electronics

MDPI

Article

A Novel Approach for Securing Nodes Using Two-Ray Model and Shadow Effects in Flying Ad-Hoc Network

Manjit Kaur [1], Deepak Prashar [1], Mamoon Rashid [2,*], Sultan S. Alshamrani [3] and Ahmed Saeed AlGhamdi [4]

[1] School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India; manjit.12438@lpu.co.in (M.K.); deepak.prashar@lpu.co.in (D.P.)
[2] Department of Computer Engineering, Faculty of Science and Technology, Vishwakarma University, Pune 411048, India
[3] Department of Information Technology, College of Computer and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; susamash@tu.edu.sa
[4] Department of Computer Engineering, College of Computer and Information Technology, Taif University, P.O. Box. 11099, Taif 21994, Saudi Arabia; asjannah@tu.edu.sa
* Correspondence: mamoon.rashid@vupune.ac.in; Tel.: +91-7814346505

Abstract: In the last decades, flying ad-hoc networks (FANET) have provided unique features in the field of unmanned aerial vehicles (UAVs). This work intends to propose an efficient algorithm for secure load balancing in FANET. It is performed with the combination of the firefly algorithm and radio propagation model. To provide the optimal path and to improve the data communication of different nodes, two-ray and shadow fading models are used, which secured the multiple UAVs in some high-level applications. The performance analysis of the proposed efficient optimization technique is compared in terms of packet loss, throughput, end-to-end delay, and routing overhead. Simulation results showed that the secure firefly algorithm and radio propagation models demonstrated the least packet loss, maximum throughput, least delay, and least overhead compared with other existing techniques and models.

Keywords: FANET; radio propagation model; RoadSide Units (RSUs); routing overhead; unmanned aerial vehicles

check for updates

Citation: Kaur, M.; Prashar, D.; Rashid, M.; Alshamrani, S.S.; AlGhamdi, A.S. A Novel Approach for Securing Nodes Using Two-Ray Model and Shadow Effects in Flying Ad-Hoc Network. *Electronics* **2021**, *10*, 3164. https://doi.org/10.3390/electronics10243164

Academic Editor: Cheng Siong Chin

Received: 23 November 2021
Accepted: 16 December 2021
Published: 19 December 2021

1. Introduction

A flying ad-hoc network is a self-organizing wireless network and it takes the form of MANETs (mobile ad-hoc networks) and VANETs (vehicular ad-hoc networks). To perform different kinds of operations, FANETs use driverless aircraft which are also known as unmanned aerial vehicles [1–6]. These can be easily installed in non-deterministic areas. Traffic monitoring during congestion, search and rescue operations, patrolling, remote data collection, environmental sensing, and agricultural management are the different applications of FANETs [7–14]. In FANET, there are two categories of communications, namely UAV-2-UAV communication and UAV-2-Infrastructure communication (Figure 1). UAV-2-UAV can be used for short-range as well as for long-range communication, which is based on the rate of transmission of information (indicated as a green line). On the other side, UAV-2-Infrastructure communication can be used for transmitting and receiving data (indicated as red line) on various operations (either from a base station or from satellite).

Further, in this study, we describe the different major design limitations. Communication is one of the crucial parameters in the design of multiple unmanned aerial vehicles. Another crucial parameter is limited battery energy [15,16]. Several other major challenges are flight trajectory selection, energy limitations, adaptive routing protocols, power constraints, etc. that require consideration in this network. The main challenge is high mobility in the FANETs. Another challenge is an irregular change in the structure of the nodes in the specified network. Many researchers have introduced many techniques and algorithms to overcome these challenges in the network [17–24]. In this research work, we discuss the solution to overcome these problems, while minimum routing overhead, low computational complexity, and maximum throughput parameters can be used efficiently for load balancing in the network.

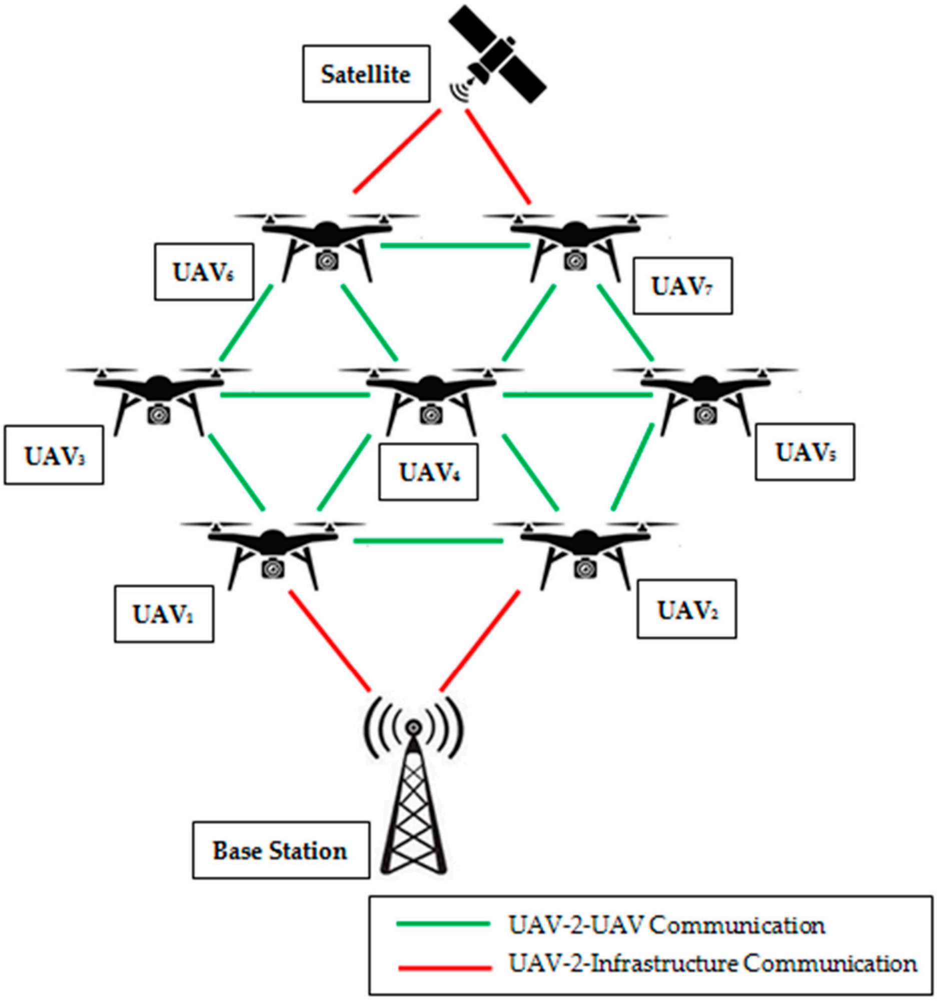


Figure 1. The architecture of flying ad-hoc networks.

There are several important characteristics of flying ad-hoc networks, such as topology change, node speed, mobility model, node mobility, energy constraints, computational power, radio propagation model, and localization, as described in Table 1 [25–28].

A subclass of UAVs can communicate with the satellite in a flying ad hoc network. There are some main differences between traditional networks and flying networks [29–31]. MANET and VANET have fewer mobility degrees than FANET. MANET and VANET are used by human beings whereas FANET flies in the sky [32–36]. In MANET and VANET, topology changes less frequently than FANET. This is due to the high mobility of flying nodes, and FANET requires the peer-to-peer connection of UAVs. MANET and VANET have less distance, but the distances among flying nodes are much greater than them [37–42].

UAVs are rapidly often are widely employed in a variety of industries, and they are gaining traction in the age of big data. The FANET node cannot be moved in most nations' flight management systems (national) due to airspace regulations. This is the most significant impediment to the expansion of the UAV network in civil aviation. In this regard, it is critical to establish different laws and policies so that the FANET node may operate freely in the air traffic control system. According to the globalized context, the UAV drone market in 2019 in the Asia Pacific was worth $7012.7 million and is expected to increase at a rate of 17.5% over the next five years. UAV rules in Europe have varied considerably, with considerable variances in criteria for flying licenses evolving with new technology, and as a result, UAV operations are continually altering in response to the demands and laws of Europe's states parties. To begin with, various nations in Europe utilize different terminology in different laws, e.g., UAV, drone, and remotely operated aircraft. This may be seen in the fast-increasing UAV market, which is predicted to be worth 10 billion euros per year in Europe until 2035, and might be worth more than 15 billion euros per year by 2050 [43].

Table 1. Characteristics of flying ad-hoc network.

Characteristics	Description
Topology change	The structure of the network rapidly changes in FANET than VANET and MANET and interface quality changes rapidly due to UAV developments.
Node speed	Smaller in size for multi-UAV systems as compared to other networks.
Mobility model	Supporting universal path to every node, UAV keeps the record plan, topology-based and randomly and regularly based pattern.
Node mobility	Highest in FANET as compared to other networks such as MANET and VANET.
Energy constraints	Some new protocols are designed for network life and do not require for mini-UAVs.
Computational Power	A serious constraint in UAV is power and far more computational power is required for the network.
Radio propagation model	As per geological structure, radio signals are the most important but it is far away from the ground and possesses LoS propagation also.
Localization	Available with GPS, AGPS, DGPS, and also available with IMU (Inertial Measurement Unit).

The technique introduced by us accurately defines the collisions in the flying nodes within the same network. Unlike most of the existing stochastic techniques, our proposed technique is not as difficult, complicated, and dependent on various vectors. Instead, it specifically depends on two metrics: load key of an optimal path and the threshold of bandwidth utilization. The major contributions of this paper can be summarized as follows:

- Based only on two parameters (load key of an optimal path and the threshold of bandwidth utilization), we provide simple yet precise terms and mathematical expressions for various crash nodes in FANET. It computes the possibilities of collisions of multiple nodes in the network, and consequently the security of multiple UAVs. We mainly derive and discuss the mathematical expressions of the predictable number of collisions in the network.
- The parameter LoK characterizes the connection of the different node paths in the network. The obtained standard mathematical expression is then used to detect the malicious node that triggered the attack in the network. Furthermore, we achieve accurate expressions compared with two effects, namely secure and insecure two ray and shadowing effects.
- To improve the efficiency of the nodes, we propose an enhanced firefly algorithm. The proposed algorithm binds the features of different parameters: low packet loss, delay, and network overhead but high throughput.
- A detailed comparative analysis has been carried out to evaluate the security of the network. We validate the obtained results in the graphical representation of the simulation.

The main goal of our proposed technique is to understand the UAVs system evolution, to help the UAVs in safe mode, without collision risk factors, and last but not least handling the issue related to the collision risks. This work involves the algorithm to evaluate the optimal route for sending data from various sources of multiple UAVs. Using the proposed methodology, there are two sections of the firefly algorithm working: one is the flashing behavior of the firefly and the other one is the step-by-step procedure, which defines the set of rules or instructions to be executed in a specific order to get the best-desired output. The firefly algorithm is used to handle optimization problems that exploit the alternating performance of fireflies in nature. Optimization is the concept to find the best path in and the term optimization is the act of making decisions and providing the best solution from the set of all feasible and possible solutions. There are three parameters of optimization techniques, namely a function to optimize, to select a value using possible solutions, and the rule of optimization.

The paper is structured into different sections as follows: In Section 2, a review of the related literature is presented. Section 3 presents our proposed analytical approach. Section 4 validates the analytical results by comparing them against simulation results. Section 5 concludes the paper and presents the future scope.

2. Related Work

A FANET is another variant of an ad-hoc network which is the sub-domain of MANET and VANET. It is not allowed to directly use the distinctive features of MANET and VANET. However, new techniques or variants of existing techniques that take into account the unique features of an unmanned aerial network are required. Table 2 provides a comparative study based on parameters that have to be tackled in the majority of existing surveys in the literature and our proposed work. Mahjri et al. [44] introduced a simple model to illustrate collisions in flying nodes using two input parameters, such as UAVs having accurate detection and avoidance capabilities as well as no accurate detection and avoidance capabilities. In the case of real-world UAV nodes, adequacy and accuracy are the main limits of this stochastic model. Belkhouche et al. [45] used kinematic equations for the deterministic case and also used for the calculations of the probability of collision between vehicles. This method does not guarantee a non-underestimation of the collision risk, ensuing in damage with respect to the security requirements.

Table 2. Characteristics of flying ad-hoc network.

Work	Packet Loss	Through-Put	End-to-End Delay	Routing Overhead	Collision Risk Assessment	Two_ray Effects (Secure vs. Insecure)	Shadowing Effects (Secure vs. Insecure)
Mahjri et al. [44]	✓	✗	✗	✗	✓	✗	✗
Belkhouche et al. [45]	✗	✗	✗	✓	✓	✗	✗
Hung et al. [46]	✗	✗	✓	✗	✓	✗	✗
Mahjri et al. [47]	✓	✗	✗	✗	✓	✗	✗
Liu et al. [48]	✓	✗	✓	✗	✗	✗	✗
Tang et al. [49]	✗	✗	✓	✓	✗	✗	✗
Temel et al. [50]	✓	✓	✓	✗	✓	✗	✗
Khabbaz et al. [51]	✗	✓	✗	✗	✗	✗	✗
Tang et al. [52]	✓	✓	✗	✗	✗	✗	✗
Wen et al. [53]	✗	✓	✗	✗	✗	✗	✗
Rosati et al. [54]	✗	✗	✗	✓	✗	✗	✗
Proposed work	✓	✓	✓	✓	✓	✓	✓

Hung et al. [46] formulated a framework and algorithm to solve the reinforcement learning (RL) problem. This framework is used for fixed-wing UAVs in the non-stationary stochastic environment. This formulation can apply for better exploration methods to speed up the learning process by using function approximation methods. Mahjri et al. [47] proposed a 3D distributed and straight-line conflict detection and alerting algorithm. This algorithm is used for only packet loss and uncertainties information at the state level for the perfect environment.

Liu et al. [48] proposed a 3D UAV relative localization framework and showed the performance which is based on the localization accuracy of the UAVs. This framework is only used for MDS-based algorithms, but it can be used for other relative localization purposes in the future. Tang et al. [49] investigated and proved the machine learning technologies in the network with a 6G intelligent network. This paper surveyed distinctive challenges in the particular networks. The proactive security methods can be used in a 6G intelligent network. Temel et al. [50] proposed a novel directional MAC protocol (LODMAC) which increased the spatial reuse and overall network capacity in the 3D environment of the existing network. This work is only limited to FANET MAC protocols. Khabbaz et al. [51] discussed how to improve the data communication performance using different parameters, such as the speed and density of the nodes in the networks. The work of Tang et al. [52] is based on location-based social networks (LBSNs) to compute the data in the cloud. Thus, the authors showed the mechanism for the effectiveness of the UAV-mounted, cloudlet-aided network with parameters accurate throughput and low packet delay. Wen et al. [53] presented a distributed optimization algorithm for flying nodes in the networks. They showed the simulation work with parameters such as improved network throughput, limited the E2E delay (end-to-end), and reduced co-channel interference. Rosati et al. [54] compared the two different routing protocols and showed the performance of the predictive–optimized link state routing (P-OLSR) and optimized link state routing (OLSR) in the flying ad-hoc networks.

In terms of world legalization, the authors discussed the UAV legislation in Germany and the significant developments in the area of UAV safety and reliability from 2017 to 2018 [55]. A further study concentrated on German UAV laws. According to European law, UAV activities in German airspace were considered in the submission. It said that Germany has established legislative frameworks to assist in the development and implementation of laws for UAV makers and operators [56].

The desire for consistent legality remains a difficult challenge for regulators since laws must account for UAV technology innovation and creative capabilities as they arise [57], which necessitates continual regulatory revisions over time. Rules are continually constantly re-evaluated and standardized in countries with current UAV legality. Practically all of the above restrictions have been developed or revised in the last few years [58]. The European Commission is now working on unifying UAV laws and establishing consistent specifications, to submit a proposal to incorporate all UAVs, irrespective of their size, into the European flight safety framework [59]. The new European drone laws (which went into effect on 1 January 2021) constitute a major step toward European standardization since they establish guidelines for all European nations, such as airspace classifications, UAV operating categories, and so on. Furthermore, the new European provisions include part of the world requirements as well as national regulatory requirements that must be met by individual European member states.

With the latest technologies, it provides results that are reliable, ideal, and best-suited. However, there are points of improvement in the computational methods involved in it that are way too high and complex. The time constraint required by them is much longer than required to produce optimal results. It refers to the initially randomized multi-valued solutions and converges the results with iteration following the global solution in an improvised manner. Due to the large randomization of selected values and large population size, some algorithms work at a slow pace. We are well aware that technology upgrades quickly with time, so do the network structures. Therefore, because of the high movements of UAVs, we get restricted to the processing power of UAVs. Such kinds of methods and techniques involve a lot of time to reach the valid result and frequently more time is consumed for an invalid output which cannot be utilized further for changing the structure of the network. These energy-based approaches are not suited for techniques using high computational and expensive parameters towards the networking area.

3. Proposed Methodology

In this section, we begin with mathematical notations and data structures of the considered network. We then consider two parts, namely the load key of an optimal path and the threshold of bandwidth utilization. Table 3 presents the lists of mathematical notations and data structures of the flying nodes. Moreover, we present the complete descriptions of the mathematical notations used. Here, we explain the metrics of the network as mentioned below:

Table 3. Mathematical notations and their meaning.

Mathematical Notations	Meaning of Notations that Used in the Expression
A_L	The average load of flying nodes
B_t	The total bandwidth of the network
B_f	Fixed bandwidth of flying nodes
LoK	Load key of an optimal path
${L_{yz}}^{Ti}$	Total load of the entire network
M	Total number of distinct destinations of flying nodes
N	Number of flying nodes
TB	Threshold of bandwidth utilization
TB_{max}	A Maximum threshold of bandwidth utilization
T_i	Time period
${V_{yz}}^{Ti}$	Vector node at the same time period of network
T_p	Transmission power of flying nodes
R_p	Receiver power of flying nodes
T_r	Transmit reciever
T_s	Transmit sender
$\mathrm{S_d}$	Sender data in a network
R_d	Receiver data in a network

A Load Key (LoK) of an Optimal Path

This metric has been defined to recognize the connection of the different node paths in the complete routing process. This is also defined as the distribution of the different packets in the network. When we analyze the network, we observe some flying nodes that are overloaded. The reason behind this is that the nodes receive the most data transmissions in the network. In this paper, we aim to change this specific load away from overloaded networks and shift to other alternate routes. We describe the metric named Load Key (LoK) for this intent, where we look for optimal paths at each flying node in the network.

Case 1: Suppose a variable as '*Ti*' which represents a time period, and the total load of the entire network is denoted as '${L_{yz}}^{Ti}$'.

In simple words, we can say it is the sum of the entire loads on all the flying nodes in the network, which is mentioned below in (1):

$$ {L_{yz}}^{Ti} = {L_{11}}^{Ti} + {L_{12}}^{Ti} + {L_{13}}^{Ti} + \ldots + {L_{1n}}^{Ti} + \ldots + {L_{n1}}^{Ti} + {L_{n2}}^{Ti} + {L_{n3}}^{Ti} + \ldots + {L_{nm}}^{Ti} \quad (1) $$

where, m is equivalent to $n-1$.

Case 2: If the flying nodes are not connected in the network, then we can use the input vector as '${V_{yz}}^{Ti}$' at the same time period, where 'y' and 'z' variables are set for nodes from 1 to n as mentioned below in (2):

$$ {L_{yz}}^{Ti} = \sum_{y=1}^{n} \cdot \sum_{z=1,\neq y}^{n} {L_{yz}}^{Ti} {V_{yz}}^{Ti} \quad (2) $$

where $V_{yz} = \begin{matrix} 0, \text{ Access of network does not through UAV} \\ 1, \text{ Access of network through UAV} \end{matrix}$

Case 3: We need to calculate the average load of the flying nodes in the network. The average load 'A_L' of the nodes is defined as:

$$A_L = \sum_{i=1}^{n} \cdot \frac{{L_{yz}}^{Ti}}{Ti} \tag{3}$$

Now, we need to substitute from (2) to (3), to obtain the final equation as:

$$A_L = \sum_{i=1}^{n} \cdot \frac{1}{Ti} \sum_{y=1}^{n} \cdot \sum_{z=1,\neq y}^{n} {L_{yz}}^{Ti} {V_{yz}}^{Ti} \tag{4}$$

B Threshold of Bandwidth Utilization (TB)

This metric has been defined to calculate the actual bandwidth of the network. TB can be defined as a link from one point to another link for the network. The metric TB can be used to monitor the efficiency of the network. This metric also can be used to improve network utilization in flying ad-hoc networks. Here, we have defined the total bandwidth 'B_t' of the network as follows:

$$B_t = \sum_{y=1}^{n} \cdot \sum_{z=1,\neq y}^{n} {V_{yz}}^{Ti}.B_f \tag{5}$$

where 'B_f' is the fixed bandwidth of the flying nodes.

The technique will result in lower overheads, less congestion, and increase efficiency. This metric can be expressed as an optimization model (TB_{max}) as stated below:

$$\text{TB}_{\text{max}} = \frac{\sum_{i=1}^{n} \cdot \frac{1}{Ti} \sum_{y=1}^{n} \cdot \sum_{z=1,\neq y}^{n} {L_{yz}}^{Ti} {V_{yz}}^{Ti}}{\sum_{y=1}^{n} \cdot \sum_{z=1,\neq y}^{n} {V_{yz}}^{Ti}.B_f} \tag{6}$$

Finally, this indicates that all the flying nodes are connected to the network with the optimal path from source to destination. There are different steps to implement the proposed methodology, such as selection of path, the possibility of paths, moving of nodes in other directions. Apart from this, it is easy to change the route of the flying nodes due to the change of the topology structure. Here, the two-ray model (Raytwo) is used for the secure routing of the nodes from one place to another using the $Rayf(x)$ function.

$$\text{Ray}_{\text{two}} = Rayf(x) = TB_{max} + \sum_{n=0}^{i} \left(T_P \cos \frac{Bt}{Bf} + T_R \sin \frac{Bt}{Bf} \right) \tag{7}$$

Furthermore, we need to calculate the secure shadow value, i.e., $Shadow(v)$, as follows:

$$\bigcup_{n=0}^{i} (T_r \cap T_s) Rayf(x) = Shadow(v) \tag{8}$$

where T_r and T_s represent transmit receiver and transmit sender, respectively.

Finally, we need to calculate the accurate flying nodes as per sender data (S_d) and receiver data (R_d) in the network,

$$\underset{0 \leq n \leq 1}{S_d, R_d} = \sum_{n=0}^{i} shadow(v) \tag{9}$$

By using Equations (8) and (9), we obtain the secure shadow effects of the flying nodes in the network and the result of this work is useful for the verification of FANET nodes, which can be directly used in all the wireless prediction area.

3.1. Selection of Path

In the path selection method, multiple paths are used in this system to send the data at the same time. When only one route is used, traffic is concentrated at a few nodes, resulting in congestion, as described in Figure 2. As a result, we use the firefly algorithm to find the optimal path as described in Algorithm 1 and we can keep the benefits of multipath routing without losing the consistency of the paths we use. Any route has a zero count at first, and the top route is chosen for packet routing. After each packet transmission over a given path, the count of that path is increased. When this count equals, the next route is chosen.

Algorithm 1. Selection of path using firefly algorithm.

```
func: Obj_func ( ), Max_Gen_func ( )
Start: Obj_func, $f(pkt)$, $pkt = (pkt_1, pkt_2, \ldots, pkt_n)^t$ [Initialization mode.]
  Generation of the initial population of different flying nodes, $pkt_i$ $(i = 1, 2, 3, \ldots, k)$
  Define light intensity ($L_i$) and light absorption coefficient ($Co_{eff}$).
  Do
    For $i = 1$: $k$, all 'k' fireflies
      For $j = 1$: $i$, all 'k' fireflies
        If ($L_i < L_j$),
            Move firefly $i$ towards $j$;
          Else
            Do not move firefly $i$ towards $j$;
        END IF
            While ($pkt < Max\_Gen\_func\ (M_G)$)
            Compute attractiveness value of the fireflies using
            $\beta = \beta_0 x e^{-yr^2} - 1! = 0$, where, $\beta_0! = 0$
      End For Loop (Inner loop of variable $j$)
    End For Loop (Outer loop of variable $i$)
        Update the latest $L_i$ of the fireflies.
        Then, rank all the fireflies and display the best-desired path.
  End Do while
End
```

3.2. Possibility of Paths

The calculated Max_Gen_func (M_G) represents the possible path and path that are categorized on the behalf of their counted attractiveness. A path with the greater firefly value shows a superior path and therefore it is used more frequently than the other paths. Consequently, a path with a greater value has a greater path selection ratio. Various paths are exploited for packet delivery to a destination. Among the various paths available for a destination, only some of the paths are used for the best path.

3.3. Moving of Nodes to Other Direction

When the selected route is not detected as the connection no longer exists, then the node should be moved to the other direction. After evaluating new solutions and updates light intensity, we need to check the path of the node, such that the path is indeed the path noted for next use. This will happen when the status field of that path is attractive. We just need to recognize, rank the fireflies, and search the path to be used next. To observe this, we should determine the current path of the node for the other paths for a similar destination.

We need to apply post-processing on the best results so far and need to visualize the flying nodes.

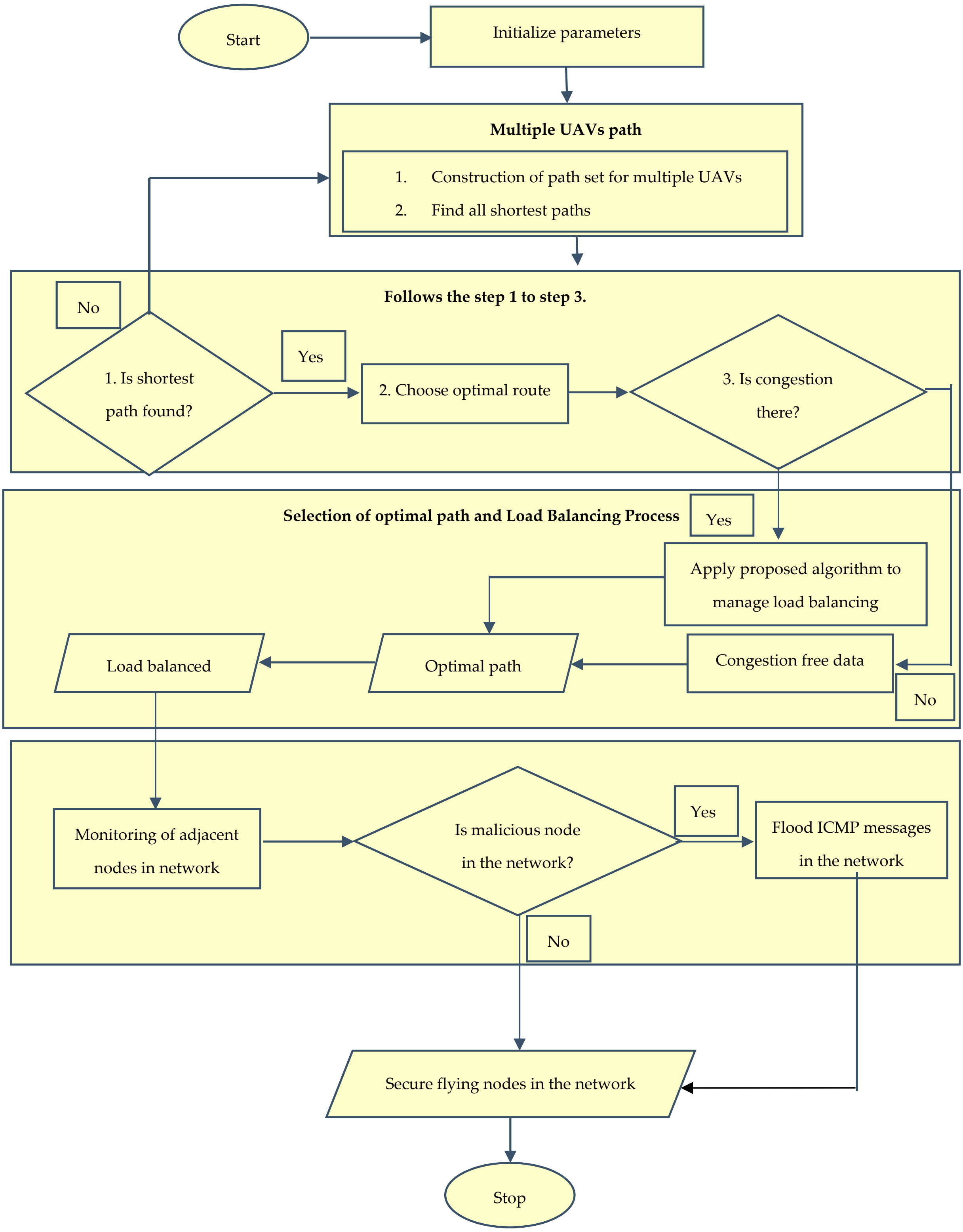

Start
Initialize parameters
Multiple UAVs path
1. Construction of path set for multiple UAVs
2. Find all shortest paths
Follows the step 1 to step 3.
No
1. Is shortest path found?
Yes
2. Choose optimal route
3. Is congestion there?
Selection of optimal path and Load Balancing Process
Yes
Apply proposed algorithm to manage load balancing
Load balanced
Optimal path
Congestion free data
No
Monitoring of adjacent nodes in network
Is malicious node in the network?
Yes
Flood ICMP messages in the network
No
Secure flying nodes in the network
Stop

Figure 2. Load balancing and secure flying nodes in the network.

4. Results and Discussions

In this section, we perform a series of simulations carried out with the NS2 tool. This work is divided into three sections, namely the working of flying nodes, detection of malicious nodes, and performance analysis of a network. The performance analysis is further sub-categorized as packet loss, throughput, end-to-end delay, and routing overhead parameters.

4.1. Working of Flying Nodes

The simulation study primarily generated different nodes in the network zone, where the beginning time of source nodes was consistently distributed over the first 60 s of the simulation time. We arbitrarily place some flying nodes in the network area. The defined area has different types of flying nodes: non-malicious flying nodes and malicious flying nodes. Non-malicious nodes are the normal nodes, which follow the rules from the source point to the destination point. On the other side, malicious nodes are the compromised modes, which do not follow the rules from the source point to the destination point. These nodes may modify or drop some packets. In the network, some nodes act as central controller units and others as UAV nodes. The characteristics of UAVs are mentioned in Table 4:

Table 4. Characteristics of UAVs.

Parameter Type	Value
Number of UAVs	100
Queue Type	Priority queue
Altitude of UAVs	40 m
Traffic Type	CBR
Directional Gain	10 dBi
Frequency	2.4 GHz
Wireless Medium	Wireless physical medium
Data Rates	54 Mbps
Packet Interval (s)	Exponential (1)
Packet Size (byte)	1024
Simulation Time	200 s
Pause Time	Variable
Antenna Type	Omni-Directional
Transmission Power	0.005 W
Speed of UAVs	Can vary upto 60 m/s
Reception Power Threshold	−95 dBm

Figure 3 shows the layout of RoadSide Units (RSUs) which can improve and promote the network performance in flying ad-hoc networks and provide additional services in the network, such as smooth traffic flow, emergency response, and safety improvement.

4.2. Detection of Malicious Nodes

In this compromised node, the proposed algorithm is evaluated and then compared with the GPMOR protocol. When the central controller unit detects that there are some malicious nodes in the network, it sends further messages through the network.

We got a malicious node that triggered the attack in the network and communication recommenced between two nodes. Again, the node is sending a request for new id registration, and it registered with a new fake ID, so we got a malicious node-triggered attack in the network. Then, flying nodes in the network receive messages and begin monitoring their neighboring nodes, as shown in Figure 4. Malicious nodes in the network are detected using the monitoring mode technique.

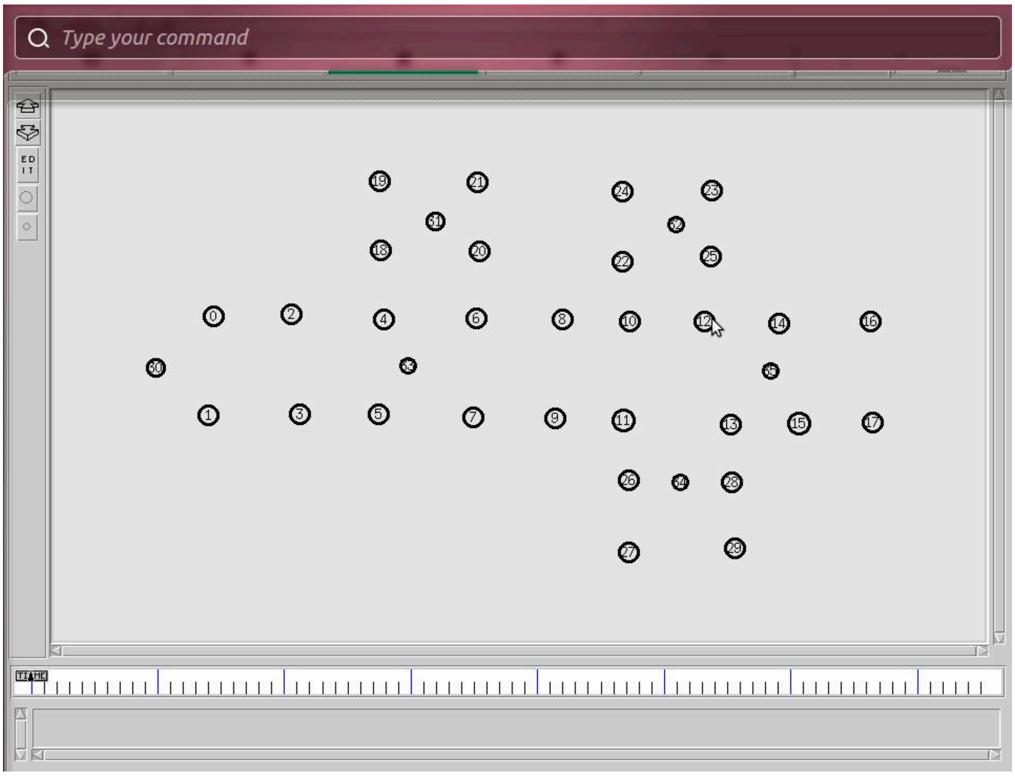
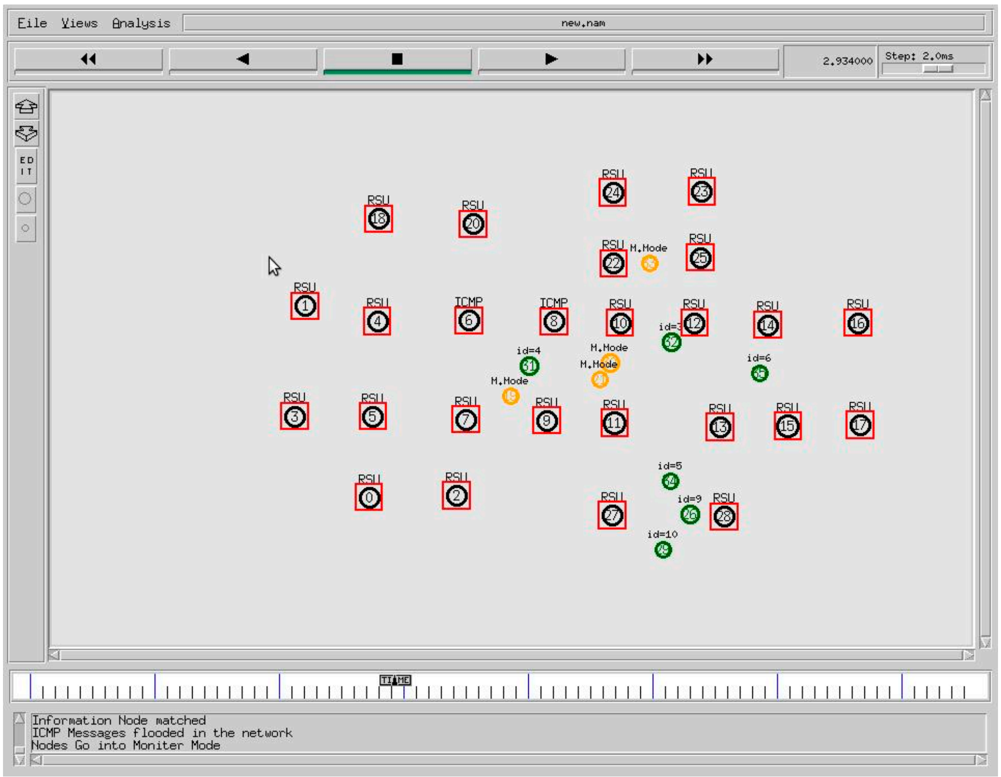


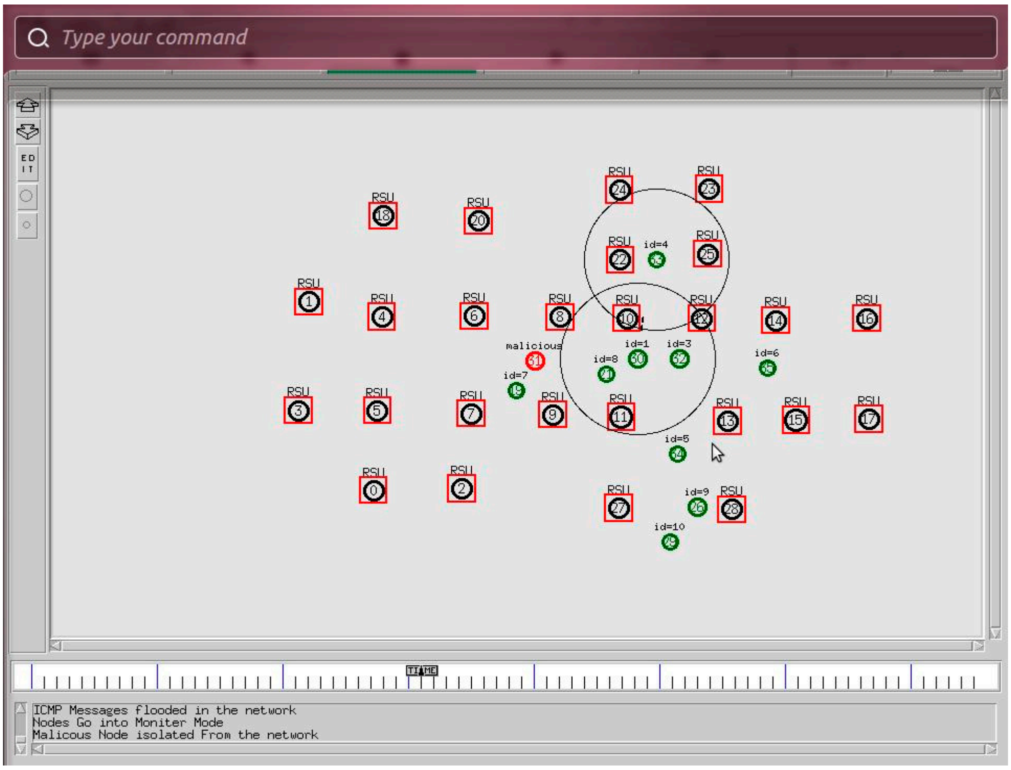
Figure 3. The layout of RSU (RoadSide Units) nodes.



```
Information Node matched
ICMP Messages flooded in the network
Nodes Go into Moniter Mode
```

Figure 4. Nodes in monitor mode.

The roadside units start flooding the ICMP messages in the networks. The nodes when receiving ICMP messages will start monitoring their adjacent nodes. When the roadside units came to know that some malicious nodes exist in the network, the roadside units flood ICMP messages in the network. The nodes in the network receive ICMP messages and start monitoring their adjacent nodes. From the monitoring, the malicious nodes are detected in the network, as shown in Figure 5.



```
ICMP Messages flooded in the network
Nodes Go into Moniter Mode
Malicous Node isolated From the network
```

Figure 5. Malicious node isolated in the network.

4.3. *Performance Analysis of a Network*

We finally provide the performance analysis of flying nodes in the network using parameters: packet loss, throughput, end-to-end delay, and routing overhead. There is a comparison between secure and insecure two_ray and shadow effects discussed in Table 5 and also displayed in the network.

Table 5. The number of packets versus time in packet loss parameter.

Secure vs. Insecure	Time	Number of Packets
Secure Two_ray	5 ms	8
Insecure Two_ray	6 ms	14
Secure shadowing	6 ms	4
Insecure shadowing	6 ms	13

4.3.1. Packet Loss Parameter

Packet loss means dropped packets in the network due to network overload, node mobility, node interferences with each other, and structure of the network. There are several reasons available for packet loss in the network.

Figure 6 displays the packet loss of flying nodes, where the *X*-axis represents the maximum speed of flying nodes in the network and the *Y*-axis represents the packet loss ratio in the network. A comparison is made between secure and insecure two_ray and shadow models in the network. The packet wise description for the packet loss parameter in flying nodes is discussed in Table 5.

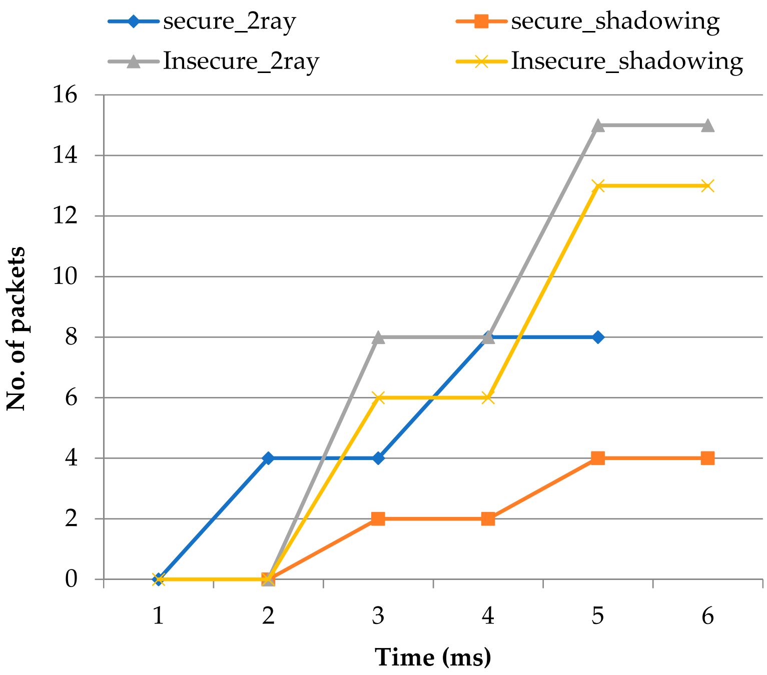


Figure 6. Packet loss of flying nodes in the network.

4.3.2. Throughput Parameter

Throughput is an important network performance parameter in flying ad-hoc networks. Throughput means the amount of information transmission in the network and the position of flying nodes can be moved from one place to another.

The distance between different flying nodes can be changed, and the limit of relating flying nodes in the network can be optimized to increase the throughput. Further, it shows the throughput of flying nodes, where the *X*-axis represents the speed of flying nodes and the *Y*-axis represents as network average throughput in Figure 7. The packet wise description for throughput parameter in flying nodes is discussed in Table 6.

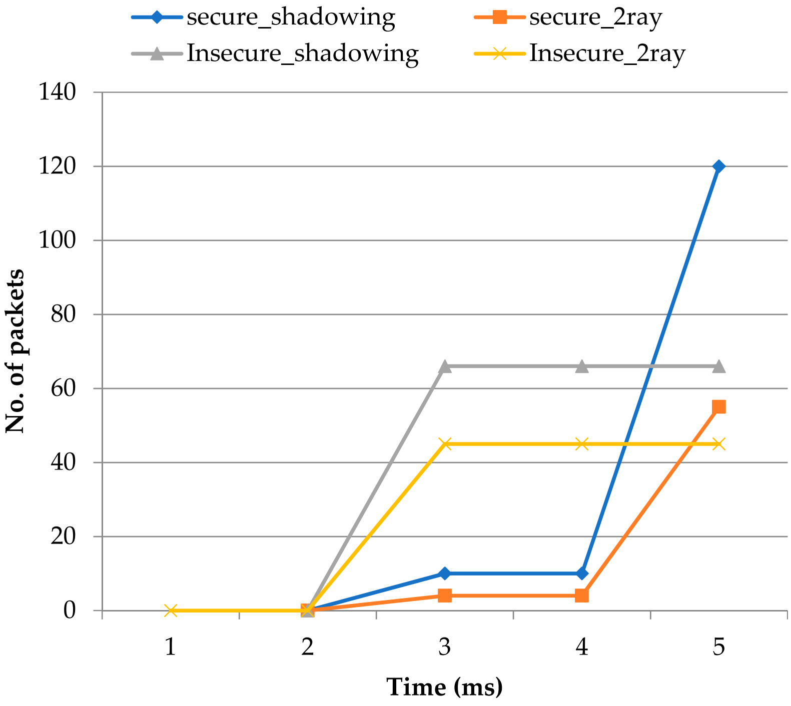


Figure 7. Throughput of flying nodes in the network.

Table 6. The number of packets versus time in throughput parameter.

Secure vs. Insecure	Time	Number of Packets
Secure Two_ray	5 ms	55
Insecure Two_ray	5 ms	45
Secure shadowing	5 ms	120
Insecure shadowing	5 ms	65

4.3.3. End-to-End Delay Parameter

Figure 8 shows the end-to-end delay (E-to-E Delay) of flying nodes. This figure shows the difference between the sending time of every node at the source and receiving time of the node at the destination. The packet wise description for the end-to-end delay parameter in flying nodes is discussed in Table 7.

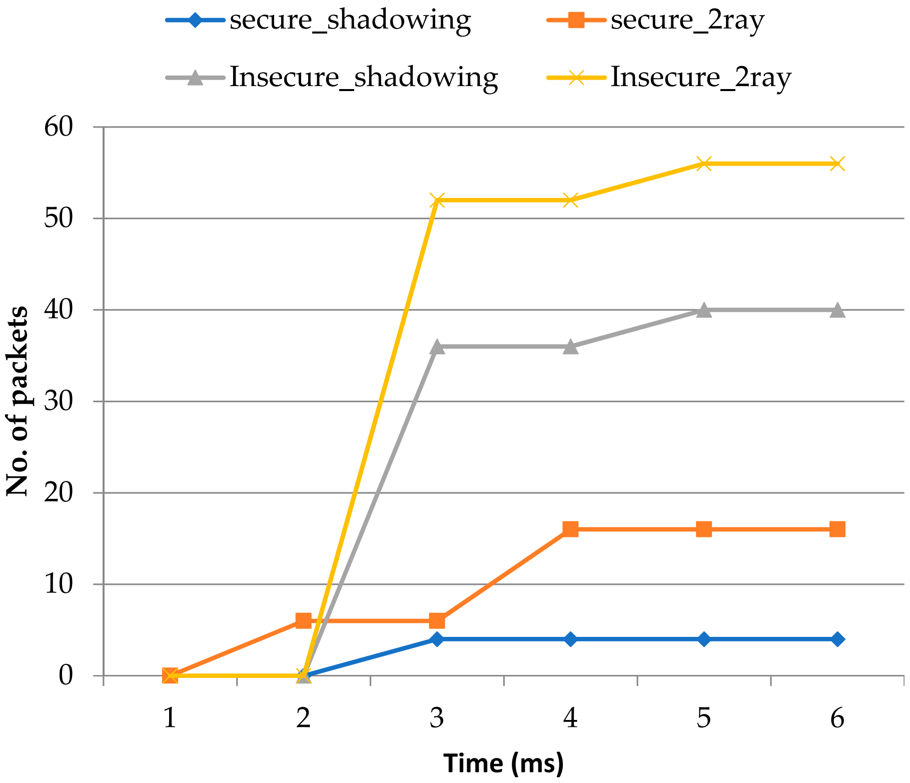


Figure 8. End-to-end delay of flying nodes in the network.

Table 7. The number of packets versus time in the end-to-end delay parameter.

Secure vs. Insecure	Time	Number of Packets
Secure Two_ray	6 ms	16
Insecure Two_ray	6 ms	56
Secure shadowing	6 ms	4
Insecure shadowing	6 ms	40

4.3.4. Routing Overhead Parameter

Figure 9 shows the routing overhead of flying nodes. This figure shows the number of extra packets collected during the network transmission process. The packet wise description for the routing overhead parameter in flying nodes is discussed in Table 8.

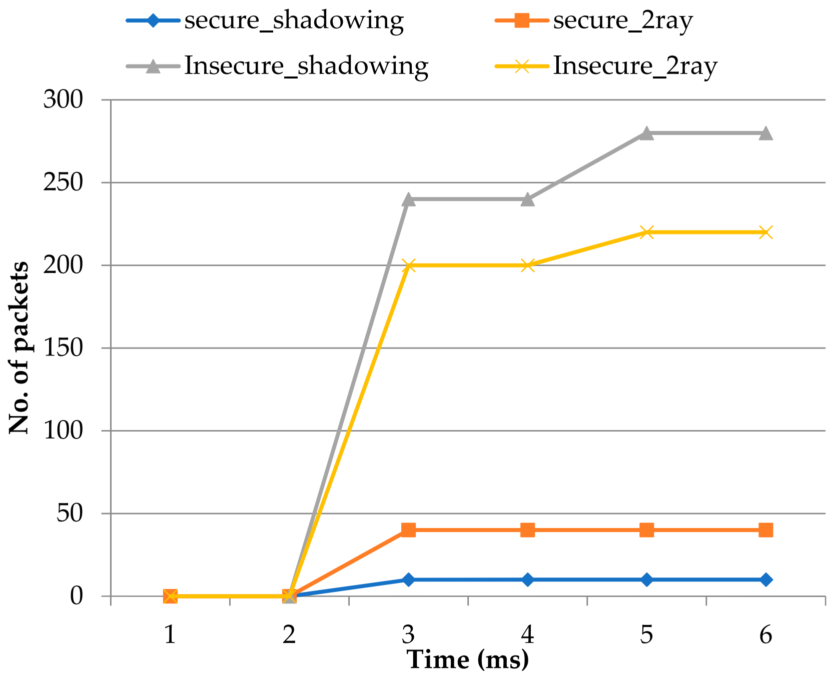


Figure 9. Routing Overhead of flying nodes in the network.

Table 8. The number of packets versus time in routing overhead parameter.

Secure vs. Insecure	Time	Number of Packets
Secure Two_ray	6 ms	40
Insecure Two_ray	6 ms	220
Secure shadowing	6 ms	5
Insecure shadowing	6 ms	280

Table 9 demonstrates the results of the proposed model. The performance parameters, such as packet loss (%), throughput (kbps), end-to-end delay (ms), and network routing overhead (byte), were analyzed in each flying node. A comparison was made between the results of insecure and secure modes for the two_ray effect and shadowing effect. In the insecure two ray effect, the packet loss value is 15%. On the other hand, by applying the secure two ray effect, the value of the packet loss is only 8%, which indicates the minimum packet loss of the flying nodes in the network. With another effect, i.e., insecure shadowing effect, the value of the packet loss of flying node is 13%. On the other hand, secure shadowing effect shows 4% packet loss in the network. In the insecure two ray effect, the throughput value is 42 kbps. By applying the secure two ray effect, the value of the throughput is only 58 kbps, which indicates the maximum throughput of the flying nodes in the network. Furthermore, in the insecure shadowing effect, the value of the throughput of the flying node is 63 kbps. On the other hand, the secure shadowing effect shows 120 kbps throughput of the flying nodes in the network.

Table 9. Comparison between secure and insecure two_ray and shadow effects.

Parameters	Total Received Packets			
Effects (in Seconds)	Packet Loss (%)	Throughput (kbps)	End-to-End Delay (ms)	Routing Overhead (Byte)
Insecure two_ray effect	15	42	57	260
Secure two_ray effect	8	58	18	48
Insecure shadowing effect	13	63	40	220
Secure shadowing effect	4	120	4	5

In the insecure two ray effect, the end-to-end delay value is 57 ms. On the other hand, by applying the secure two ray effect, the value of the end-to-end delay is only 18 ms. In the insecure shadowing effect, the value of the end-to-end delay of the flying node is 40 ms, and the secure shadowing effect showing end-to-end delay value is 4 ms in the network, which indicates the minimum end-to-end delay of the flying nodes in the network. In the insecure two ray effect, the routing overhead value is 260 bytes. On the other hand, by applying the secure two ray effect, the value of the routing overhead is only 48 bytes. In the insecure shadowing effect, the value of the routing overhead of the flying node is 220 bytes. On the other hand, the secure shadowing effect shows 5 bytes routing overhead in the network.

Furthermore, this indicates the minimum routing overhead of the flying nodes in the network. To conclude, it is showing minimum packet loss, maximum throughput, minimum end-to-end delay, and minimum routing overhead of the flying nodes in the network.

5. Conclusions

The major revelation from this study is that we have considered the firefly algorithm which holds three major relevant aspects for the optimization technique. The deployment of an efficient approach has played a major role in achieving the secure optimization of flying nodes in the network. We analyzed the different factors used to evaluate the optimal route for sending data from various sources of multiple UAVs and detected the malicious nodes in the network using the two-ray model and shadow effects.

The conducted simulations provide useful and important insights concerning the accuracy of the proposed algorithm for the load balancing technique. Furthermore, the simulation showed the results with different parameters, such as packet loss, throughput, end-to-end delay, routing overhead with secure and insecure two-ray and shadow effects, which further indicates that the parameters can extend the predictable objective by adjusting the flying node position in the ad-hoc network. Further research is required to compare with more security models of the flying nodes in the future. Because FANETs are subject to a variety of attacks, the geographic position-oriented routing protocol can be improved to include the identification of different types of attacks in its design. In the future, it can be improved by creating a new strategy for detecting and locating rogue nodes among Internet of Things devices.

Author Contributions: M.K. and D.P. made contributions to conception and manuscript writing; S.S.A. and A.S.A. examined and supervised this research and outcomes; M.R. revised and polished the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Taif University Research Supporting Project number (TURSP-2020/311), Taif University, Taif, Saudi Arabia.

Data Availability Statement: The data will be shared on request to the first author of the paper.

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

Abbreviations

List of abbreviations used in the study:

3D distributed	Three-Dimensional distributed
3D UAV	Three-Dimensional Unmanned Aerial Vehicle
6G	Sixth Generation
AGPS	Assisted Global Positioning System
Co_{eff}	Light Absorption Coefficient
DGPS	Differential Global Positioning System
E2E Delay	End-to-End Delay
FANETs	Flying Ad-hoc Networks
Func	Function
GPMOR	Geographic Position Mobility Oriented Routing

GPS	Global Positioning System
ICMP	Internet Control Message Protocol
IMU	Inertial Measurement Unit
kbps	kilobits per second
LBSNs	Location-Based Social Networks
LODMAC	Location Oriented Directional Medium Access Control
LoK	Load key of an optimal path
LoS	Line-of-Sight
MAC	Medium Access Control
MANETs	Mobile Ad-hoc Networks
Max_Gen_func	Maximum Generation Function
MDS	Multi-Dimensional Scaling
mini-UAVs	mini-Unmanned Aerial Vehicles
ms	milliseconds
multi-UAV	Multiple Unmanned Aerial Vehicle
NS2	Network Simulator2
Obj_func	Objective Function
OLSR	Optimized Link State Routing
pkt	Packet
P-OLSR	Predictive–Optimized Link State Routing
RL problem	Reinforcement Learning problem
RSUs	RoadSide Units
TB	Threshold of Bandwidth Utilization
UAVs	Unmanned Aerial Vehicles
UAV-2-Infrastructure communication	Unmanned Aerial Vehicle-2-Infrastructure communication
UAV-2-UAV communication	Unmanned Aerial Vehicle-2-Unmanned Aerial Vehicles Communication
VANETs	Vehicular Ad-hoc Networks

References

1. Fotouhi, A.; Ding, M.; Hassan, M. DroneCells: Improving spectral efficiency using drone-mounted flying base stations. *J. Netw. Comput. Appl.* **2021**, *174*, 102895. [CrossRef]
2. Ancel, E.; Capristan, F.M.; Foster, J.V.; Condotta, R.C. Real-time risk assessment framework for unmanned aircraft system (UAS) traffic management (UTM). In Proceedings of the 17th Aiaa Aviation Technology, Integration, And Operations Conference, Denver, CO, USA, 5–9 June 2017; p. 3273.
3. Dentler, J.; Rosalie, M.; Danoy, G.; Bouvry, P.; Kannan, S.; Olivares-Mendez, M.; Voos, H. Collision avoidance effects on the mobility of a uav swarm using chaotic ant colony with model predictive control. *J. Intell. Robot. Syst.* **2019**, *93*, 227–243. [CrossRef]
4. Hussen, H.R.; Choi, S.C.; Park, J.H.; Kim, J. Predictive geographic multicast routing protocol in flying ad hoc networks. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719843879. [CrossRef]
5. Minaeian, S.; Liu, J.; Son, Y.J. Vision-based target detection and localization via a team of cooperative UAV and UGVs. *IEEE Trans. Syst. Man Cybern. Syst.* **2015**, *46*, 1005–1016. [CrossRef]
6. Ray, P.P.; Mukherjee, M.; Shu, L. Internet of things for disaster management: State-of-the-art and prospects. *IEEE Access* **2017**, *5*, 18818–18835. [CrossRef]
7. Sharma, V.; Srinivasan, K.; Chao, H.C.; Hua, K.L.; Cheng, W.H. Intelligent deployment of UAVs in 5G heterogeneous communication environment for improved coverage. *J. Netw. Comput. Appl.* **2017**, *85*, 94–105. [CrossRef]
8. Yang, Y.; Zhang, J.; Cai, K.Q.; Prandini, M. Multi-aircraft conflict detection and resolution based on probabilistic reach sets. *IEEE Trans. Control. Syst. Technol.* **2016**, *25*, 309–316. [CrossRef]
9. Condomines, J.P.; Zhang, R.; Larrieu, N. Network intrusion detection system for UAV ad-hoc communication: From methodology design to real test validation. *Ad Hoc Netw.* **2019**, *90*, 101759. [CrossRef]
10. Lin, X.; Yajnanarayana, V.; Muruganathan, S.D.; Gao, S.; Asplund, H.; Maattanen, H.L.; Wang, Y.P.E. The sky is not the limit: LTE for unmanned aerial vehicles. *IEEE Commun. Mag.* **2018**, *56*, 204–210. [CrossRef]

11. Tang, F.; Fadlullah, Z.M.; Kato, N.; Ono, F.; Miura, R. AC-POCA: Anticoordination game based partially overlapping channels assignment in combined UAV and D2D-based networks. *IEEE Trans. Veh. Technol.* **2017**, *67*, 1672–1683. [CrossRef]
12. Li, W. Formation-preserving properties of cooperative kinematic agents with or without external influence of target attraction. *IEEE Trans. Autom. Control.* **2017**, *63*, 1737–1744. [CrossRef]
13. Mazuelas, S.; Shen, Y.; Win, M.Z. Spatiotemporal information coupling in network navigation. *IEEE Trans. Inf. Theory* **2018**, *64*, 7759–7779. [CrossRef]
14. Liu, Z.; Dai, W.; Win, M.Z. Mercury: An infrastructure-free system for network localization and navigation. *IEEE Trans. Mob. Comput.* **2017**, *17*, 1119–1133. [CrossRef]
15. Kumar, K.; Kumar, S.; Kaiwartya, O.; Kashyap, P.K.; Lloret, J.; Song, H. Drone assisted flying ad-hoc networks: Mobility and service-oriented modeling using neuro-fuzzy. *Ad Hoc Netw.* **2020**, *106*, 102242. [CrossRef]
16. Dai, W.; Shen, Y.; Win, M.Z. A computational geometry framework for efficient network localization. *IEEE Trans. Inf. Theory* **2017**, *64*, 1317–1339. [CrossRef]
17. Wang, Y.; Wu, Y.; Shen, Y. Joint spatiotemporal multipath mitigation in large-scale array localization. *IEEE Trans. Signal Process* **2018**, *67*, 783–797. [CrossRef]
18. Liu, Y.; Shen, Y.; Guo, D.; Win, M.Z. Network localization and synchronization using full-duplex radios. *IEEE Trans. Signal Process.* **2017**, *66*, 714–728. [CrossRef]
19. Liu, D.; Xu, Y.; Wang, J.; Chen, J.; Wu, Q.; Anpalagan, A.; Xu, K.; Zhang, Y. Opportunistic utilization of dynamic multi-UAV in device-to-device communication networks. *IEEE Trans. Cogn. Commun. Netw.* **2020**, *6*, 1069–1083. [CrossRef]
20. Kulmer, J.; Leitinger, E.; Grebien, S.; Witrisal, K. Anchorless cooperative tracking using multipath channel information. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 2262–2275. [CrossRef]
21. Arribas, E.; Mancuso, V.; Cholvi, V. Coverage optimization with a dynamic network of drone relays. *IEEE Trans. Mob. Comput.* **2019**, *19*, 2278–2298. [CrossRef]
22. Muthusenthil, B.; Kim, H.; Prasath, V.B. Location Verification Technique for Cluster Based Geographical Routing in MANET. *Informatica* **2020**, *31*, 113–130. [CrossRef]
23. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442. [CrossRef]
24. Gao, A.; Hu, Y.; Liang, W.; Lin, Y.; Li, L.; Li, X. A QoE-oriented scheduling scheme for energy-efficient computation offloading in UAV cloud system. *IEEE Access* **2019**, *7*, 68656–68668. [CrossRef]
25. Oubbati, O.S.; Lakas, A.; Zhou, F.; Güneş, M.; Yagoubi, M.B. A survey on position-based routing protocols for Flying Ad hoc Networks (FANETs). *Veh. Commun.* **2017**, *10*, 29–56. [CrossRef]
26. Ge, X.; Ye, J.; Yang, Y.; Li, Q. User mobility evaluation for 5G small cell networks based on individual mobility model. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 528–541. [CrossRef]
27. Lyu, J.; Zeng, Y.; Zhang, R. UAV-aided offloading for cellular hotspot. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 3988–4001. [CrossRef]
28. Saini, T.K.; Sharma, S.C. Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept. *Ad Hoc Netw.* **2020**, *103*, 102148. [CrossRef]
29. Mairaj, A.; Baba, A.I.; Javaid, A.Y. Application specific drone simulators: Recent advances and challenges. *Simul. Model. Pract. Theory* **2019**, *94*, 100–117. [CrossRef]
30. Merwaday, A.; Güvenç, I. Handover count based velocity estimation and mobility state detection in dense HetNets. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 4673–4688. [CrossRef]
31. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.H.; Debbah, M. A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2334–2360. [CrossRef]
32. Bensalem, A.; Boubiche, D.E. EBEESU: ElectriBio-inspired Energy-Efficient Self-organization model for Unmanned Aerial Ad-hoc Network. *Ad Hoc Netw.* **2020**, *107*, 102236. [CrossRef]
33. Naqvi, S.A.R.; Hassan, S.A.; Pervaiz, H.; Ni, Q. Drone-aided communication as a key enabler for 5G and resilient public safety networks. *IEEE Commun. Mag.* **2018**, *56*, 36–42. [CrossRef]
34. Sun, J.; Wang, Z.; Huang, Q. Cyclical NOMA based UAV-enabled wireless network. *IEEE Access* **2018**, *7*, 4248–4259. [CrossRef]
35. Ma, Z.; Guo, Q.; Ma, J.; Zhang, Z.; Ma, H.; Peng, L.; Li, Y. VaSe-MRP: Velocity-aware and stability-estimation–based multi-path routing protocol in flying ad hoc network. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719883128. [CrossRef]
36. Yang, D.; Wu, Q.; Zeng, Y.; Zhang, R. Energy tradeoff in ground-to-UAV communication via trajectory design. *IEEE Trans. Veh. Technol.* **2018**, *67*, 6721–6726. [CrossRef]
37. Zeng, Y.; Zhang, R. Energy-efficient UAV communication with trajectory optimization. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3747–3760. [CrossRef]
38. Zeng, F.; Hu, Z.; Xiao, Z.; Jiang, H.; Zhou, S.; Liu, W.; Liu, D. Resource allocation and trajectory optimization for QoE provisioning in energy-efficient UAV-enabled wireless networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 7634–7647. [CrossRef]
39. Aadil, F.; Raza, A.; Khan, M.F.; Maqsood, M.; Mehmood, I.; Rho, S. Energy aware cluster-based routing in flying ad-hoc networks. *Sensors* **2018**, *18*, 1413. [CrossRef]
40. Kaur, M.; Verma, S. Flying Ad-Hoc Network (FANET): Challenges and Routing Protocols. *J. Comput. Theor. Nanosci.* **2020**, *17*, 2575–2581. [CrossRef]

41. Zhan, C.; Lai, H. Energy minimization in Internet-of-Things system based on rotary-wing UAV. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 1341–1344. [CrossRef]
42. Zorbas, D.; Pugliese, L.D.P.; Razafindralambo, T.; Guerriero, F. Optimal drone placement and cost-efficient target coverage. *J. Netw. Comput. Appl.* **2016**, *75*, 16–31. [CrossRef]
43. SESAR. European Drones Outlook Study, 2016. Available online: https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf (accessed on 14 May 2021).
44. Mahjri, I.; Dhraief, A.; Belghith, A.; Gannouni, S.; Mabrouki, I.; AlAjlan, M. Collision risk assessment in Flying Ad Hoc aerial wireless networks. *J. Netw. Comput. Appl.* **2018**, *124*, 1–13. [CrossRef]
45. Belkhouche, F. Modeling and calculating the collision risk for air vehicles. *IEEE Trans. Veh. Technol.* **2013**, *62*, 2031–2041. [CrossRef]
46. Hung, S.M.; Givigi, S.N. A Q-learning approach to flocking with UAVs in a stochastic environment. *IEEE Trans. Cybern.* **2016**, *47*, 186–197. [CrossRef]
47. Mahjri, I.; Dhraief, A.; Belghith, A.; Al Mogren, A.S. Slide: A straight line conflict detection and alerting algorithm for multiple unmanned aerial vehicles. *IEEE Trans. Mob. Comput.* **2017**, *17*, 1190–1203. [CrossRef]
48. Liu, Y.; Wang, Y.; Wang, J.; Shen, Y. Distributed 3D Relative Localization of UAVs. *IEEE Trans. Veh. Technol.* **2020**, *69*, 11756–11770. [CrossRef]
49. Tang, F.; Kawamoto, Y.; Kato, N.; Liu, J. Future intelligent and secure vehicular network toward 6G: Machine-learning approaches. *Proc. IEEE* **2019**, *108*, 292–307. [CrossRef]
50. Temel, S.; Bekmezci, I. LODMAC: Location oriented directional MAC protocol for FANETs. *Comput. Netw.* **2015**, *83*, 76–84. [CrossRef]
51. Khabbaz, M.; Antoun, J.; Assi, C. Modeling and performance analysis of UAV-assisted vehicular networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 8384–8396. [CrossRef]
52. Tang, F.; Fadlullah, Z.M.; Mao, B.; Kato, N.; Ono, F.; Miura, R. On a novel adaptive UAV-mounted cloudlet-aided recommendation system for LBSNs. *IEEE Trans. Emerg. Top. Comput.* **2018**, *7*, 565–577. [CrossRef]
53. Wen, S.; Deng, L.; Liu, Y. Distributed optimization via primal and dual decompositions for delay-constrained FANETs. *Ad Hoc Netw.* **2020**, *109*, 102288. [CrossRef]
54. Rosati, S.; Krużelecki, K.; Heitz, G.; Floreano, D.; Rimoldi, B. Dynamic routing for flying ad hoc networks. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1690–1700. [CrossRef]
55. Cramer, M.; Wieland, M. UAS-Regulierung, oder: Nichts ist beständiger als der Wandel. Kresse, W. Reports. *J. Photogramm. Remote Sens. Geoinf. Sci.* **2019**, *87*, 123–135.
56. Borst, L.; Wiesenberg, M.-P.; von Hesler, F. Hogan Lovells, 2020. Available online: https://www.hoganlovells.com/~{}\{\}/media/hogan-lovells/pdf/2020-pdfs/2020_06_01_iplr77_drones-in-the-german-skies-new-eu-regulations-take-flight.pdf?la=en (accessed on 27 May 2021).
57. Radovic, M. Drone Industry Insight, 2019. Available online: https://droneii.com/drone-regulation (accessed on 4 June 2021).
58. Jones, T. *International Commercial Drone Regulation and Drone Delivery Services*; RAND Corporation: Santa Monica, CA, USA, 2017.
59. LLC. Regulation of Drones-The Low Library of Congress, 2016. Available online: https://www.loc.gov/law/help/regulation-ofdrones/regulation-of-drones.pdf (accessed on 22 April 2021).