

Article

Optimized Path Planning Strategy to Enhance Security under Swarm of Unmanned Aerial Vehicles

Kayalvizhi Manikandan *  and Ramamoorthy Sriramulu

Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203, India

* Correspondence: km3833@srmist.edu.in

Abstract: Unmanned Aerial Vehicles (UAVs) are widely deployed in military surveillance operations, especially the quadcopter UAVs which are easy to operate and considerably quieter. However, UAVs encounter problems in secure path planning during navigation and are prone to cyber security attacks. Further, due to the UAV battery capacity, the operating time for surveillance is limited. In this paper, we propose a novel Resilient UAV Path Optimization Algorithm (RUPOA) which provides an optimal path under security attacks such as denial-of-service (DoS) and Man-in-the-Middle (MITM) attacks. The performance efficiency of the proposed path planning algorithm is compared with the existing path planning algorithms based on execution time. To achieve secure path planning in UAVs and to mitigate security attacks, a blockchain-aided security solution is proposed. To prevent security attacks, smart contracts are generated where the devices are registered with gasLimit. The blockchain consensus mechanism allows for secure and tamper-free transmission of data between the Ground Control Station (GCS) and a swarm of UAVs. The performance efficiency of the blockchain model is evaluated based on network latency which is the total execution time across the blockchain network.



Citation: Manikandan, K.; Sriramulu, R. Optimized Path Planning Strategy to Enhance Security under Swarm of Unmanned Aerial Vehicles. *Drones* **2022**, *6*, 336. <https://doi.org/10.3390/drones6110336>

Academic Editors: Oleg Yakimenko and Xiwang Dong

Received: 26 September 2022

Accepted: 27 October 2022

Published: 2 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: unmanned aerial vehicles; secure path planning; cyber security attacks; Ethereum; smart contract

1. Introduction

Path navigation is one of the important problem areas to be researched in a swarm of Unmanned Aerial Vehicles (UAVs) for achieving the optimal path from the source to target. In the literature, there are many proposals for optimizing path navigation problems for a swarm of UAVs but still, there are many issues in optimal path navigation due to UAVs' high mobility. The focus of path navigation plans should consider an obstacle-free environment for UAV swarm operations. It should compute a secure path in the minimum time to ensure successful surveillance operations. The collision in path planning occurs during a search for a safe trajectory path. Analyzing drone movements helps them to reach the goal safely and avoid collisions en route. Different types of drones based on the rotor blade quantity are used for planning the navigation path. Multiple UAVs are employed in search and rescue operations [1], which is referred to as a Swarm of UAVs. For efficient path planning [2,3], multiple UAVs need to collaborate continuously. The process of planning a path to navigate is considered an elementary task for drones of different types. The task assignment and coordination process are carried out efficiently with the help of a base station or Ground Control Station (GCS) for managing UAVs. Both online and offline path planning of UAVs is possible. Path planning in UAVs can be achieved by meta-heuristic optimal path planning algorithms which provide an optimal path for navigating during a surveillance operation.

In three-dimensional path planning, the involvement of humans makes path planning more accessible, but in a few areas where humans are less capable, it is difficult to complete the surveillance operation. Three-dimensional path planning requires a three-dimensional workspace to help UAVs travel from source to destination easily. The optimized solution

of path planning has been analyzed from different perspectives by many researchers. The following is the list of steps followed in initiating path planning:

- (a) The search space is utilized differently from the grid map to another point.
- (b) An algorithm's deterministic or non-deterministic solution helps formulate the arrangement from source to destination without having any conflict path.
- (c) In real-time execution, UAVs produce a flight trajectory from the obtained path.

Several applications from various domains use UAVs as an emerging technology. For UAV navigation [4], real-time optimization for training neural networks and achieving optimal paths is considered useful for various applications [5–7]. UAVs are used in multiple environments such as disaster management [8], intelligent cities and surveillance [9,10], power line inspection [11], remote sensing and package delivery [12,13], wind turbine inspection [14], agriculture, firefighting, and traffic surveillance [15,16].

The flight and drone safety management process are managed by monitoring, controlling and automating flight operations. The secure integration of UAVs in managing drones was established by an initiative of the National Aeronautics and Space Administration. Even the flight path of small UAVs is regulated by the UAS traffic management plan for path navigation. The safe operation of multiple UAVs is managed with the help of the UTM pilot program by the US Federal Aviation Administration. The UAS pilot program also supports low-level navigational safety management for unmanned aircraft systems (UAS). Network communication creates numerous challenges and hindrances in providing efficient path planning for UAVs. Based on the Internet of drones and UAVs, many researchers have conducted studies to address the challenges of UAVs [17].

Using Internet web services, UAVs have been monitored by a UAV map planner that enables the remote-controlled operation of UAVs. Various research on UAV path planning has focused on the energy consumption of UAVs [18]. Numerous security issues were identified for a swarm of UAV operations and were addressed using different security mechanisms. The complex optimization problem in path planning was solved with the help of a swarm of metaheuristic algorithms. Compared with other algorithms and mathematical programming, the metaheuristic algorithm is regarded as one of the best algorithms because of its wide applicability [19,20]. The two main features of the metaheuristic algorithm are intensification and diversification [21]. While the diversification phase provides a solution for efficient utilization of search space, the identification phase offers the best solution for path planning problems. To solve large problems in a faster manner, metaheuristic algorithm can be used to achieve a robust method [22].

Nature-inspired algorithms are popular in resolving optimization issues. Physics-inspired charged systems and music-inspired harmony search depend on metaheuristic algorithms [23,24]. A naturally inspired algorithm is classified as a biologically-inspired algorithms.

Over the last few years, nature-inspired algorithms have been used to determine an optimal path between the starting position and the target point. The navigation path designed for UAVs should be free from obstacles and collisions. In addition, secure path planning for managing UAVs must primarily include the factors navigation, trajectory planning and motion planning. During path planning, automated UAVs are involved in planning an accurate path that satisfies these factors.

On the other hand, collision avoidance and trajectory planning must be calculated efficiently in the path navigation process. Path planning is made possible in a complex environment with the help of a three-dimensional view. As the obstacles in path planning are not identified using a two-dimensional method, a three-dimensional approach to path planning is considered. Further, in a complex environment, surveillance and navigation of a path demand a three-dimensional path-planning technique [25]. Automated UAVs decide their path on their own and are operated in a challenging high-mobility environment [26].

The main contribution of this study is to examine existing nature-inspired algorithms and find the gaps in achieving optimal paths under uncertain dynamic environments and securing the UAV swarm network. The nature-based algorithms are mostly devised

from the evolution of swarm behaviours. Therefore, for a successful deployment of UAVs in military surveillance operations, both the security and optimal utilization of the UAV resources to achieve an optimal path should be considered. This paper focuses on providing a solution for achieving both optimal paths and securing the communication of UAV swarm networks from cyber security attacks such as MITM and DoS by utilizing solutions from blockchain.

This paper includes the following sections. In Section 2, existing works in path planning and the need for security in UAVs are discussed. Sections 3 and 4 discuss the proposed RUPOA algorithm and the blockchain model. Section 5 discusses securing UAV networks from security attacks. In Sections 6 and 7, the simulation setup and experimental results of the proposed algorithm are illustrated. Section 8 provides conclusions on the proposed work and its performance.

2. Existing Works

In this section, the existing works on finding an optimal path for a swarm of UAVs using nature-inspired metaheuristic algorithms for path navigation are discussed.

UAVs deployed for military surveillance operations operate under dynamic environments with many uncertain factors such as environmental changes, moving obstacles, lightning, collision with other UAVs, terrain features and so on. Therefore, the UAVs need a system that allows them to use resources efficiently and monitor their activities throughout the surveillance operations. While operating in a high mobility dynamic environment, many obstacles are encountered during surveillance operations.

UAV communication links are more prone to security issues and vulnerabilities. One of the major drawbacks of UAV communication is data leakage where the attackers probe UAV systems and eavesdrop on the communication channel for sensitive data. Researchers have used trajectory design to address the eavesdropping problem [27]. Communication through Raspberry Pi was considered an efficient method of secure path planning through UAVs. An unexpected attack in the travelling path of the drone was managed with the integration of Raspberry Pi to secure the path. However, the performance of the approach using Raspberry Pi was not analyzed to prove its efficiency. Implementing the MAC Protocol helps address the challenges caused by waypoint alteration and path modification [28]. Further, the communication between the UAV and base station and among the UAVs must be secured. The major field of UAVs is military surveillance, due to their portability and utility for stealth operations so the data shared in the UAV swarm network should be free from security vulnerabilities [29]. The communication links should also be secured, which can be achieved using blockchain that helps protect the integrity of data shared in the network [30].

To determine the feasible path from source to destination, many different planning systems have been implemented using nature-inspired meta-heuristic algorithms. Various kinds of issues in the network have been addressed using meta-heuristic algorithms, and many methods were studied for finding the shortest path [31]. Compared with other algorithms, the meta-heuristic algorithm results in a shorter travel time from source to destination and helps to achieve a close to optimal path.

The following algorithms provide the same output as the meta-heuristic algorithm in the implementation of both two-dimensional and three-dimensional operations:

- Particle swarm optimization [32–34]
- Whale optimization algorithm [35]
- Sine cosine algorithm [36]

Neural network training, image segmentation, and numerical function optimization [37] show improved performance in real-world problems. The metaheuristic algorithm integrated with Grey Wolf Optimization [38] was extended to implement 3D path planning of multiple UAVs.

UAV path planning performance can be improved with the implementation of a genetic algorithm which considers large-scale path planning of UAVs. The Gale–Shapely

algorithm integrated with the genetic algorithm helps the area coverage during simulation processing. The researcher proposed path planning and task assignment through an analysis of an energy-efficient system. The Gale–Shapely algorithm helps to address the issue caused by the task assignment problem. Data was collected from the nodes using the Hamiltonian Path. In UAV path planning, the brute force search technique is an effective method of UAV path planning. In a small number of possible states, the brute force search technique analyzes a problem without requiring specific knowledge of it.

Among nature-inspired algorithms, the Ant Colony Algorithm (ACO) can be used to find solutions where the parameters are chosen from values of a finite set. It chooses a value from a set of finite values to maximize the objective since the problems are NP-hard where the performance degrades when the problem is complex. ACO focuses only on selected regions and does not cover the entire search space.

Many researchers have focused on the Grey Wolf Optimization (GWO) algorithm. The behaviour of the Grey Wolf algorithm was optimized based on social leadership and hunting in nature. Exploration is the significant phase of a metaheuristic algorithm. The UAV nodes are grouped into alpha and beta. Beta provides accurate feedback on the decisions made by the alpha group and helps in making correct decisions in path-making. The shortest UAV planning path was achieved using a deployment scheme considering the navigation parameters under a dynamic environment. The load and scanning bandwidth were used to evaluate the UAV path using clustering analysis. The path of the algorithm was optimized by using the improved PSO algorithm. The research on classification proves that omega can be considered a minor fitness classification in GWO. Alpha was regarded as one of the best fitness solutions in GWO. During navigation, the UAVs could not follow the path laid by the sharp retrieval path provided by GWO. The polynomial functions used for vehicular mobility were used for improving the speed of the vehicle. The campaign results were calculated based on successful deviates of the polynomial. The initial phase of path planning sub-points was generated based on the trajectory formation of the vehicles. Avoiding barriers or sharp turns in the path was achieved by using sub-points in the closed path. The smoother projection path planning was achieved with the help of a fifth-order polynomial.

To solve a particular problem, comparing the physical properties of the metaheuristic algorithm is considered a challenging task in stabilizing the right direction. The Ant Colony (ACO) Algorithm, Whale Optimization Algorithm (WOA), Dijkstra, A* and deterministic algorithms are for low-level navigation of UAVs. Table 1 shows a summary of nature-inspired swarm algorithms, their search behaviour and their limitations.

Table 1. Summary of existing swarm algorithms.

Algorithm	Author	Search Technique	Limitations
Grey Wolf Optimization (GWO)	[39,40]	Search prey and hunting	Enormous number of parameters
Ant Colony Optimization (ACO)	[41]	Mutation and Selection	Time-consuming in the communication medium
Whale Optimization Algorithm (WOA)	[42]	Bubble-net foraging	Low solution accuracy
Bee Colony Algorithm (BCA)	[43]	Mutation and selection	Not able to provide complete optimal solution
Bat Algorithm (BA)	[44]	Emission of pulse rate and loudness	Enormous number of control parameters

The swarm behaviour algorithms consist of the Grey Wolf Optimization (GWO) algorithm, Ant Colony Optimization Algorithm (ACO), Whale Optimization Algorithm (WOA), Bee Colony Algorithm (BCA) and Bat Algorithm (BA). The main scope of these algorithms is to adapt the natural behaviour in finding optimal solutions to real-time complex problems. However, each algorithm focuses on environments with a single objective space and

the number of parameters considered for an optimal path is excessively large, creating an additional overhead in pathfinding for UAVs in dynamic environments. Most of the existing algorithms maintain a routing table of the neighbour nodes and provide an optimal path. Mostly the routing table tracks the neighbour node hop count. If the nodes in the chosen optimal path encounter any security attacks, the optimal path is compromised, and the integrity of the network is lost. Therefore, in the proposed algorithm, the routing table maintains additional parameters specific to the UAV position and energy consumption, which helps to track the position of all the UAVs under a dynamic environment and ensures that only the authorized UAVs registered in the smart contract operate in the network.

The UAV network also needs to be secured [45]. Since the data transfers are performed in real-time they are more prone to security attacks. Many services for the management of drones and their traffic are designed in network systems which face many challenges during navigation. The existing systems mainly focus on using cryptographic keys to encrypt and decrypt data, but the UAV system requires a more standard security mechanism for ensuring data security. The third-party authority's dependence on public-key cryptography is considered a challenge in the implementation. The computation and memory storage of the system are not considered in the performance of the secure path. Still, those factors must be included for efficient algorithm implementation.

Additionally, blockchain helps to protect the data shared in the network. The utilization of drones with blockchain technology is improved due to the nature of blockchain functionalities implemented in the path optimization of UAVs. Therefore, the proposed algorithm provides a solution to achieve an optimal path in less time and secure the communication link in the UAV network. To secure the UAV network from security attacks, a smart contract is initially used to register the UAVs. Each UAV is assigned with a particular gasLimit which denotes the resource capacity of the UAV. If the UAV exceeds its gasLimit, it is no longer functional in the UAV network. If a UAV is compromised and acts as a threat actor, it needs to consume gasLimit to launch a successful security attack. The performance of the drone with blockchain is analyzed based on the security mitigation rate. The data collected in the drones could assure integrity by using a new framework that integrates cloud storage with blockchain for efficient implementation. The UAV path's safety and privacy were guaranteed with blockchain technology's help.

3. Proposed Secured Blockchain Model for Optimal Path Planning in UAV Swarm

The nature-inspired meta-heuristic algorithm is used to provide an optimal path in the swarm of UAVs. When operating as a swarm, the UAVs encounter many obstacles which degrade the network performance. The algorithm proposed is inspired by swarm algorithms that provide an optimal path, and when used with the combination of the blockchain consensus algorithm, the communication and data are also secured in the network.

Figure 1 shows the proposed network layout of UAVs operating as a swarm. When UAVs are operating in a swarm in a real-time dynamic environment, the distance between the UAVs and their position needs to be updated in real-time to find the optimal path, and when the surveillance course of action changes, the UAV swarm network should be capable of adopting the change of course without any degradation in the network performance.

The existing path-planning algorithms focus on exploitation rather than the exploration of the search space. Thus, the existing nature-inspired algorithms are not feasible for generating optimal solutions in a dynamic search space. Inspired by the existing swarm algorithms such as the ACO, GWO, WOA, BCA, and BA, our proposed algorithm Resilient UAV Path Optimization Algorithm (RUPOA) derives the fitness function by calculating the energy level of each UAV node, which is based on the path length of a UAV node under dynamic conditions. Figure 2 presents the proposed system model, where the secure path planning is performed utilizing the blockchain consensus algorithm, and the PBFT Smart contracts are generated where the UAV nodes are registered with gasLimit. The complete activity of each of the nodes is shared with its neighbouring nodes and a routing table is generated for each node. The routing table consists of details of the neighbouring nodes,

their position, node_ID, and authorized certificates, which assure the nodes are registered in the network. Therefore, by maintaining the complete activity details of the neighbouring nodes, any malicious nodes or compromised nodes can be easily identified and removed from the network.

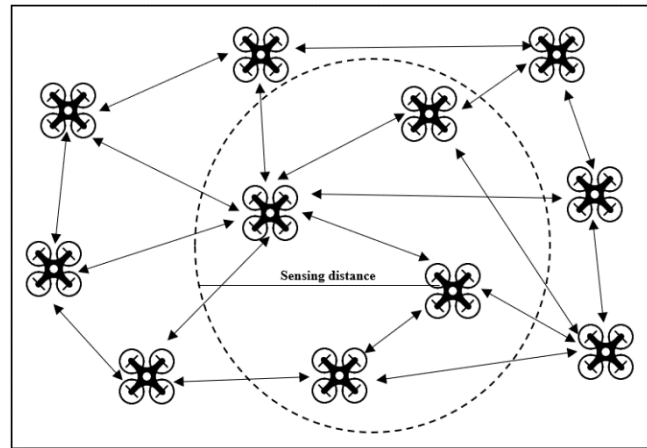


Figure 1. UAV swarm network.

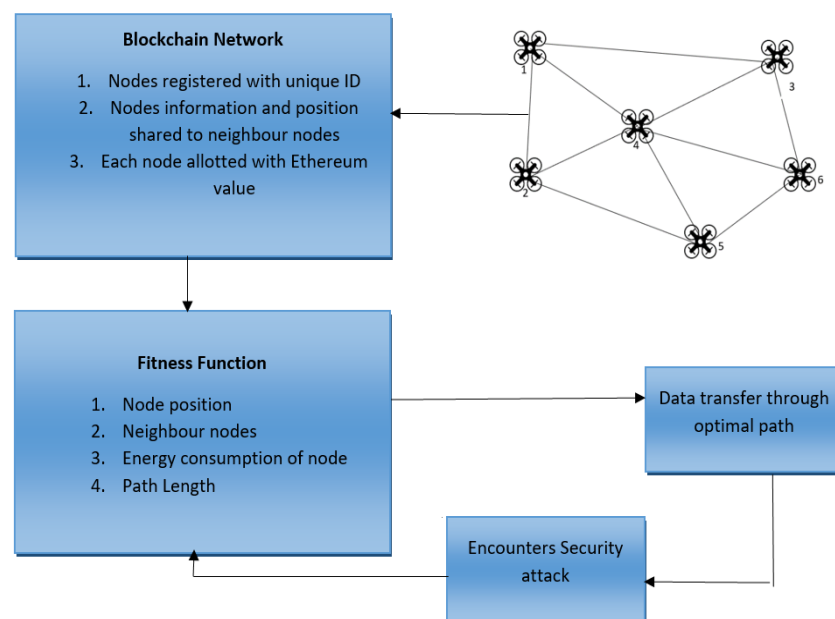


Figure 2. Proposed system model.

The blockchain network model allows authorization of the UAV nodes in the network and secures the communication from attackers. Ethereum usage, which is growing rapidly, allows decentralized applications and smart contracts to be developed in blockchain incorporating its features. The data such as node position and neighbouring node details are tracked as the node's position changes dynamically during the surveillance operation. The smart contracts bind the nodes in the network and authorize each node and its certificate to verify its legitimacy. A gasLimit is assigned to each node in the network which denotes the maximum capacity of resources that it can handle. Whenever a node performs any action, its gasLimit is reduced. By assigning a gasLimit for each node, security is assured, whereby a node consuming its full gasLimit indicates that the node is under attack or compromised.

The proposed secured model uses Ethereum for authorizing the nodes in the swarm network and implements a blockchain smart contract. The smart contract allows identification of the trusted and malicious devices in the network. Initially, in the UAV swarm

network, the UAV nodes are registered in the system and each node is assigned a gasLimit. Once the registration is complete, each device is authenticated with a unique ID and the assigned gasLimit is the resource allotted to the node. The communication among the UAV nodes and between the UAV and base station are monitored and authorized by the smart contract managed by the server node. The allotted gasLimit in each node is set which is used to prevent security attacks such as DoS.

For secure communication in the UAV network, a smart contract is deployed in the server node. Here in this paper, it is assumed that the trusted nodes are server nodes. All the UAV nodes in the network are registered in the smart contract. Only the trusted server node can authorize the UAV nodes to be added or removed from the network, so any new node that needs to be added to the network is authorized by only the server node. Once the nodes are registered in the network, the node's identity is managed by the smart contract which helps it to track the activities of the nodes. When any node encounters a security attack or if the server suspects any malicious activity in a node, the server can remove the node from the network, which secures the UAV network from security attacks.

4. Resilient UAV Path Optimization Algorithm (RUPOA) Methodology

The main concern in the existing algorithms is that they are not feasible for providing an optimal path under uncertain dynamic environments when the nature of operations is not stable and the network encounters uncertain natural factors such as wind or smoke, or faces security attacks on communication links. Here, the proposed algorithm RUPOA helps to achieve an optimal path and secures the communication among UAVs and UAV-to-GCS.

Figure 3 shows the proposed flow diagram for finding the optimal path for a UAV based on the proposed RUPOA. The Algorithm 1 which is proposed, generates the optimal path for a swarm of UAVs. The main drawback of the existing methods is that the UAV network generates an optimal path, but if the nodes of the generated path encounter any security attacks, the optimal path is compromised and the whole UAV operation fails. The proposed system initially generates an optimal path, and if any of the nodes are under security attacks, the proposed algorithm automatically generates the next optimal path by removing the attacked node from the network and keeping the system secure. Initially, the UAV node's details such as node position, neighbour nodes and energy consumption are collected and secured using blockchain smart contracts.

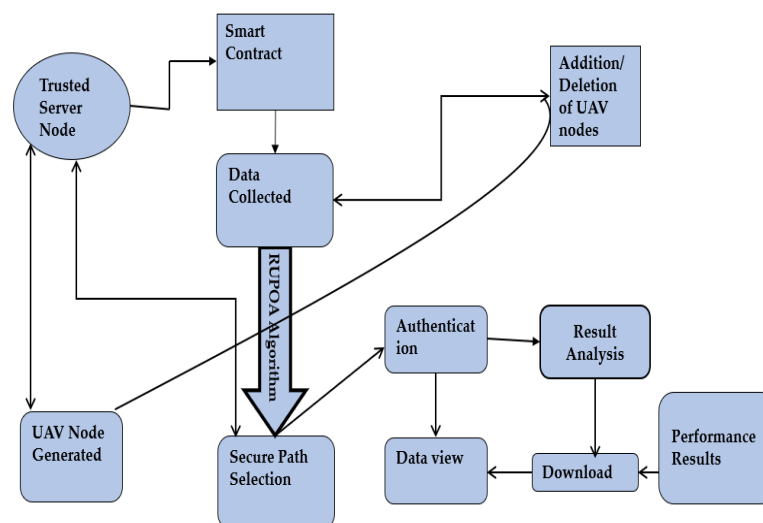


Figure 3. Flow of secure path planning.

Algorithm 1: Resilient UAV Path Optimization Algorithm (RUPOA)

```

1. Initialization of the node parameters: Nmax, Dmax, etc.
2. for k = 1 to P do
3.   for l = 1 to t do
4.     Xk,l = 1 + rand mod M, Memory initialization
5.     y = Turns, PL (i,j), z
6.     Define population size (p), neighbours list (NL), energy (E)
7.   end for
8. Evaluate fitness function for each node
9. end for
10. Find Xbest
11. while N = Nmax do
12.   for k = 1 to P do
13.     Perform the fitness Calculation
14.     xi(l + 1) = xi(l) + y + PL(i,j)
15.   end for
16.   for k = 1 to P do
17.     Perform exploration
18.   end for
19. Find best solution
20. Sort and find xbest, where best ∈ (1, 2, . . . , S)
21. N = N + 1
22. If xbest = y
23.   Find xbest + 1, where best ∈ (1, 2, . . . , S)
24. Return xbest1
25. end while
26. Return xbest

```

The algorithm incorporates a genetic reproduction mechanism to enhance the performance. The classically used algorithm was replaced by adaptive genetic reproduction with crossover and mutation. The global optimization efficiency strategy was performed with a crossover operator's help. The further development of an algorithm was accomplished with the help of a vectorized vision of crossover. Binomial and exponential are the two ways used for determining the crossover probability. The evolutionary mutation algorithm controls mutation probability. Various benchmark algorithm problems were validated to improve the algorithm's efficiency. According to the well-known function, the benchmark of the problem was identified as low or high. A single run was unable to judge an algorithm's performance due to the random nature of the metaheuristic algorithm.

The performance of the approach was improved with many trials based on independent population initialization. To find the number of nodes in the planned path is to find the probabilistic feasibility of UAVs. The risk level in the simulation is denoted by each obstacle X that gives a chance for each constraint μ .

$$f(x) = 1/(2\pi) d/2 \sum | 1/2 \exp[-1/2(X - \mu)] \quad (1)$$

The probability of avoiding collision by static or dynamic obstacles is determined by calculating the possible region of X_{ti} , where for each dynamic block, i random number is generated to represent the centre location, and the UAV position by each step is represented as t . The risk domain data and risk level are defined by an alpha symbol. The equivalent deterministic constraint is converted into a probabilistic control by applying a different formula. The introduction of relative uncertainty helps to address a common form of uncertainty problem with UAVs that is solved with the following equation:

$$D_{xt}/d_t = N_t + F_t + D_t \quad (2)$$

The n -dimensional space is determined using an n -dimensional decision space which helps to reduce space by using an optimization algorithm that consumes less energy. The

UAV node is represented using the iteration variable D_t for physical diffusion, and the UAV's foraging motion is represented by F_t . Neighbour UAV nodes are represented by N_t . The mutual effects of the algorithm are maintained by using a high density of UAV individuals based on theoretical arguments.

5. Securing UAV Network from Security Attacks

The proposed blockchain network defends the UAV swarm network from security attacks such as denial-of-service, man-in-the-middle, Sybil and wormhole attacks. The focus is to authorize the UAV nodes in the network and make the network resilient under security attacks. This can be achieved by authorizing the UAVs and then allowing the UAVs to consume resources based on the allotted gasLimit. The blockchain smart contract ensures that only the authorized nodes are allowed to be operated in the network. Even if an attacker UAV tries to intrude into the network, it needs to consume all its energy and resources to successfully launch security attacks in the UAV swarm network. This is because all the UAVs are authorized by registering in the smart contract and the neighbour UAVs need to reach consensus to accept the new UAV node into the network. As a result, the attacker UAV must consume all its resources in order to be authorized into the UAV swarm network.

5.1. Denial-of-Service (DoS) Attack

The most common security attack that affects UAV networks is the DoS attack, which can drain the UAV resources completely and compromise the network. The proposed model addresses this security attack when a UAV node sends data to overload the network and consumes maximum resources. As shown in Figure 4, a node in the UAV network bombarding the server with false data in a DoS attack can be prevented by the gasLimit assigned to each node. This is because once the node once reaches its gasLimit, it cannot accept any more data. In our proposed blockchain model, the gasLimit assigned to each node prevents the node from consuming data when it exceeds the gasLimit. Therefore, by this method, the system can never be overloaded with data or the resources drained. Further, any attempted DoS attack that tries to drain the system resources cause the malicious node to drain its own resources and become disconnected from the network. Thus, once the gasLimit is utilized to its maximum or drained, the malicious node activity is automatically terminated, and the system is prevented from unwanted data overloading.

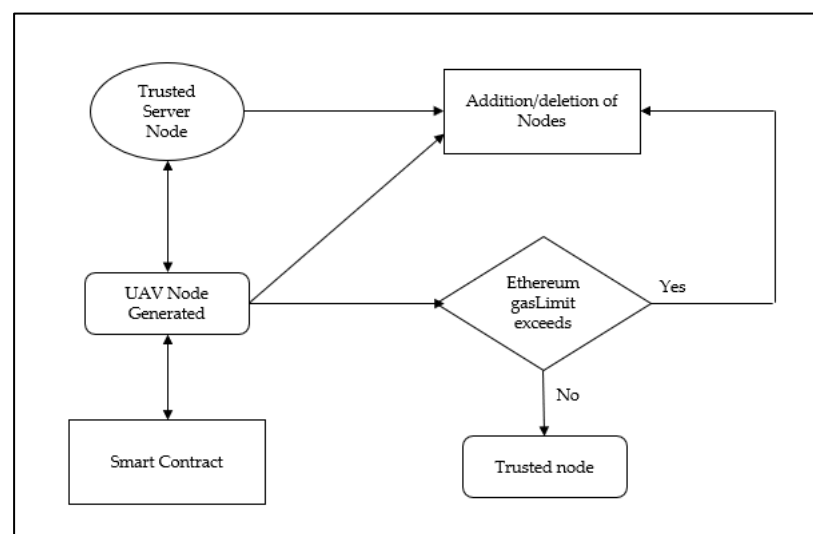


Figure 4. Proposed blockchain Ethereum gasLimit model.

5.2. Man-in-the-Middle (MITM) Attack

Nowadays, UAVs are extensively deployed in all areas; however, they are specifically used in military services for weather monitoring, rescue, and stealth operations. Compared with manned aircraft, UAVs have more advantages in terms of efficiency and adaptability but still come with some limitations. The fundamental drawback is that UAVs have limited ability to cope with uncertain factors and are more vulnerable to command-and-control attacks, as depicted in Figure 5.

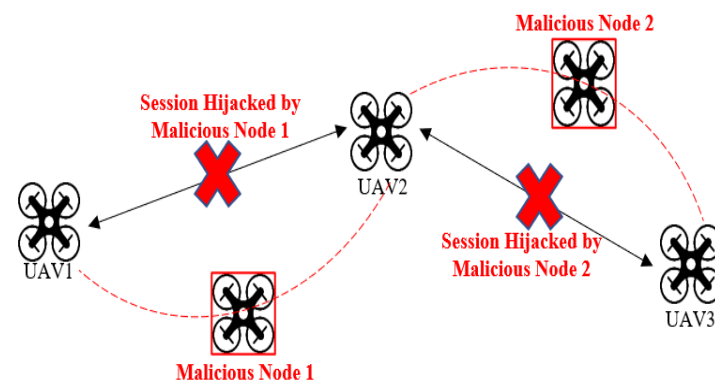


Figure 5. MITM attack on UAVs.

The most common attack is the injection of malicious payload in the Ground Control Station (GCS) where the successful injection of code leads to session hi-jacking attacks in which the entire operation can be compromised. UAVs are more prone to wireless attacks. They are more vulnerable to man-in-the-middle attacks and command injection, allowing the attackers to take control of the drone. Security flaws in commercial drones can allow an attacker to take control of it using open-source tools. UAVs controlled by WIFI employ IEEE 802.11 standards. The communication link between the base station and the UAV via Wi-Fi network is vulnerable to cyber-attacks. UAVs can be hijacked by performing MITM. For a successful MITM attack, Remote commands need to be used. The attacker can internally change the configuration settings of the UAV and hijack the session. For successful remote command execution, the attacker must be aware of any of these parameters such as Network ID, Baud Rate, destination address high (DH), destination address low (DL) with which the attacker can launch a successful MITM attack. Therefore, the MITM attack can be prevented by our proposed blockchain model where if any attacker node is trying to enter the network, the node needs to be authorized by the smart contract. As the UAV nodes are already registered in the network and for each node, a Node_ID is generated to authorize itself in the UAV network. So, any external node trying to join the network will drain its resources and based on the blockchain consensus mechanism, the external node will be automatically rejected from the network.

5.3. Worm Hole Attack

Figure 6 describes the wormhole attack also known as the tunnelling attack. This attack is achieved by compromising one or two nodes, to tunnel the data. And by tunnelling, the malicious node tries to steal the data from another node. The proposed blockchain model detects this attack when there is a change of activity in the UAV network. Since the server node is capable of adding/removing the UAV nodes in the network, it monitors the activity of all the registered nodes in the network.

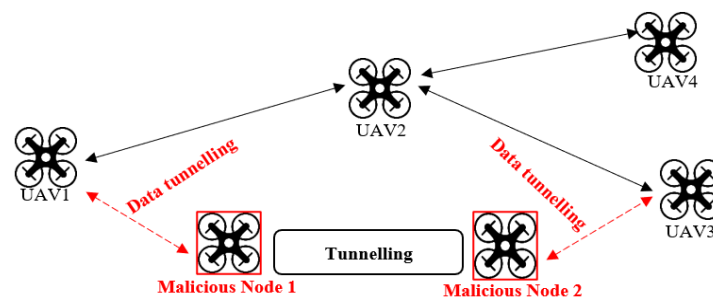


Figure 6. Wormhole attack.

Thus, even if an attacker node is added to the UAV network, its resources are drained due to the assigned gasLimit during the tunnelling and it is automatically rejected from the network.

5.4. Sybil Attack

In a swarm of UAV networks, a Sybil attack uses fake authorizations within the UAV swarm network. This attack is successfully executed when the fake node tries to influence the network and gains the consensus of the majority of the nodes in the network. However, in our proposed work, the nodes identified are verified by the trusted server node which authorizes the identity of the node when it is deployed in the network, and each node is registered and authenticated in the network. Therefore, if an untrusted node is trying to join the swarm of the UAV network, it needs to be authorized by the server using the established Ethereum smart contract. Even though the node is added to the network, due to the allotted Ethereum gasLimit, the malicious node drains its resources and becomes unable to obtain the consensus of the majority of the nodes.

6. Simulation Setup

Simulation cases were designed based on different stages to verify the probabilistic feasibility. Stage one consists of choosing the nodes in the planned path. The risk level in the simulation is denoted by parameter α every time step t for each obstacle given a chance for each constraint. Stage two in the simulation depended on random trial validations. For each dynamic block, the random number i was generated to represent the centre location, and the vehicle for each step is represented as t . Each real obstacle located in the centre i was generated randomly to check the planned path of the UAV. The risk level for each step t is represented by generating random numbers. According to the risk level, the α current case random test was repeated several times. The total number of hurdles is based on static uncertain and deterministic UAVs. Better performance in path planning is achieved with the help of the proposed RUPOA. The better route in the planning space was provided by selection and cross-over operations which help to find the right optimal path under security attacks. The dual population search iteration technique was used to improve the single population in search iteration. The most significant factor for the nodes with its nearest target is represented $n_{ij} = 1/dy$, which allows it to select the next nearest node from the routing table when the neighbour node is under security attack. Denial of service and distributed denial of services (DDOS) were the different types of attacks considered in the path planning of UAVs. Most of the resource consumption and overload problems servers are caused by DDOS. The use of Ethereum helps to address the issue of managing the resources within the limit. For the simulation environment, Ubuntu Linux 22.04.1 was used as an operating system. The simulated environment was entirely built in Java 1.8.0_202, and the entire swarm of the UAV network topology was generated using the class files and importing weka classifiers. Ethereum gasLimit is used to set up the node resource level. The interaction between the device and server is initiated using a simulation process.

Different parameters were used to calculate the efficient path for UAVs: α denotes the risk level, and the value was assumed to be 0.05; and t represents varying time for each path iteration. The subsidiary population size of the proposed RUPOA is represented

by P , and the total number is represented by the parameter n . In the reproduction pool, each individual is represented by the parameter s from each population. According to the category and individual size, new individual s is evaluated. The population parameters are represented by αA , βA , MA , αB , βB , and MB when determining the maximum and minimum values to achieve an optimal path.

7. Simulation Results

The simulation results are compared when the execution time taken for the proposed algorithm is optimal compared with the existing algorithms. The results are presented in this section. Considering the experimental setup, the GUI was developed in Java with the machine learning packages `weka.classifiers` for simulating the proposed methodology and the results are compared. In Figure 7, the UAV network is simulated with 50 UAV nodes and the results of secure path planning are compared. Figure 8 shows the secure optimal path generated from the inputted source and destination values. From the optimal path generated from source node 8 to destination node 40, the secure optimal path is [8,21,27,40]. When the UAV swarm operates in an uncertain dynamic network, node 21 encounters a man-in-the-middle attack, as depicted in Figure 9. Based on the proposed blockchain model, the server removes the malicious node from the network, chooses the next trusted neighbour node and generates a new optimal path [8,17,27,35,40]. The proposed RUPOA algorithm maintains a list of all its neighbour nodes, which are registered in the UAV network using the blockchain smart contract. Thus, each node is identified in the network and achieves non-repudiation. The proposed RUPOA algorithm calculates the fitness function value, which provides all the available paths for each node and its neighbour nodes. The algorithm also provides the optimal path based on the neighbour node position, path length and energy consumption of each path, and the optimal path is achieved with fewer parameters. Thus, each node in the UAV network maintains a routing table which contains the details calculated from the fitness function, and the RUPOA algorithm generates the optimal path. Each node's identity is secured based on its assigned blockchain smart contract and `gasLimit` so it achieves non-repudiation. When the network encounters security attacks such as MITM, DoS, wormhole or Sybil attacks, the malicious node resource is drained and it exceeds the `gasLimit`, which automatically removes it from the UAV network. Then the next neighbour node is selected that provides the next best optimal path, as represented in Figure 4.

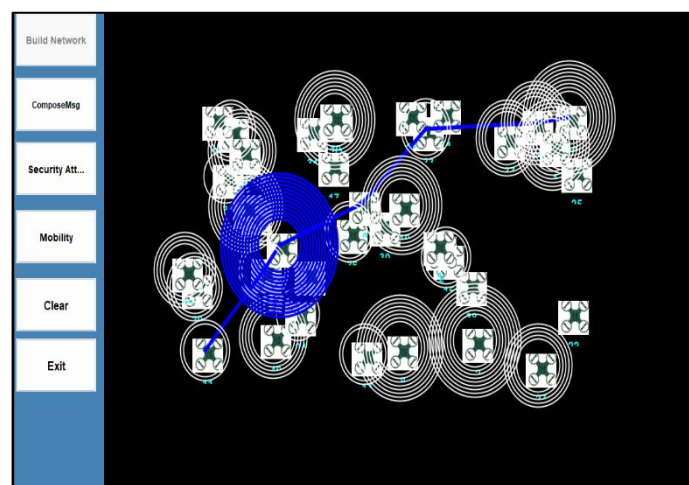


Figure 7. UAV swarm network of 50 nodes.

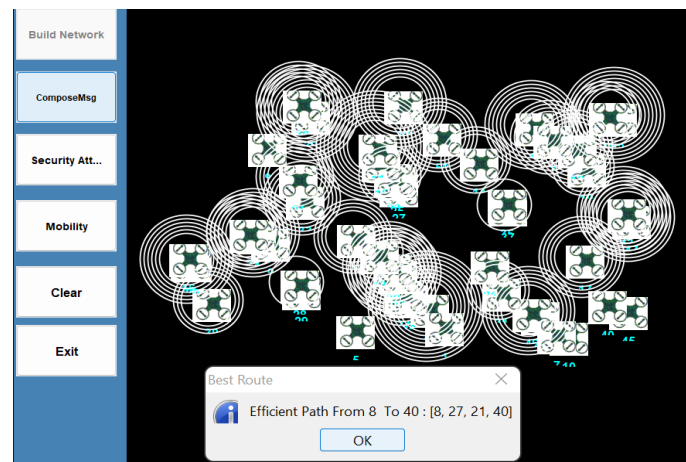


Figure 8. Secure optimal path from source to destination.

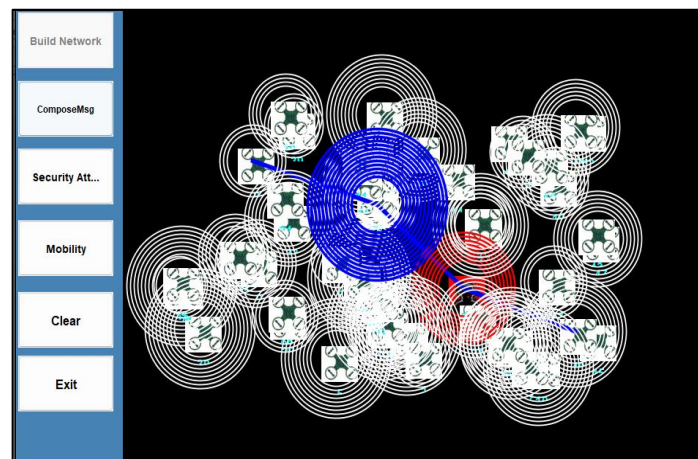


Figure 9. Attacked node removed from UAV swarm.

The experimental results are shown in Table 2. The proposed RUPOA using blockchain Ethereum smart contracts secures the swarm of UAV networks from security attacks and provides a secure optimal path under security attacks performed under multiple iterations. The results are generated with an increasing number of UAV nodes (20, 30, 40 and 50 nodes) where the proposed model can achieve optimal path under security attacks and show scalability.

Table 2 shows the execution time taken for the proposed algorithm and the results are compared with the existing works. From the results, the execution of the proposed algorithm is optimal when compared with the existing works.

The data values are generated from the simulation results where the optimal path is provided based on the energy consumed by the nodes. If the distance between two nodes is longer, then the energy consumption is high. Therefore, the optimal path is chosen based on a shorter neighbour node path length, and the optimal path is the most energy-conserving path.

The results in Tables 3 and 4 show the execution time taken for the attack mitigation and secure path selection and the energy consumed from source to destination. From the simulation results shown in Tables 3 and 4, the energy consumed by the proposed algorithm is less compared with the existing algorithms. The attack mitigation rate in Table 5 shows that the proposed RUPOA is effective under dynamic environments for a swarm of UAVs.

Table 2. Proposed RUPOA optimal path performance results with increasing numbers of UAVs.

No. of UAVs	Input Parameter		Optimal Path	Energy Consumption (Joules)	Security Attack	Resilient Optimal Path	Energy Consumption under Security Attack (Joules)
	Source	Destination					
20	1	18	1, 14, 6, 18	0.096	Man-in-the-Middle attack	1, 14, 16, 18	0.099
	9	20	9, 17, 3, 2, 20	0.097	Denial-of-Service	9, 17, 12, 10, 19, 20	0.098
	8	13	8, 7, 2, 10, 13	0.098	Wormhole attack	8, 11, 20, 19, 13	0.098
	6	17	6, 3, 17	0.096	Sybil attack	6, 16, 12, 17	0.099
30	2	26	2, 28, 26	0.097	Man-in-the-Middle attack	2, 10, 4, 26	0.099
	3	10	3, 11, 10	0.098	Denial-of-Service	3, 1, 17, 10	0.099
	7	25	7, 17, 23, 25	0.096	Wormhole attack	7, 21, 18, 20, 25	0.099
	6	22	6, 10, 22	0.097	Sybil attack	6, 11, 10, 22	0.098
40	2	22	2, 18, 3, 22	0.096	Man-in-the-Middle attack	2, 18, 26, 22	0.099
	4	35	4, 40, 35	0.096	Denial-of-Service	4, 36, 35	0.098
	3	24	3, 6, 27, 24	0.098	Wormhole attack	3, 1, 2, 30, 24	0.099
	8	39	8, 38, 39	0.096	Sybil attack	8, 6, 39	0.097
50	8	40	8, 27, 21, 40	0.097	Man-in-the-Middle attack	8, 27, 35, 17, 40	0.099
	5	24	5, 46, 24	0.096	Denial-of-Service	5, 2, 22, 24	0.097
	12	39	12, 14, 15, 35, 39	0.098	Wormhole attack	12, 14, 20, 39	0.099
	25	48	25, 37, 48	0.096	Sybil attack	25, 22, 48	0.099

Table 3. Comparison of execution time.

Algorithm	Execution Time for Attack Mitigation (s)	Execution Time for Path Selection (s)
RUPOA	0.098	0.98
Grey Wolf Algorithm	0.83	7.34
Ant Colony Algorithm	0.74	8.54
Whale Optimization Algorithm	0.67	8.04
Bee Colony Algorithm	0.62	7.7
Bat Algorithm	1.42	1.55

Table 4. Comparison of Energy Consumption.

Algorithm	Energy Consumption (Joules)	Energy Consumed under Security Attack (Joules)
RUPOA	0.08	0.098
Grey Wolf Algorithm	0.54	0.64
Ant Colony Algorithm	0.56	0.64
Whale Optimization Algorithm	0.74	0.97
Bee Colony Algorithm	0.50	0.64
Bat Algorithm	0.82	0.96

Table 5. Attack mitigation rate in proposed model.

Algorithm	Attack Mitigation Time in the Proposed Model (s)
Man-in-the-Middle attack	0.098
Wormhole attack	0.98
Sybil attack	1.9
Denial-of-Service attack	9.7

Figure 10 illustrates a comparison of the average execution times of the proposed and existing algorithms. The values are calculated for an increasing number of UAVs (10, 20, 30, 40 and 50) in the swarm network and the average results are compared. The average results

show that the proposed algorithm provides a secure optimal path in a shorter execution time compared with the existing algorithms.

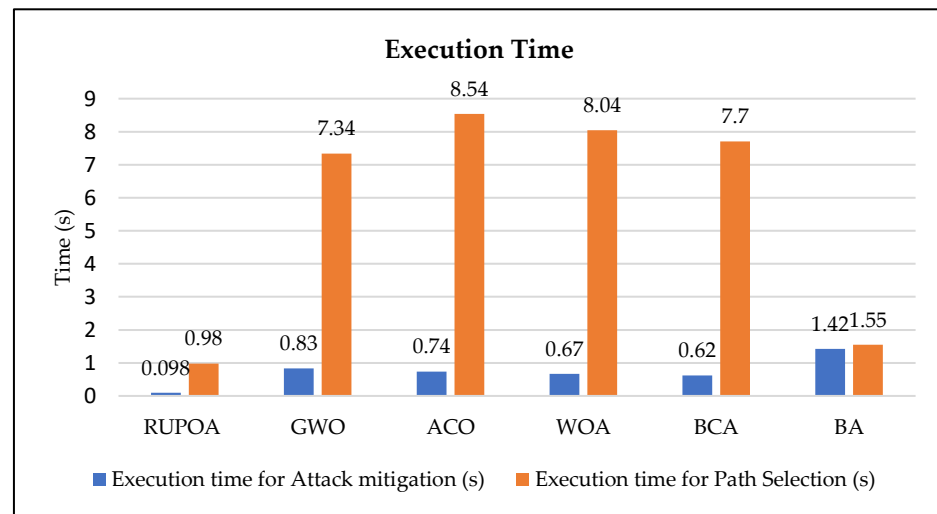


Figure 10. Execution time of the proposed algorithm.

Figure 11 shows the average energy consumption of the proposed RUPOA. The results prove that the proposed algorithm consumes less energy in both path selection and attack mitigation compared with the existing algorithms.

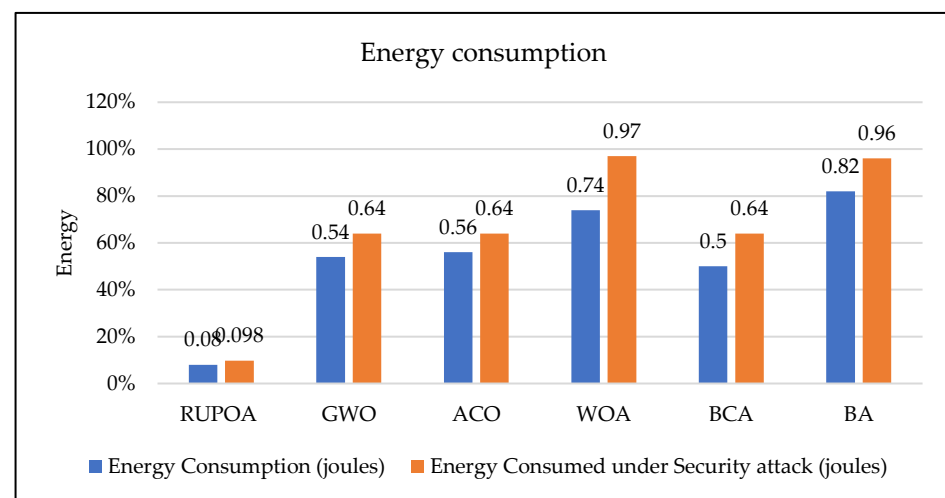


Figure 11. Comparison of energy consumed under security attacks.

The attack mitigation and the path selection accuracy of the proposed algorithm achieve a secure optimal path in less execution time compared with the existing algorithms. The secure optimal path in the UAVs allows finding the resilient optimal path when the network is under security attacks such as DoS, MITM, Sybil attack and wormhole attacks, and mitigates the attack in a shorter execution time.

Figure 12 shows the average attack mitigation rate of the proposed algorithm that provides an optimal path even under security attacks using the Ethereum consensus of the blockchain system, protecting the UAV network from security attacks. Figure 13 shows the energy consumption of the UAV nodes for an increased number of UAVs. Based on these results, the energy consumption of the proposed algorithm is less compared with the existing algorithms.

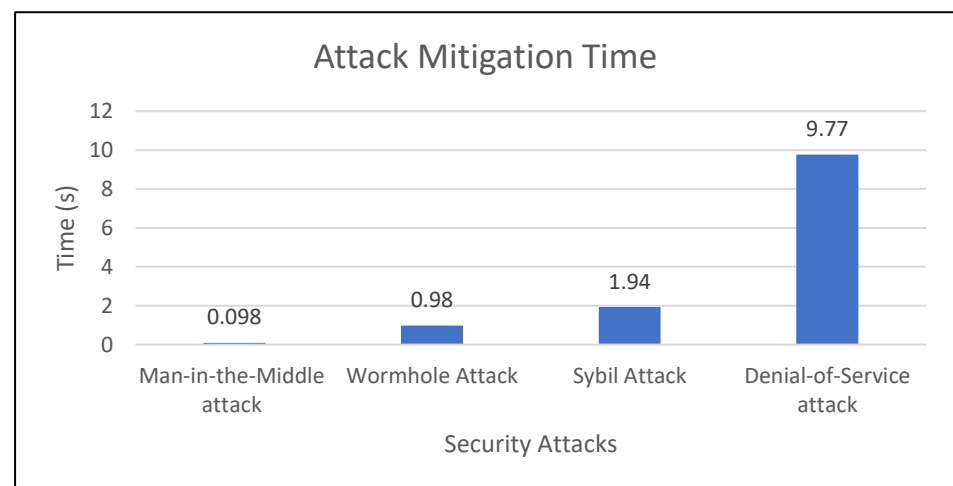


Figure 12. Attack mitigation rate.

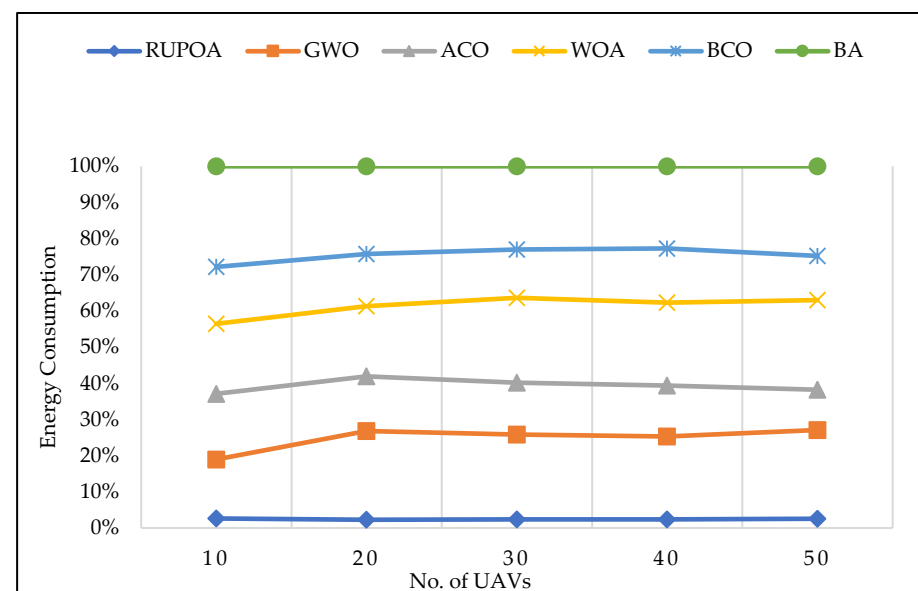


Figure 13. Energy consumption with increased numbers of UAVs.

8. Conclusions

This paper has developed a new RUPOA algorithm for secure navigation of path planning in a swarm of UAVs. The proposed algorithm integrates the concepts of the energy rate of UAVs and authentication of UAVs to enhance efficient optimal and secure path planning. Further, the proposed algorithm RUPOA generates an optimal path in less execution time and is also capable of generating the next optimal path under security attacks. The energy of the UAVs is drained when the neighbour nodes are unreachable and at a long distance. Therefore, the proposed algorithm aims to reduce the distance of communication among the neighbour nodes. It maintains a routing table which tracks the position and energy of all the neighbour nodes and chooses the optimal path in less execution time. In addition, compared with the existing algorithms, the attack mitigation percentage is optimal in the proposed algorithm. Considering the efficiency of the proposed algorithm, the simulation results presented show the attack mitigation accuracy rate and the path selection accuracy of the proposed algorithm as optimal. Further, the attack mitigation rate of the proposed algorithm under multiple attack scenarios is presented, and the proposed model is capable of mitigating security attacks in less time under path planning in a swarm of UAVs.

Author Contributions: Conceptualization, K.M. and R.S.; methodology, K.M. and R.S.; validation, R.S.; writing—original draft preparation, K.M.; writing—review and editing, K.M. and R.S.; visualization, K.M. and R.S.; supervision, R.S.; project administration, R.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Alotaibi, E.T.; Alqefari, S.S.; Koubaa, A. Lsar: Multi-uav collaboration for search and rescue missions. *IEEE Access* **2019**, *7*, 55817–55832. [\[CrossRef\]](#)
- Bekhti, M.; Abdennebi, M.; Achir, N.; Boussetta, K. Path planning of unmanned aerial vehicles with terrestrial wireless network tracking. In Proceedings of the 2016 Wireless Days (WD), Toulouse, France, 23–25 March 2016; pp. 1–6.
- Bellingham, J.S.; Tillerson, M.; Alighanbary, M.; How, J.P. Cooperative path planning for multiple UAVs in dynamic and uncertain environments. *IEEE Conf. Decis. Control* **2002**, *3*, 2816–2822.
- Bohat, V.K.; Arya, K.V. An effective gbest-guided gravitational search algorithm for real-parameter optimization and its application in training of feed forward neural networks. *Knowl.-Based Syst.* **2018**, *143*, 192–207. [\[CrossRef\]](#)
- Bollino, K.; Lewis, L.R. Collision-free multi-UAV optimal path planning and cooperative control for tactical applications. In Proceedings of the AIAA Guidance, Navigation and Control Conference and Exhibit, Honolulu, HI, USA, 18–21 August 2008; p. 7134.
- Bortoff, S.A. Path planning for UAVs. *Am. Control. Conf. ACC* **2000**, *1*, 364–368.
- Cheikhrouhou, O.; Khoufi, I. A comprehensive survey on the Multiple Traveling Salesman Problem: Applications, approaches and taxonomy. *Comput. Sci. Rev.* **2021**, *40*, 100369. [\[CrossRef\]](#)
- Cheikhrouhou, O.; Koubaa, A.; Zarrad, A. A cloud based disaster management system. *J. Sens. Actuator Netw.* **2020**, *9*, 6. [\[CrossRef\]](#)
- Chen, X.; Li, Z.; Yang, Y.; Qi, L.; Ke, R. High-resolution vehicle trajectory extraction and denoising from aerial videos. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3190–3202. [\[CrossRef\]](#)
- Cheng, Z.; Wang, E.; Tang, Y.; Wang, Y. Real-time Path Planning Strategy for UAV Based on Improved Particle Swarm Optimization. *J. Comput.* **2014**, *9*, 209–214. [\[CrossRef\]](#)
- Cui, M.; Zhang, G.; Wu, Q.; Ng, D.W.K. Robust trajectory and transmit power design for secure UAV communications. *IEEE Trans. Veh. Technol.* **2018**, *67*, 9042–9046. [\[CrossRef\]](#)
- Choudhary, G.; Sharma, V.; You, I. Sustainable and secure trajectories for the military Internet of Drones (IoD) through an efficient Medium Access Control (MAC) protocol. *Comput. Electr. Eng.* **2019**, *74*, 59–73. [\[CrossRef\]](#)
- Cugurullo, F. Urban artificial intelligence: From automation to autonomy in the smart city. *Front. Sustain. Cities* **2020**, *2*, 38. [\[CrossRef\]](#)
- Ding, X.C.; Rahman, A.R.; Egressed, M. Multi-UAV convoy protection: An optimal approach to path planning and coordination. *IEEE Trans. Robot.* **2010**, *26*, 256–268. [\[CrossRef\]](#)
- Duan, H.B.; Ma, G.J.; Luo, D.L. Optimal formation reconfiguration control of multiple UCAVs using improved particle swarm optimization. *J. Bionic Eng.* **2008**, *5*, 340–347. [\[CrossRef\]](#)
- Geraerts, R. Planning short paths with clearance using explicit corridors. In Proceedings of the 2010 IEEE International Conference on Robotics and Automation, Anchorage, AK, USA, 3–7 May 2010; pp. 1997–2004.
- Gharibi, M.; Boutaba, R.; Waslander, S.L. Internet of drones. *IEEE Access* **2016**, *4*, 1148–1162. [\[CrossRef\]](#)
- Gramajo, G.; Shankar, P. An efficient energy constraint based UAV path planning for search and coverage. *Int. J. Aerosp. Eng.* **2017**, *2017*, 8085623. [\[CrossRef\]](#)
- Yang, K.; Sukkarieh, S. 3D smooth path planning for a UAV in cluttered natural environments. In Proceedings of the 2008 IEEE/RSJ International Conference on Intelligent Robots and Systems, Nice, France, 22–26 September 2008; pp. 794–800.
- Yang, X.S. *Nature-Inspired Metaheuristic Algorithms*; Luniver Press: UK, 2010.
- Gandomi, A.H.; Yang, X.S.; Talatahari, S.; Deb, S. Coupled eagle strategy and differential evolution for unconstrained and constrained global optimization. *Comput. Math. Appl.* **2012**, *63*, 191–200. [\[CrossRef\]](#)
- Talbi, E.G. *Metaheuristics: From Design to Implementation*; John Wiley & Sons: Hoboken, NJ, USA, 2009.
- Horn, J.; Nafpliotis, N.; Goldberg, D.E. A niched Pareto genetic algorithm for multiobjective optimization. In Proceedings of the First IEEE Conference on Evolutionary Computation. IEEE World Congress on Computational Intelligence, Orlando, FL, USA, 27–29 June 1994; pp. 82–87.
- Tang, W.J.; Wu, Q.H. Biologically inspired optimization: A review. *Trans. Inst. Meas. Control* **2009**, *31*, 495–515. [\[CrossRef\]](#)
- Shanmugavel, M.; Tsourdos, A.; Zbikowski, R.; White, B. Path planning of multiple UAVs with clothoid curves in two dimensions. *IFAC Proc. Vol.* **2007**, *40*, 461–466. [\[CrossRef\]](#)

26. Chen, H.; Wang, X.-m.; Li, Y. A survey of autonomous control for uav. In Proceedings of the 2009 International Conference on Artificial Intelligence and Computational Intelligence, Shanghai, China, 7–8 November 2009; Volume 2, pp. 267–271.
27. Zhang, G.; Wu, Q.; Cui, M.; Zhang, R. Securing UAV communications via joint trajectory and power control. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 1376–1389. [[CrossRef](#)]
28. Hayat, S.; Yanmaz, E.; Muzaffar, R. Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2624–2661. [[CrossRef](#)]
29. Lin, C.; He, D.; Kumar, N.; Choo, K.K.R.; Vinel, A.; Huang, X. Security and privacy for the internet of drones: Challenges and solutions. *IEEE Commun. Mag.* **2018**, *56*, 64–69. [[CrossRef](#)]
30. Kapitonov, A.; Lonshakov, S.; Krupenkin, A.; Berman, I. Block chain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs. In Proceedings of the 2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS), Linköping, Sweden, 3–5 October 2017; pp. 84–89.
31. Huang, D.; Zhao, D.; Zhao, L. A new method of the shortest path planning for unmanned aerial vehicles. In Proceedings of the 2017 6th Data Driven Control and Learning Systems (DDCLS), Chongqing, China, 26–27 May 2017; pp. 599–605.
32. Kamboj, V.K. A novel hybrid PSO–GWO approach for unit commitment problem. *Neural Comput. Appl.* **2016**, *27*, 1643–1655. [[CrossRef](#)]
33. Wang, Y.; Cai, F.; Wang, Y. Dynamic path planning for mobile robot based on particle swarm optimization. *AIP Conf. Proc.* **2017**, *1864*, 020024.
34. Mo, H.; Xu, L. Research of biogeography particle swarm optimization for robot path planning. *Neurocomputing* **2015**, *148*, 91–99. [[CrossRef](#)]
35. Mirjalili, S.; Lewis, A. The whale optimization algorithm. *Adv. Eng. Softw.* **2016**, *95*, 51–67. [[CrossRef](#)]
36. Mirjalili, S. SCA: A sine cosine algorithm for solving optimization problems. *Knowl.-Based Syst.* **2016**, *96*, 120–133. [[CrossRef](#)]
37. Kang, M.; Liu, Y.; Ren, Y.; Zhao, Y.; Zheng, Z. An empirical study on robustness of UAV path planning algorithms considering position uncertainty. In Proceedings of the 2017 12th International Conference on Intelligent Systems and Knowledge Engineering (ISKE), Nanjing, China, 24–26 November 2017; pp. 1–6.
38. Khairuzzaman, A.K.M.; Chaudhury, S. Multilevel thresholding using grey wolf optimizer for image segmentation. *Expert Syst. Appl.* **2017**, *86*, 64–76. [[CrossRef](#)]
39. Mirjalili, S.; Saremi, S.; Mirjalili, S.M.; Coelho, L.D.S. Multi-objective grey wolf optimizer: A novel algorithm for multi-criterion optimization. *Expert Syst. Appl.* **2016**, *47*, 106–119. [[CrossRef](#)]
40. Dewangan, R.K.; Shukla, A.; Godfrey, W.W. Three dimensional path planning using Grey wolf optimizer for UAVs. *Appl. Intell.* **2019**, *49*, 2201–2217. [[CrossRef](#)]
41. Dorigo, M.; Di Caro, G. Ant colony optimization: A new meta-heuristic. In Proceedings of the 1999 Congress on Evolutionary Computation-CEC99 (Cat. No. 99TH8406), Washington, DC, USA, 6–9 July 1999; Volume 2, pp. 1470–1477.
42. Dai, Y.; Yu, J.; Zhang, C.; Zhan, B.; Zheng, X. A novel whale optimization algorithm of path planning strategy for mobile robots. *Appl. Intell.* **2022**, 1–15. [[CrossRef](#)]
43. Muntasha, G.; Karna, N.; Shin, S.Y. Performance Analysis on Artificial Bee Colony Algorithm for Path Planning and Collision Avoidance in Swarm Unmanned Aerial Vehicle. In Proceedings of the 2021 International Conference on Artificial Intelligence and Mechatronics Systems (AIMS), Bandung, Indonesia, 28–30 April 2021; pp. 1–6.
44. Agarwal, T.; Kumar, V. A systematic review on bat algorithm: Theoretical foundation, variants, and applications. *Arch. Comput. Methods Eng.* **2022**, *29*, 2707–2736. [[CrossRef](#)]
45. Khan, N.A.; Brohi, S.N.; Jhanjhi, N.Z. UAV's applications, architecture, security issues and attack scenarios: A survey. In *Intelligent Computing and Innovation on Data Science*; Springer: Singapore, 2020; pp. 753–760.