating blockchain technology, this paper aims to create a decentralized and tamper-proof security framework that ensures the integrity of path planning and communication data in UAVs network. This approach enhances trust, reduces the risk of unauthorized access, and improves the overall resilience of UAV networks, making them more robust and reliable for critical missions.

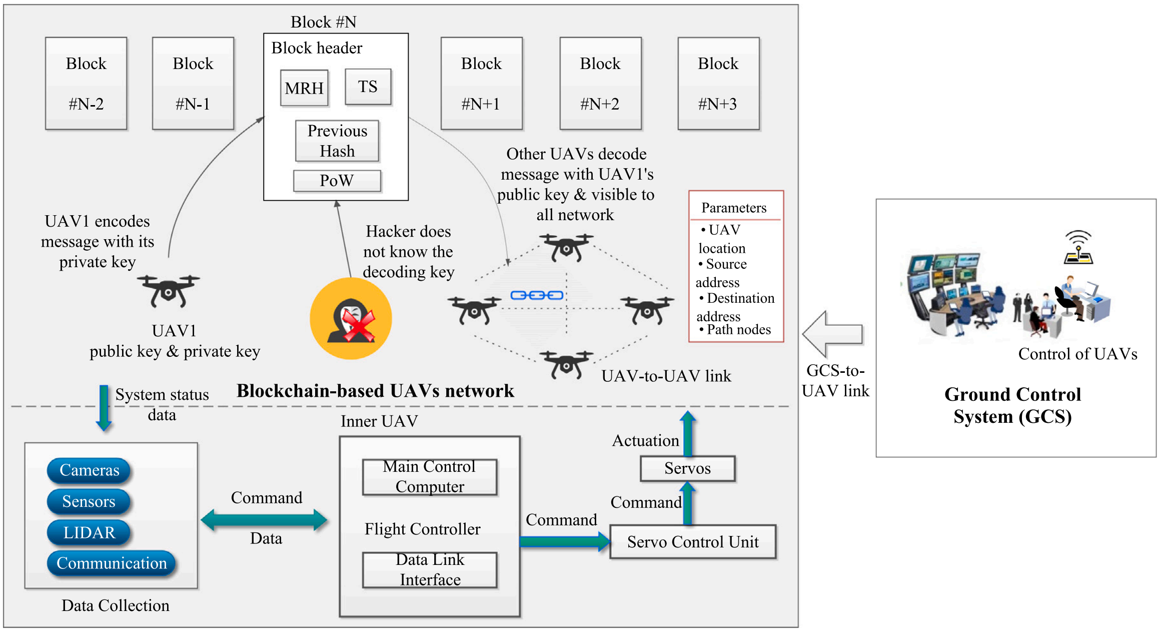

Fig. 2. System model.

1.2. Contributions

The key contributions of this paper are described as follows.

- A blockchain-based system model is proposed for secure path planning in UAVs communication networks.
- We present two models, *i.e.*, UAVs path planning and trust model. The UAVs path planning model includes the registration process and optimal route (travelling salesman problem approach with a genetic algorithm) whereas trust model describes an authentication and security system of UAVs.
- In the end, we used Ethereum platform to establish the blockchain network that shows the computational overhead in UAVs communication network. Additionally, a practical demonstration using a Genetic algorithm shows the impact on optimal routes of UAVs.

1.3. Organization

The remaining part of the paper is structured in the following manner. The system model is presented in Section 2. The problem definition related to path planning for UAVs is formulated in Section 3. The proposed scheme is discussed in Section 4. Section 5 is dedicated to the Experimental Results. Finally, Section 6 presents the conclusion and future works of the study.

2. System model

This section presents a blockchain-based UAVs network for the path planning system model, shown in Fig. 2. This model consists of three main components, *i.e.,* UAVs, Ground control system (GCS), and blockchain network. In this model, UAVs form a blockchain network to perform complex commissions. GCS is assigned and interacts with the UAVs communication network for data collection and data distribution. The information of the UAVs, such as location, source address, destination address, path nodes, is all stored on public ledgers of a blockchain. It provides a real-time facility to UAVs for taking further decisions in path planning and avoiding UAVs collisions. The description of each component of the system model is described as follows.

2.1. Unmanned aerial vehicles

As depicted in Fig. 2, Unmanned Aerial Vehicles (UAVs) are equipped with two types of communication data links, namely UAVs-to-UAVs link and Ground Control Station (GCS)-to-UAVs or radio communication links [16]. Each link carries distinct information. For instance, UAVs-to-UAVs links facilitate the exchange of interaction messages among UAVs, while GCS-to-UAVs links enable the transmission of directions from the GCS, as well as audio/video and other relevant information [17]. The system model for UAVs path planning encompasses the inner UAV, which encompasses the high-level functional components. The layered framework incorporates data collection, a flight controller, actuators, and various sensors. The data collection layer comprises onboard sensors, such as LIDAR track, back and front cameras, and smart devices for sending and receiving. These components gather data from external sources, which is then processed by the UAVs central control system for mapping, localization, and decision-making. The flight controller serves as the core component for processing and controlling the UAVs. It acquires, manages, controls, and processes data from different sources, subsequently providing updated information to the servo control units [18].

2.2. Ground control system

The GCS is a system that consists of both hardware and software and is used on the ground. Its purpose is to enable operators of unmanned aerial vehicles (UAVs) to interact with and control the payloads of the UAVs. This is achieved by adjusting different parameters such as rotors, throttle, and flight surfaces in order to facilitate autonomous operation. Additionally, the GCS is equipped with multiple screens, some of which may be designed with high-brightness features to ensure easy operation even in bright daylight. These screens display various information including maps, instrument overlays, camera feeds from the payloads, flight parameters, and other relevant data.

In addition, the GCS has the responsibility of receiving the gathered data from the UAVs and issuing commands to adjust the movement path, turning angle, rotation angle, and other parameters of the UAVs. It also handles other operations and controls the physical behaviour of the UAVs. It functions similar to a server that collects the original data from the UAVs, hashes it for integrity protection, and then sends both the original and hashed data across the blockchain network to create a permanent record of the information. Moreover, this information can serve various purposes in the planning of UAVs' paths.

2.3. Blockchain network

Blockchain is a distributed peer-to-peer (P2P) public ledger technology that does not rely on a central authority to establish trust. From the introduction of Bitcoin, this technology has been used in various applications such as cryptocurrency, secure storage, smart grid, UAVs, asset transfer, *etc.* [19,20]. Each block is combined with an earlier block using a cryptography data structure known as a hash pointer. All the participant nodes concurrently verify all transactions. These nodes also auditing the content and following the hash pointers. Such type of network ensures tamper-proof, transparent, and immutable system.

In the system model, blockchain is utilized to share information about UAVs, including their location, path nodes, initial point, and target point, among other UAVs that are connected in a network. This sharing of information is essential for real-time collision-free path planning. To accomplish this, all the UAVs' information is collected and stored on the network within a specified time frame. Subsequently, this information is encrypted, digitally signed, and organized into blocks. These blocks are then transmitted publicly on the blockchain network for verification and validation purposes. This approach not only ensures a high level of transparency, security, trust, and efficiency in UAVs' path planning but also enables the utilization of smart contracts. By incorporating public and private keys within the blockchain, UAVs can communicate with each other through a shared channel, while safeguarding against data breaches by unauthorized third-parties. In this manner, blockchain plays a crucial role in facilitating the use of digital signatures, thereby enabling data source and entity authentication between UAVs and third-party agents involved in UAVs' path planning.

3. Problem definition

In this section, we present the problem definition in UAVs path planning, which is defined as finding a path from the source to destination. The main aim is to determine the full path of the UAVs and it must be collision-free path. The planned motion of UAVs gratifies the kinematic constraints, *i.e.,* electrical and kinetic energy [21]. It includes motion planning, trajectory planning, and navigation.

For defining a path in UAVs path planning, we present a 3-D view as 2-D view-based path planning is unable to determine all obstacles.

Now, we introduce a three-dimensional (3_D) path planning environment for UAVs in which there are stationary obstacles, denoted as $Ob = Ob_1, Ob_2, \ldots, Ob_n$, within the 3-D space. The objective is to find a path from the initial point P_i to the goal point P_g. The free workspace WS_f represents the flight area without any obstacles or surrounding issues. Hence, the path planning problem for UAVs in a 3-D environment can be described as finding a path (P_i, P_g, WS_f), which involves various functions as defined in the following equations. Let us consider a function defined as follows.

$$\beta[0,T] \rightarrow 3_D \tag{1}$$

where [0, T] is defined as the covered region. Here, T is represented as a time. Then, the following equations hold.

$$\beta(0) = P_i \rightarrow at\ origin\ time \tag{2}$$

$$\beta(T) = P_g \rightarrow at\ goal\ time \tag{3}$$

$$\exists \phi = \beta(\alpha) \in WS_f \tag{4}$$

For all, α in the interval [0,T], ϕ is referred to as the path planning of the UAVs. In order to achieve an optimal path planning, it is necessary to minimize the cost ($cost$), time ($time$), and energy ($energy$). As a result, it can be defined using the following equations.

$$\beta'(cost, time, energy) = min\ \beta(cost, time, energy) \tag{5}$$

where, β is the function of the entire set of feasible paths, while β' is a function for computing the optimal path.

Thus, the overall cost of communication (Com_{total}) for minimizing the time and expenses in the path planning of UAVs is defined as follows:

$$Com_{total} = S_t + (O_t + H_t)Com_{link} \tag{6}$$

where, S_t represents the start-up time, O_t denotes the overhead time, H_t signifies the per-hop time of the UAVs, and Com_{link} denotes the communication links from the source to the destination.

The primary concerns in the path planning of UAVs is to tackle the security challenges that arise within the UAV network. A number of significant challenges are outlined and discussed below.

- **Path length:** The total distance traversed by UAVs from the beginning to the end determines the length of the journey. In order to ensure efficiency in terms of time, cost, and energy consumption, the path must be optimal.
- **Jamming of UAVs signal:** The jamming signals of UAVs have the potential to be hacked due to their reliance on the directions given by the GCS for flying control and navigation. This can result in a single point of failure, as the system functions similarly to a centralized system.
- **UAVs hijack and poisoned data:** UAV networks are vulnerable to various types of attacks, such as spoofing, Denial-of-Service (DoS), man-in-the-middle (mitm), and eavesdropping, due to their dynamic nature. The presence of wrong UAV in the network can lead to the compromise of the entire system by transmitting inaccurate information. This type of data is commonly referred to as poisoned data. Initially, the participating UAVs input this data, but it is later seized by adversaries or intruders.
- **Mid-air collisions of UAVs:** Nowadays, the UAVs network consists of a significant number of UAVs, which may have a high likelihood of encountering conflicting routes. This is primarily due to a minor delay in the directions provided by the control unit, resulting in a potentially severe issue.

From the challenges mentioned above, it is evident that blockchain technology has the ability to safeguard data and signals that are continuously updated on the UAVs network. This technology ensures the security and privacy of UAVs signals through the utilization of features such as smart contracts,consensus protocols, hashing, public as well as private keys, and more. Consequently, blockchain technology is well-suited for UAVs path planning as it effectively mitigates signal interference. As the number of UAVs in the airspace increases, it becomes crucial to integrate and regulate their movement and usage with the air traffic control system. This integration can be achieved by leveraging blockchain technology, as discussed in [19]. UAVs can independently determine their path by utilizing an on-board blockchain copy that contains information about the paths of other UAVs and input data from the traffic control system.

4. Proposed scheme

In this section, we propose a secure UAVs path planning scheme using blockchain technology. This technology can easily avoid MITM attack, spoofing, misinterpretation of information *etc.*, because of cryptographic hash primitives. Moreover, using consensus mechanisms on a blockchain, it is difficult for the hacker to detect information on the UAVs network. Suppose the hacker wants to hack or modify the UAVs information. In that case, he will recalculate the hash value of the majority blocks on the network that requires a high amount of processing power, which is impossible onboard UAVs. So, to address the challenge of authentication in UAVs path planning, we propose two models, *i.e.,* (i) UAVs path planning model, and (ii) trust model, which ensures privacy and security in UAVs path planning network.

4.1. UAVs path planning model

In this particular model, the implementation of blockchain technology guarantees the ability to track and trace the entire network of UAVs. Each UAV possesses its own private key, which remains inaccessible to anyone else. Address information stored on a blockchain is utilized to monitor any illicit activities carried out by the UAVs. The privacy and security measures inherent in a blockchain wallet effectively prevent attackers from compromising the UAVs network. In a similar vein, if a hacker were to gain access to and destroy a UAV's private key, the UAVs would no longer be able to unlock their attributes via the attribute server. Consequently, hackers would be unable to verify the tasks assigned to the UAVs by the system administrator (SA) and, as a result, would not be able to obtain the UAVs' attributes.

The main goals of this model are as follows: (i) Ensuring the security of UAVs communications in the network by verifying both the senders and receivers. (ii) Monitoring and keeping track of data transfer. (iii) Protecting against attacks from certificate authority (CA). To accomplish these objectives, we have designed two key modules within the UAVs path planning model, namely, (i) the UAVs registration module and (ii) the data transfer validation module. The first module registers the UAVs on a blockchain by providing them with a certificate. The second module verifies data transfer requests by allowing them to create and add a block on a blockchain once the request is validated.

4.1.1. UAVs registration

For a secure registration of UAVs on a blockchain, CA must give UAVs an enrolment certificate to connect them to UAVs path planning network. The step-wise description of UAVs registration is described as follows.

(1) Suppose UAVs $= (U_1, U_2, U_3, \dots, U_n)$ wants to be a part of blockchain-based UAVs network.
(2) The private key (SA_{sk}) of the SA is set as $x \in Z_q^*$, and its public key (SA_{pk}) is computed as X = xp. Similarly, the private key (TA_{sk}) of the trusted node (TA) is set as $y \in Z_q^*$, and its public key (TA_{pk}) is computed as Y = yp, where, p and q represent the generators G_1 and G_2 respectively.
(3) Then, they must register into the system initialization that has SA who generates a public key (PU_{U_i}), private key (PK_{U_i}), and the secret key (U_{sig1}) which is (x_i, y_i) for the UAVs, where i ∈ n, n is the number of UAVs in the network.
(4) The UAVs public key sets, private key sets, and the secret signature key sets are $PU_U = (PU_{U_1}, PU_{U_2}, \dots, PU_{U_n})$, $PK_U = (PK_{U_1}, PK_{U_2}, \dots, PK_{U_n})$, and $U_{sig} = (U_{sig1}, U_{sig2}, \dots, U_{sig3})$, where n is the number of UAVs in the network.
(5) The UAVs' source address (SA_i) and destination address (DA_i) are generated using the UAV's public key.
(6) In the end, the SA provides certificates to every UAV once they have completed registration on the UAVs network, and these certificates are denoted as $Cer_U = (Cer_{U1}, Cer_{U2}, \dots, Cer_{Un})$.

This registration module of UAVs build trust on one another in the blockchain network and allows submit the transaction of a blockchain.

4.1.2. Data transfer request

This module focuses on the transmission of a path request from a single UAV to the blockchain network. The blockchain operates by utilizing active smart contracts to authenticate and validate the path, ensuring all necessary information regarding the UAVs' routes is thoroughly examined. The request must include identification details for both the source and destination addresses, in addition to specific attributes related to the path and trajectory. These attributes encompass the rotation angle, trajectory path, and rotation axis, *etc.*

The path a UAV wants to do collision-free path planning is done by the transaction between the UAVs and the blockchain is T_U.

$$T_U = (SA_i, DA_i, R, time) \tag{7}$$

where SA_i is the source address, DA_i is the destination address, R represents the UAV request for collision-free path planning, and $time$ is the creation period of the transaction. The steps to follow collision-free path for UAVs is described as follows.

(1) A UAV sending a path planning request to a blockchain-based UAVs network where after complete validation and verification constructs a block and broadcast.
(2) In this particular module, the blockchain disseminates requests to the appropriate voters, as depicted in step 2.
(3) Voters retrieve the attribute values from an Attribute Server in order to acquire the necessary attribute data for validating each UAV's request (steps 3 and 4).
(4) This particular step holds significant importance within our module as it primarily focuses on attaining consensus in a blockchain and validating all the attributes being retrieved (steps 5 and 6).
(5) In steps 7 and 8, there are two important tasks. The first one is to inform the requesters about the response, while the second one is to create a block for recording vital details (see Fig. 3).

4.1.3. Shortest path using travelling salesman

The most well-known computational problem is the travelling salesman problem. To determine the optimal solution, a brute-force method can be employed, which evaluates every possible tour and selects the best one. However, a more efficient approach can be adopted by using dynamic programming instead of brute force. It should be noted that there is no polynomial-time algorithm available for this problem. Hence, we use Travelling salesman to solve this problem in UAVs communication network. It optimizes the routing of multiple UAVs to complete each task efficiently. This algorithm is also used to determine the shortest possible route that allows UAVs to visit a set of predetermined targets exactly once before returning to the starting point. This optimization is crucial for reducing energy consumption, minimizing travel time, and maximizing the operational efficiency of UAVs.

For example, In a graph of 'n' vertices, there are (n - 1)! possibilities for the object to be travel. Here, we have a graph $G = (V, E)$, where V represents a set of cities and E demotes a set of weighted edges. An edge $e(u, v)$ signifies a connection between vertices u and v. The distance between vertex u and v is denoted by $d(u, v)$, and it is important to note that this distance is always non-negative. Based on the aforementioned assumptions, the UAV aims to travel from city 1 to city j, with the intention of visiting various cities along the way. The path taken from city 1 to city j constitutes a partial tour for the UAV. The first step is to identify the goal city j, as this will determine which cities are most convenient to visit from the initial point, city 1. Subsequently, it is crucial to keep track of all the cities that have been visited thus far, in order to avoid repetition. Therefore, this becomes a suitable subproblem for UAVs in terms of path planning, and it can be solved by applying the travelling salesman problem.

For a specific group of cities that the UAVs plan to visit during the tour, denoted as S, the set can be defined as $1, 2, 3, \dots, n$ with the condition that it must include the starting point 1 and the destination point $j \in S$. We can refer to the length of the shortest path that visits each node in S exactly once as $C(S, j)$, with the initial point being 1 and the goal point being j.

When $|S| > 1$, we define $C(S, 1) = \infty$ because it is not possible for the path to both start and end at 1.

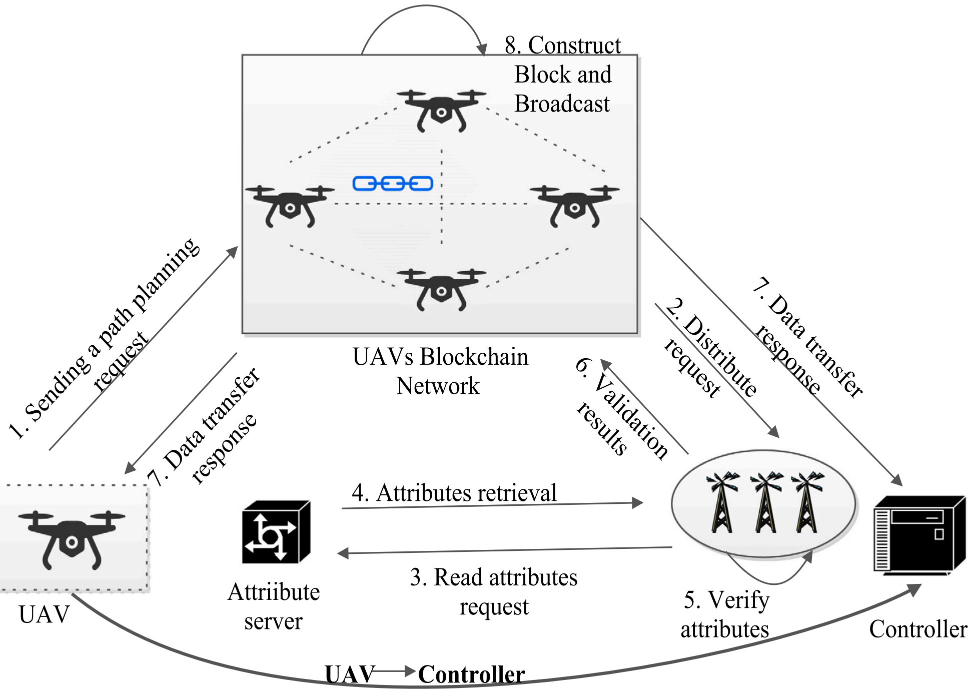

Fig. 3. Request transfer for UAV-controller communication.

Compute the value of $C(S, j)$ by breaking it down into smaller subproblems. Our objective is to begin at city 1 and conclude at city j, while choosing the subsequent city in a specific manner.

$$C(S, j) = \min(C(S - \{j\}), i) + d(i, j) \tag{8}$$

where, $i \in S$ and $i \neq jc(S, j)$

$$C(S, j) = \min C((s - \{j\}), i) + d(i, j) \tag{9}$$

where, $i \in S$ and $i \neq j$. Algorithm 1 defines the travelling salesman problem in UAVs path planning is described as follows.

Algorithm 1 Travelling Salesman Problem

```
procedure Function($SHORTEST\_PATH\_SELECTION$)
    C (1, 1) = 0
    for ($S = 2; S \leq size(N); S++$) do
        for all subsets $S \in 1, 2, 3, ...., n$ of size s and containing 1
        C(S,1) = ∞
        for all $j \in S$ and $j \neq 1$
        $C(S, j) = \min C(s - \{j\}), i) + d(i, j)$
        for $i \in S$ and $i \neq j$
        Return
        $\min jC(1, 2, 3, \dots, n, j) + d(j, i)$
    end for
end procedure
```

4.1.4. Optimal route

This module provides a detailed explanation of the most efficient path for planning the route of UAVs in the communication network. The network consists of various checkpoints. The flow chart illustrated in Fig. 4 displays the genetic algorithm utilized for UAVs path planning. A concise overview of each step involved in the genetic algorithm is presented below.

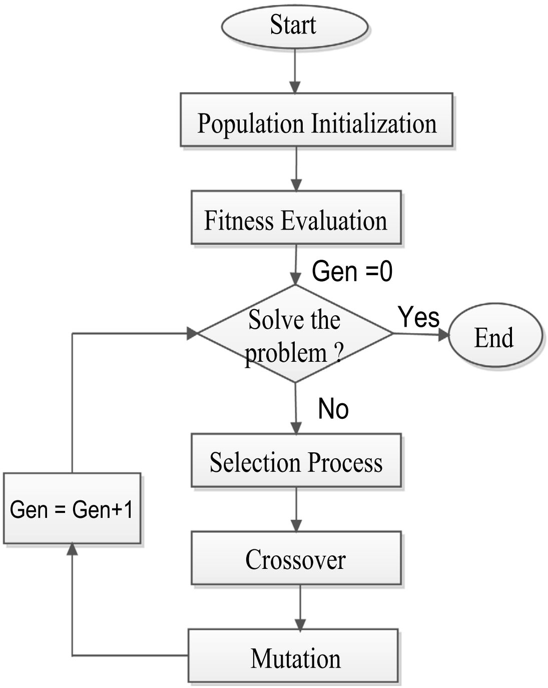

Fig. 4. Flow chart of proposed genetic algorithm for UAVs path planning.

- **Population Initialization:** The genetic algorithm is based on the first population, and then the algorithm gets better results iteration by iteration. The first population is produced randomly, which changes the genetic algorithm into an evolutionary model. As per the structure of the genetic algorithm, chromosomes are composed of binary codes. So, we prefer integer coded-based chromosome design. Each route for UAVs path planning is referred to as a chromosome sample. Each checkpoint is referred to as a gene in the genetic algorithm. Here, we will examine

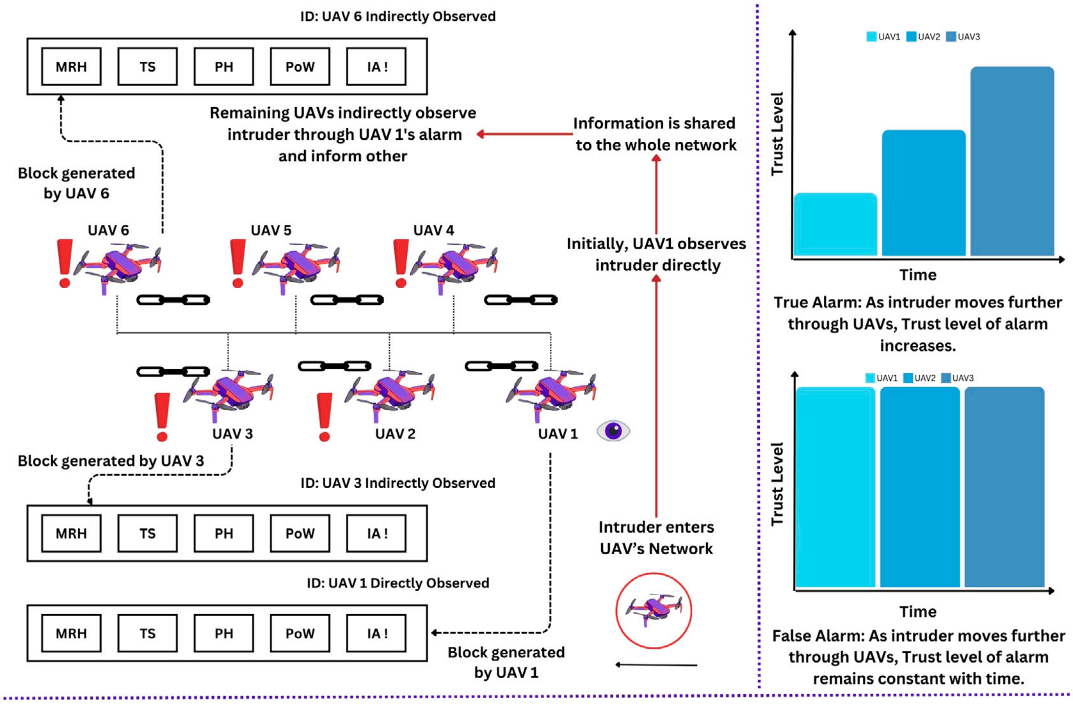
ID: UAV 6 Indirectly Observed
MRH
TS
PH
PoW
IA !
Remaining UAVs indirectly observe intruder through UAV 1's alarm and inform other
Information is shared to the whole network
Block generated by UAV 6
UAV 6
UAV 5
UAV 4
Initially, UAV1 observes intruder directly
UAV 3
UAV 2
UAV 1
Block generated by UAV 3
ID: UAV 3 Indirectly Observed
MRH
TS
PH
PoW
IA !
Intruder enters UAV's Network
ID: UAV 1 Directly Observed
MRH
TS
PH
PoW
IA !
Block generated by UAV 1
UAV1
UAV2
UAV3
Trust Level
Time
True Alarm: As intruder moves further through UAVs, Trust level of alarm increases.
UAV1
UAV2
UAV3
Trust Level
Time
False Alarm: As intruder moves further through UAVs, Trust level of alarm remains constant with time.

Fig. 5. Trust level of true alarm rises while the trust level of false alarms stays constant with time.

two regulations, specifically, that every checkpoint or location is visited just once and that UAVs must return to their initial location.

- **Fitness function:** In the proposed plan, our focus is on solving the problem of the travelling salesman in order to find the most efficient route for UAVs path planning. Therefore, the fitness value is determined by calculating the total route of the UAVs path planning. The primary objective of the fitness function is to minimize the overall route by selecting the optimal route checkpoints.
- **Mating Pool Selection:** We used the Roulette wheel selection idea in this process, which assigned each probability of selection based on the fitness value. With this approach, we employ elitism to select the most exceptional individuals from the population. These individuals will seamlessly transfer their superior qualities to the next generation, guaranteeing the persistence of the most accomplished individual.
- **Crossover:** For the crossover process, we used a two-point crossover. In this, two checkpoints are selected from both different chromosomes of the population and exchanged.
- **Mutation:** This procedure is essential for the algorithm to avoid local convergence and incorporate new pathways in the population to explore the remaining areas of the solution space.

4.2. Trust model

Blockchain ensures the confidentiality and protection of information pertaining to unmanned aerial vehicles (UAVs) through the process of sharing and validating data among the distinct parties associated with UAVs in the network. This mechanism aids in establishing a resilient transmission of data among UAVs. The integrity of all data sets is confirmed at multiple checkpoints on a blockchain to guarantee the accuracy and consistency of the data. Furthermore, by employing public–private key pairs and cryptographic primitives, the resilience of UAVs' path planning networks is enhanced, thereby fortifying them against various forms of attacks such as Man-in-the-Middle (MITM) attacks and spoofing attempts orchestrated by adversaries.

In order to establish trust among UAVs within a network, we propose the implementation of a trust model that is built upon a blockchain framework. This model serves the purpose of generating an alarm system whenever any unauthorized access or intrusion occurs within the surveillance areas of the UAV network. By utilizing this technology, the verification of intrusion events, such as hacking or unauthorized manipulation of data, is made possible. This, in turn, ensures a heightened level of trust through the activation of the alarm system. Whenever an intrusion event takes place, the UAVs are able to detect it by utilizing the information stored within public ledgers. Subsequently, this information is relayed to neighbouring UAVs by means of adding a block containing the details of the intrusion onto the blockchain, as depicted in Fig. 5. It is important to note that each UAV transmits encrypted messages in a unique manner, depending on whether they directly or indirectly detected the presence of an intruder. The sequential explanation of the trust model pertaining to path planning for UAVs is described in (Fig. 5).

(1) An unauthorized person infiltrates the network of UAVs with the intention of participating in malicious activities targeting the UAVs.
(2) UAV1 assumes the role of the initial observer, directly detecting the intruder. In the event that multiple UAVs perceive the same intruder occurrence, it can be confirmed as valid. Conversely, if only a single UAV detects the intruder, it is regarded as truth; however, it is viewed with suspicion.
(3) In this particular instance involving an actual incursion, the initial participant, referred to as UAV1, assumes the role of the observer, diligently monitoring the situation. Following UAV1's surveillance, UAV2 and UAV3 will subsequently undertake their own observations. Accordingly, the level of trust pertaining to the alarm is heightened, as depicted in Fig. 5(a).
(4) In the case of false alarm, only a single notification is received, specifically originating from UAV1, and its level of trust continues to be reduced, as indicated in Fig. 5(b). Moreover, if it is determined that UAV1 has disseminated false information to its neighbouring units, it is liable to penalties and loses its position of trust within the network of unmanned aerial vehicles.

Table 1
Simulation parameters.

Parameters	Reference value
UAVs range	[1, 10]
Speed	[10, 60] Km/h
Altitude	[100, 400] m
Travel	20 Km
Network size	4, 6, 8 UAVs
Workload	100 transactions
Consensus	Ethereum (PoA)
Docker	19.03 version
Simulation environment	Intel(R) i5, 8GB RAM, Ubuntu 16.04.5, 64core CPU
Population	1000
Number of checkpoints	25
Crossover rate	80%
Mutation rate	0.01
Elitism	75%
Generation	2000
Distance	0–2200 Km
Number of city lists	200

(5) The neighbouring UAVs have the capability to determine whether UAV1 is consistently transmitting harmful data, as each UAV keeps a current record of the IDs belonging to all the direct observers.

In this way, the distributed trust model, demonstrates its advantage in identifying false alarms. Hence, it is crucial for path planning networks of UAVs as the loss of trust in an alarm could result in undetected instances of real intrusion.

5. Results and discussion

The proposed scheme is evaluated and discussed with two ways, *i.e.,* (i) performance evaluation using a blockchain and (ii) optimal route evaluation using a Genetic algorithm. The parameters used in results and discussion are discussed in Table 1.

5.1. Performance evaluation

For blockchain-based simulation in UAVs communication network, we set an environment of private Ethereum. The simulation allows for a maximum of ten UAVs, and each UAV has the capability to travel a distance of 20 kilometres at a speed of 60 kilometres per hour, while maintaining a maximum altitude of 400 m. The details of the performance evaluation parameters are discussed in Table 1.

We have used the JPBC library to test the registration and data transfer request cryptographic operations []. To evaluate the proposed scheme based on cryptographic operations, we have observed the communication cost and computation cost of UAVs. We have considered three scenarios: registration, data transfer request, and the number of UAVs in one group. We have observed UAVs' computation and communication costs corresponding to these three scenarios, as shown in Fig. 6. Fig. 6(a) shows the computation costs in ms w.r.t. the registration and data transfer request. Similarly, Fig. 6(b) shows the communication costs in bits w.r.t. the registration and data transfer request. Finally, Fig. 6(c) shows the communication and computation costs w.r.t the number of UAVs in a group.

5.2. Optimal route evaluation

For optimal route in UAVs path planning, we have implemented the genetic algorithm in Python. The shared library in Python helps in mathematical calculations. Firstly, we initialize the population generation phase. After that, the genetic algorithm is executed to find the optimal route using the travelling salesman problem. The parameters used for the simulation for optimal route of UAVs are described in Table 1.

Using the parameters defined, we have implemented the genetic algorithm for UAVs path planning having travelling salesman problem. On the other hand, elitism and mutation in the genetic algorithm allow better offspring in every iteration. With this, Fig. 7(a) shows the comparison between generation and distance in a genetic algorithm. However, this figure describes the route variation for UAVs path planning concerning the generation increment of the genetic algorithm. From this, we observe the best route distance and checkpoints for UAVs path planning in the genetic algorithm having travelling salesman problem, which is described as follows.

Fig. 7(b) shows the difference in initial route checkpoints and best route checkpoints for UAVs path planning after applying the genetic algorithm on a randomly generated population. Similarly, Fig. 7(c) shows the initial and best route distance in UAVs path planning. The best route is short as well as optimal as we are using the travelling salesman problem. It finds the minimum route between the initial point and the goal point from all the possible routes.

5.3. Blockchain network performance

The relationship between the number of sealers and the average throughput of the various transaction sending rates is illustrated in Fig. 8.The system obtains maximum throughput when all transactions are processed and added to the blockchain at transaction rates of 100, 200, and 500 tx/sec.The average latency is inversely proportional to the throughput, as illustrated in Fig. 9. For a network with a moderate sending rate, the average latency of the various transaction sending rates is between 3.3 and 4 s. Nevertheless, the latency experiences a substantial increase of up to 11 microseconds as a result of a larger network size and a higher sending rate. The delay increases as the transaction rate increases, as it requires additional time to distribute the corresponding volume of data to all sealers, as illustrated in Fig. 9. The implementation platform is supported by a maximal throughput of 350 tx/sec, as demonstrated in the results of 8.

6. Conclusion

This paper introduces a solution that utilizes blockchain technology to determine the most efficient route for UAVs in their path planning. The approach employed is based on the travelling salesman problem, and incorporates a genetic algorithm. The main goal of the proposed scheme is to enhance the security and authentication of path planning within UAV communication networks. The simulation results clearly demonstrate the positive impact of the proposed scheme. In the simulation, each checkpoint must be visited once, and the UAVs must ultimately return to their initial point. The results indicate that a genetic algorithm is well-suited for achieving optimal path planning for UAVs. Furthermore, it is acknowledged that the complexity of the problem can be further increased by incorporating additional constraints arising from the dynamic environment, which will be explored in future research.

CRediT authorship contribution statement

Shubhani Aggarwal: Writing – original draft, Methodology, Conceptualization. **Ishan Budhiraja:** Writing – original draft, Investigation, Formal analysis. **Sahil Garg:** Writing – review & editing, Resources. **Georges Kaddoum:** Writing – review & editing, Resources, Project administration. **Bong Jun Choi:** Writing – review & editing, Resources, Funding acquisition. **M. Shamim Hossain:** Writing – review & editing, Resources, Project administration, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

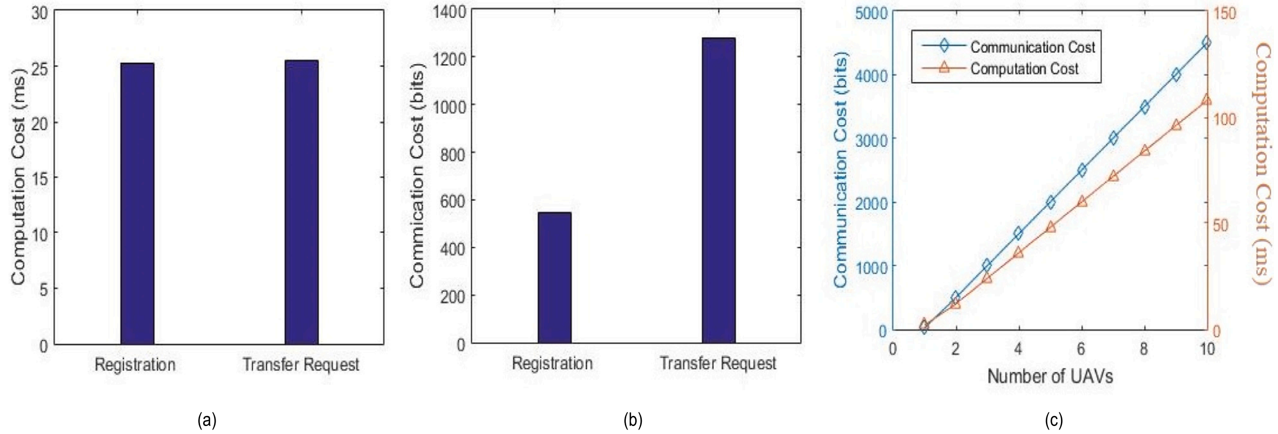

Fig. 6. (a) Computation cost of registration and transfer request, (b) Communication cost of registration and transfer request, and (c) Communication cost and computation cost w.r.t number of UAVs.

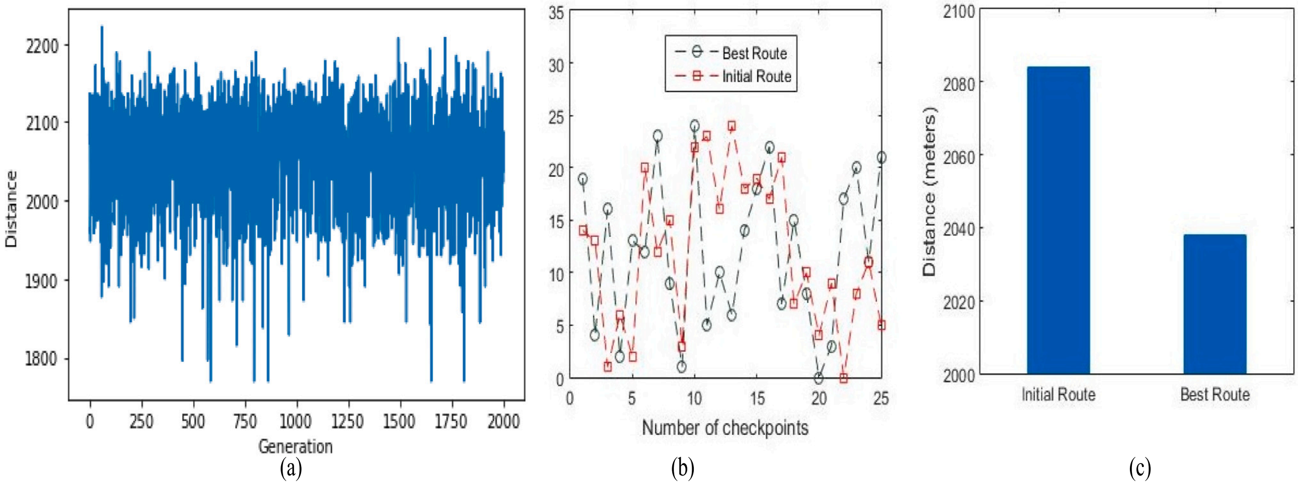

Fig. 7. (a) Randomly generated distance with respect to generation, (b) Comparison between route checkpoints, and (c) Comparison between route distance.

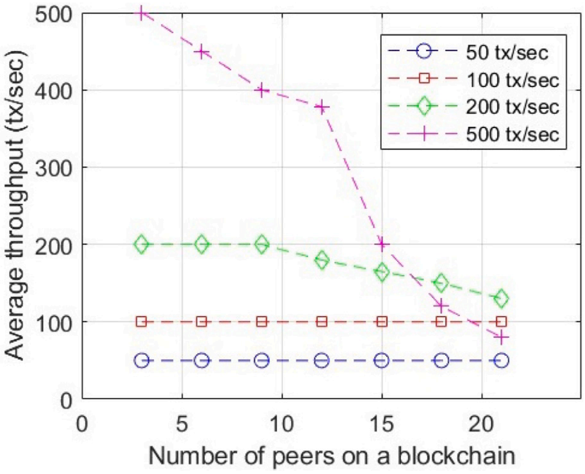

Fig. 8. Average throughput vs Number of peers on a blockchain.

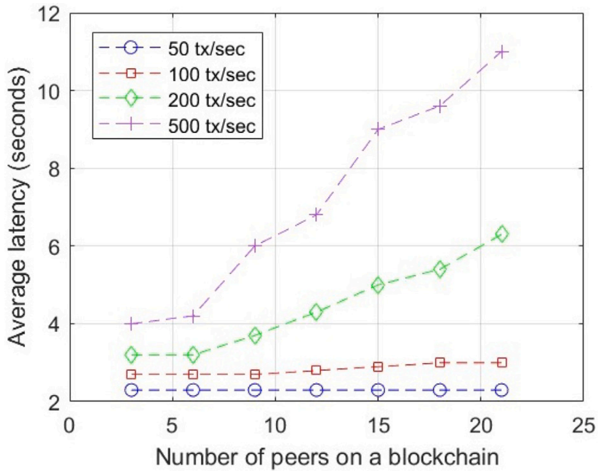

Fig. 9. Average latency vs Number of peers on a blockchain.

Acknowledgements

This work was supported by the Researchers Supporting Project number (RSP2024R32), King Saud University, Riyadh, Saudi Arabia. This research was also supported by the MSIT Korea under the NRF Korea (NRF-2022R1A2C4001270) and under the Convergence Security Core Talent Training Business Support Program (IITP-2024-RS-2024-00426853) supervised by the IITP.

References

[1] C. Lin, D. He, N. Kumar, K.-K.R. Choo, A. Vinel, X. Huang, Security and privacy for the internet of drones: Challenges and solutions, IEEE Commun. Mag. 56 (1) (2018) 64–69.

[2] H. Shakhatreh, A.H. Sawalmeh, A. Al-Fuqaha, Z. Dou, E. Almaita, I. Khalil, N.S. Othman, A. Khreishah, M. Guizani, Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges, IEEE Access 7 (2019) 48572–48634.

[3] A. Sharma, P. Vanjani, N. Paliwal, C.M.W. Basnayaka, D.N.K. Jayakody, H.-C. Wang, P. Muthuchidambaranathan, Communication and networking technologies for UAVs: A survey, J. Netw. Comput. Appl. (2020) 102739.

[4] P.K. Selvam, G. Raja, V. Rajagopal, K. Dev, S. Knorr, Collision-free path planning for UAVs using efficient artificial potential field algorithm, in: 2021 IEEE 93rd Vehicular Technology Conference, VTC2021-Spring, IEEE, 2021, pp. 1–5.

[5] J. Chen, C. Du, Y. Zhang, P. Han, W. Wei, A clustering-based coverage path planning method for autonomous heterogeneous UAVs, IEEE Trans. Intell. Transp. Syst. (2021).

[6] A. De Marinis, F. Iavernaro, F. Mazzia, A minimum-time obstacle-avoidance path planning algorithm for unmanned aerial vehicles, Numer. Algorithms (2021) 1–23.

[7] S. Aggarwal, N. Kumar, Path planning techniques for unmanned aerial vehicles: A review, solutions, and challenges, Comput. Commun. 149 (2020) 270–299.

[8] D. Mandloi, R. Arya, A.K. Verma, Unmanned aerial vehicle path planning based on A* algorithm and its variants in 3d environment, Int. J. Syst. Assur. Eng. Manag. 12 (5) (2021) 990–1000.

[9] Q. Wang, M. Xu, Z. Hu, Path planning of unmanned aerial vehicles based on an improved bio-inspired tuna swarm optimization algorithm, Biomimetics 9 (7) (2024) 388.

[10] A. Puente-Castro, D. Rivero, E. Pedrosa, A. Pereira, N. Lau, E. Fernandez-Blanco, Q-learning based system for path planning with unmanned aerial vehicles swarms in obstacle environments, Expert Syst. Appl. 235 (2024) 121240.

[11] S. Aggarwal, N. Kumar, S. Tanwar, Blockchain envisioned UAV communication using 6G networks: Open issues, use cases, and future directions, IEEE Internet Things J. (2020).

[12] S. Aggarwal, N. Kumar, M. Alhussein, G. Muhammad, Blockchain-based UAV path planning for healthcare 4.0: Current challenges and the way ahead, IEEE Netw. 35 (1) (2021) 20–29.

[13] A. Islam, S.Y. Shin, Bus: A blockchain-enabled data acquisition scheme with the assistance of uav swarm in internet of things, IEEE Access 7 (2019) 103231–103249.

[14] K. Gai, Y. Wu, L. Zhu, K.-K.R. Choo, B. Xiao, Blockchain-enabled trustworthy group communications in UAV networks, IEEE Trans. Intell. Transp. Syst. (2020).

[15] I. García-Magariño, R. Lacuesta, M. Rajarajan, J. Lloret, Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain, Ad Hoc Netw. 86 (2019) 72–82.

[16] A.Y. Javaid, W. Sun, V.K. Devabhaktuni, 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.

[17] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, M. Debbah, A tutorial on UAVs for wireless networks: Applications, challenges, and open problems, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2334–2360.

[18] R. Altawy, A.M. Youssef, Security, privacy, and safety aspects of civilian drones: A survey, ACM Trans. Cyber-Phys. Syst. 1 (2) (2016) 1–25.

[19] S. Aggarwal, R. Chaudhary, G.S. Aujla, N. Kumar, K.-K.R. Choo, A.Y. Zomaya, Blockchain for smart communities: Applications, challenges and opportunities, J. Netw. Comput. Appl. 144 (2019) 13–48.

[20] N. Kumar, S. Aggarwal, P. Raj, The Blockchain Technology for Secure and Smart Applications across Industry Verticals, vol. 121, Academic Press, 2021.

[21] I. Hasircioglu, H.R. Topcuoglu, M. Ermis, 3-d path planning for the navigation of unmanned aerial vehicles by using evolutionary algorithms, in: Proceedings of the 10th Annual Conference on Genetic and Evolutionary Computation, 2008, pp. 1499–1506.