drones

MDPI

Article

Dwarf Mongoose Optimization-Based Secure Clustering with Routing Technique in Internet of Drones

Fatma S. Alrayes [1], Jaber S. Alzahrani [2], Khalid A. Alissa [3], Abdullah Alharbi [4], Hussain Alshahrani [5], Mohamed Ahmed Elfaki [5], Ayman Yafoz [6], Abdullah Mohamed [7] and Anwer Mustafa Hilal [8,*]

[1] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[2] Department of Industrial Engineering, College of Engineering at Alqunfudah, Umm Al-Qura University, Mecca 24382, Saudi Arabia
[3] Saudi Aramco Cybersecurity Chair, Networks and Communications Department, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam 31441, Saudi Arabia
[4] Department of Computer Science, Community College, King Saud University, Riyadh 11437, Saudi Arabia
[5] Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra 11911, Saudi Arabia
[6] Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 22254, Saudi Arabia
[7] Research Centre, Future University in Egypt, New Cairo 11845, Egypt
[8] Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam Bin Abdulaziz University, AlKharj 16278, Saudi Arabia
* Correspondence: a.hilal@psau.edu.sa

check for updates

Citation: Alrayes, F.S.; Alzahrani, J.S.; Alissa, K.A.; Alharbi, A.; Alshahrani, H.; Elfaki, M.A.; Yafoz, A.; Mohamed, A.; Hilal, A.M. Dwarf Mongoose Optimization-Based Secure Clustering with Routing Technique in Internet of Drones. *Drones* **2022**, *6*, 247. https://doi.org/10.3390/drones6090247

Academic Editors: Shiva Raj Pokhrel, Hai L. Vu and Jinho Choi

Received: 29 July 2022
Accepted: 1 September 2022
Published: 9 September 2022

Abstract: Over the last few years, unmanned aerial vehicles (UAV), also called drones, have attracted considerable interest in the academic field and exploration in the research field of wireless sensor networks (WSN). Furthermore, the application of drones aided operations related to the agriculture industry, smart Internet of things (IoT), and military support. Now, the usage of drone-based IoT, also called Internet of drones (IoD), and their techniques and design challenges are being investigated by researchers globally. Clustering and routing aid to maximize the throughput, reducing routing, and overhead, and making the network more scalable. Since the cluster network used in a UAV adopts an open transmission method, it exposes a large surface to adversaries that pose considerable network security problems to drone technology. This study develops a new dwarf mongoose optimization-based secure clustering with a multi-hop routing scheme (DMOSC-MHRS) in the IoD environment. The goal of the DMOSC-MHRS technique involves the selection of cluster heads (CH) and optimal routes to a destination. In the presented DMOSC-MHRS technique, a new DMOSC technique is utilized to choose CHs and create clusters. A fitness function involving trust as a major factor is included to accomplish security. Besides, the DMOSC-MHRS technique designs a wild horse optimization-based multi-hop routing (WHOMHR) scheme for the optimal route selection process. To demonstrate the enhanced performance of the DMOSC-MHRS model, a comprehensive experimental assessment is made. An extensive comparison study demonstrates the better performance of the DMOSC-MHRS model over other approaches.

Keywords: drone communication; energy efficiency; security; clustering; multi-hop routing; Internet of drones

1. Introduction

With the growth of modern wireless communication technology, the Internet of things (IoT) is becoming a broadly utilized technology in the domain of several intellectual applications and services [1]. Eventually, the rise in interconnectivity between numerous things or objects has produced massive data. But, such IoT applications were not as much as effective for making decisions, and data perception lacked the participation of human cognition processing. Currently, cognitive computing has grabbed the attention of IoT authors [2]. The IoT with the cognitive capability called cognitive IoT (CIoT) allows an object or things to study several data from devices or gadgets which is connected, i.e., sensors, UAVs, etc. Drones or unmanned aerial vehicles (UAV) are becoming a developing technology that has communication, sensing, storage, and processing abilities [3]. It is employed in diverse industries such as the Internet of things (IoT) scenarios, intelligent transportation systems, and smart cities. The placement of a swarm of UAVs for IoT services is a reality for numerous applications namely tracking and surveillance, package delivery, search and rescue, and public safety [4]. Such IoT-assisted applications facilitate the new pattern called the Internet of drones (IoD). It could offer a capability to a UAV drone network for accessing drones and users through the Internet. The features of drones are easy mobility and deployment, which makes UAVs helpful for transmission. Since drones are movable, it is utilized as information carriers i.e., sending the data to remote destinations [5]. When the destination does not in direct interaction range of the UAV, the transmission happens through multiple hops. The swarm of UAVs cooperates to constitute a network for sending the data to the destinations. Though reliability, survivability, and scalability were the distinctive traits of IoD; however, it put forward many complexities in transmissions and drones networking [6]. The UAV's higher mobility makes the topologies very rapid, leading to communication issues.

The self-organizing UAV network constitutes a plurality of clusters by a clustering technique, with every cluster made up of some cluster members (CM) and a cluster head (CH) [7]. Such CHs form the high-layer virtual backbone network and present two critical operations they are direct interactions between CHs and a medium for cross-cluster transmission. The CMs in the same cluster interact directly via a single hop; however, the data sent between clusters were initially forwarded to the CH, and then forwarded to the CH of the cluster in which the destiny node was positioned via the virtual backbone networks [8]. The CH after sends to the destiny nodes for achieving cross-cluster transmission. In a clustered IoD, when a compromised node was chosen as a CH, this node not just illegitimately acquired information from the normal node but even forge data distributed to the sink [9]. In addition, attackers could grab control of the entire network by compromising tiny CHs; compromising every CHs becomes a very alluring target for them. As a drone-related network suffers from the same susceptibilities, secure CH choosing for the IoD becomes vital for its successful operations [10].

1.1. Existing Works on Cluster-Based Routing in IoD

In [11], the operation of drones in ad hoc mode and their cooperation with vehicles in vehicular ad hoc networks (VANET) were learned to aid the detection and routing procedure of malicious vehicles. A routing protocol termed vehicular routing unit (VRU) can be devised that involves two different ways they are routing packets of data between UAVs using a protocol termed VRU_u and supplying packets of data between vehicles by using drones utilizing a protocol called VRU_vu. In [12], a novel systematic structure can be presented for solving the issue of multi-drone collaborative task allotment. It can be developed as a combinatorial optimizing issue and resolved by the enhanced clustering technique. The main goal was to enable multi-drone for completing tasks has less energy utilization. Since the drone count increased, it appears that flight safety problems such as collisions between the drones, and an enhanced multi-UAV collision-resistant approach related to the enhanced artificial potential domain were devised. Namdev et al. [13] modeled a whale optimization algorithm-related optimized link state routing (WOA-OLSR) over a flying ad hoc network (FANET) for providing optimum routing for secure and energy-efficient FANET. The efficacy of OLSR can be improvised with the help of WOA and assessed performance displays superior efficacy of WOA-OLSR.

In [14], the optimal CH selection depends upon blockchain (BC) transactions, residual energy (RE), mobility, online duration, connectivity, and reputation by utilizing improved artificial bee colony optimization (IABC). The presented IABC uses two distinct search equations for onlooker bee and employee bee for enhancing exploitation abilities and convergence rate. In addition, a lightweight BC consensus technique, the AI-proof of witness consensus algorithm (AI-PoWCA) can be projected that employs the optimal CH for mining. In [15], drones that can act as mobile sinks were taken into account and prevailing work on wireless sensor network (WSN)-UAV atmosphere authentication was protracted. A secure authentication structure utilizing an elliptic-curve crypto-system was provided. The projected structure can be assessed to assure it is resilient to renowned potential assaults relevant to password guessing, data confidentiality, key impersonation, and mutual authentication.

In [16], a secure and reliable routing protocol (SecRIP) for the FANET can be devised for reliable and efficient data communication. This script operates toward the improvement of the quality of experience (QoE) metrics and quality of service (QoS). The script operates on two methods: the dragonfly technique and the chaotic algae technique; such methods serve the functionalities of cluster management, selection, and data communication in intercluster. Khan et al. [17] project a new routing approach as the extension of AntHocNet because of mobile features; it is called a flying nature-inspired method. Moreover, a case study was performed for improving the signal power with the help of modeled learning technique named decision tree (DT).

1.2. Paper Contributions

This study develops a new dwarf mongoose optimization-based secure clustering with a multi-hop routing scheme (DMOSC-MHRS) in the IoD environment. The goal of the DMOSC-MHRS technique involves the selection of CHs and optimal routes to a destination. In the presented DMOSC-MHRS technique, a new DMOSC technique is utilized to choose CHs and create clusters. A fitness function (FF) involving trust as a major factor is included to accomplish security. Besides, the DMOSC-MHRS technique designs a wild horse optimization-based multi-hop routing (WHOMHR) scheme for the optimal route selection process. To demonstrate the enhanced performance of the DMOSC-MHRS model, a comprehensive experimental assessment is made.

1.3. Paper Organization

The organization of the paper is given as follows. Section 2 introduces the proposed DMOSC-MHRS model and the experimental analysis of the DMOSC-MHRS model is provided in Section 3. Lastly, Section 4 concludes the study with major findings and possible future enhancements.

2. The Proposed Secure Clustering with Routing Protocol

In this study, a new DMOSC-MHRS technique has been developed for secure cluster-based communication in the IoD environment. The DMOSC-MHRS technique proficiently chooses CHs and optimal routes to a destination. The major intention of the proposed model is to accomplish security, energy efficiency, and improved lifetime. Figure 1 showcases the overall procedure of the DMOSC-MHRS algorithm.

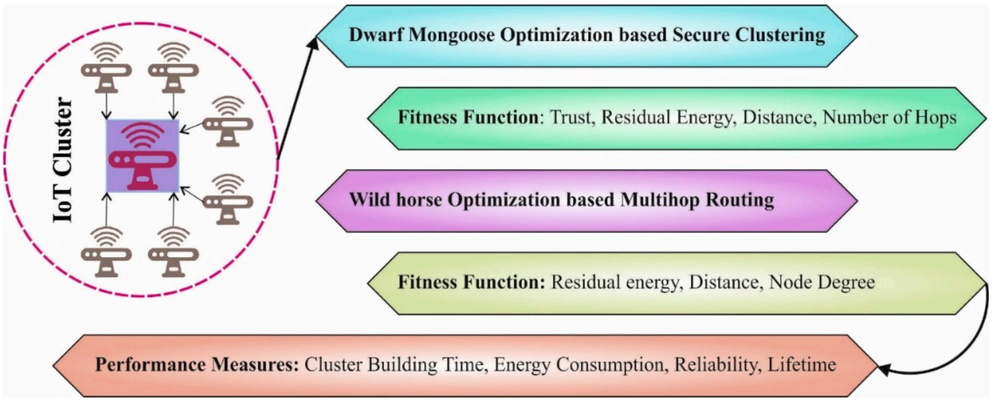
IoT Cluster
Dwarf Mongoose Optimization based Secure Clustering
Fitness Function: Trust, Residual Energy, Distance, Number of Hops
Wild horse Optimization based Multihop Routing
Fitness Function: Residual energy, Distance, Node Degree
Performance Measures: Cluster Building Time, Energy Consumption, Reliability, Lifetime

Figure 1. The overall process of the DMOSC-MHRS algorithm.

2.1. Overview of DMO Algorithm

The DMO technique inspires the performance of dwarf mongooses when determining their food [18]. Generally, the DMO starts with setting the primary value to a group of solutions utilizing the subsequent equation:

$$x_{i,j} = l_j + rand \times \left(u_j - l_j\right) \tag{1}$$

whereas *rand* refers to the arbitrary number created in zero and one. u_j and l_j implies the restrictions of the searching area. The swarm of DMO has three groups such as babysitters, alpha group, and scouts. All the groups have their individual performance for capturing the food, and the particulars of these groups are provided as:

2.1.1. Alpha Group

The fitness of all the solutions is calculated if the population was established. Equation (2) computes the possible value for all the fitness populations, and alpha female (α) is selective and dependent on this probability.

$$\alpha = \frac{fit_i}{\Sigma_{i=1}^{n} fit_i} \tag{2}$$

n relates to the number of mongooses from the alpha group. The number of babysitters was represented by bs. Peep is the vocalization of the dominant female which keeps the family on track.

All the mongooses sleep from the primary sleeping mound that is fixed $\varnothing$. The DMO utilized for generating a candidate food place.

$$X_{i+1} = X_i + phi \times peep \tag{3}$$

The sleeping mound was offered in Equation (4) then all the repetitions, whereas *phi* signifies the uniformly distributed arbitrary value in -1 and 1.

$$sm_i = \frac{fit_{i+1} - fit_i}{\max\{|fit_{i+1}, fit_i|\}} \tag{4}$$

Equation (5) comprises the average value of sleeping mounds.

$$\varphi = \frac{\Sigma_{i=1}^{n} sm_i}{n} \tag{5}$$

If the babysitting alters condition is met, this technology advances to the scouting phase, in which the next sleeping mound or food source is assumed.

2.1.2. Scout Group

As mongooses are identified to not go back to past sleep mounds, the scout's appearance is for the next sleeping mounds, making sure to search. In this method, scout and forage were carried out concurrently. This drive was exhibited then a successful/unsuccessful search for a novel sleeping mound. Specifically, the migration of mongooses is contingent on their entire efficiency. The scout mongoose is defined in Equation (12).

$$X_{i+1} = \begin{cases} X_i - CF * phi * rand * \left[X_i - \vec{M}\right] \ if \ \varphi_{i+1} > \varphi_i \\ \\ X_i + CF * phi * rand * \left[X_i - \vec{M}\right] \end{cases} \tag{6}$$

In which *rand* demonstrates a random number from the range of zero and one, $CF = (1 - \frac{iter}{\text{Max}_{iter}})^{(2\frac{iter}{\text{Max}_{iter}})}$ whereas the parameter which regulates the mongoose group, the collective-volitive movement was reduced linearly as the iterations developed. $\vec{M} = \Sigma_{i=1}^{n} \frac{X_i \times sm_i}{X_i}$ in which the mongoose's movement to the novel sleeping mound was defined by this vector.

2.1.3. Babysitters Group

The babysitters were commonly inferior group members which continue with the young and cycle on a regular basis allowing the alpha female (mother) for leading the rest of the group on daily forage expeditions. The number of babysitters was proportional to the size of the population; it can be a stimulus for the technique by decreasing the entire population size dependent upon the percentage set. The scout and food source data earlier indicated by the family members replaces them by resetting the use of the babysitter interchange parameter.

2.2. Design of DMOSC Technique

In the presented DMOSC-MHRS technique, a new DMOSC technique is utilized to choose CHs and create clusters. The FF in this MOTAHO is used for choosing the topical CH derived. Now, the FF is expressed by the four dissimilar parameters namely number of hops, trust, distance, and residual energy (RE) [19].

Trust: In CH selection, trust is regarded as a key parameter in the FF to improve security. The mutual trust made in a specific period is used for accomplishing the transmission.

Direct trust (DT) is predicated on the approximate period of communication among i^{th} node and d^{th} destination n. DT is measured as the gap on the list of actual and the projected period of i^{th} node for authenticating the public key expressed by the d^{th} destination. Hence, DT including i^{th} node and d^{th} the destination is given by,

$$DT_i^d(\tau) = \frac{1}{3}\left[DT_i^d(\tau-1) - \left(\frac{\tau_{appx} - \tau_{est}}{\tau_{appx}}\right) + \omega\right] \tag{7}$$

In Equation (7), τ_{appx} defines the approximate period and τ_{est} determines the estimated period to authenticate the public keys. In other words, τ_{appx} and τ_{est} are the expected period for sending and receiving the public keys via the destination and also the node. ω implies the opinion parameter of this node.

The node with the opinion parameter is plotted based on DT. However, the node without a witness parameter is authenticated by the indirect trust (IDT) as follows that is given by,

$$IDT_i^d(\tau) = \frac{1}{r}\sum_{i=1}^{r} DT_i^d(d) \tag{8}$$

In Equation (8), r denotes the total neighbors of node i.

Recent trust (RT) is measured by the DT and IDT along with the crucial validity and admits the destination or sink that is given in part of the moment.

$$RT_i^d(\tau) = \alpha^* DT_i^d(\tau) + (1-\alpha)^* IDT_i^d(\tau) \tag{9}$$

where $\alpha = 0.3$.

$$g_1 = DT_i^d(\tau) + IDT_i^d(\tau) + RT_i^d(\tau) \tag{10}$$

Distance: It determines the distance (g_2) amongst the CH to the BS and the next-hop node. Since the energy usage of nodes is proportionate to the distance of the communication path. Consequently, it is essential to determine the communication path with a lesser distance for diminishing energy utilization.

Residual energy: The candidate CH with higher RE (g_3) formulated in Equation (11) is greatly desirable at the time of CH selection. Since the CH has to perform different operations namely data transmission, collection, and aggregation.

$$g_3 = \sum_{i=1}^{a} E_{CH_i} \tag{11}$$

In the above equation, E_{CH_i} illustrates the RE of CH.

Some hops: Some standard nodes belonging to the specific CH are described by some hops. The energy utilization of CH is lesser when it has a lesser number of hops. Therefore, the CH with lesser hops is regarded in the number of hops (g_4) and CH selection is formulated as follows.

$$g_4 = \sum_{i=1}^{a} I_i \tag{12}$$

In Equation (12), the number of standard nodes for the specific CH can be represented as I_i. The mentioned objective values were converted into one objective related to the weighted sum technique as presented below in Equation (13).

$$f = \delta_1 \times g_1 + \delta_2 \times g_2 + \delta_3 \times g_3 + \delta_4 \times g_4 \tag{13}$$

where the δ_1, δ_2, δ_3, and δ_4 represents the weights allotted to every FF value. The devised FF was utilized from the DMOSC approach to choose an optimum CH.

2.3. Process Involved in WHOMHR Technique

In this study, the DMOSC-MHRS technique designs a WHOMHR scheme for optimal route selection process. The WHO algorithm is a metaheuristic algorithm dependent upon the social life of wild horses [20]. During this technique, distinct performances are demonstrated by wild horses namely leading, chasing, grazing, hunting, and mating. The horses were categorized into two social groups such as territorial and non-territorial. But, the WHO technique concentrates on the non-territorial group that comprises group leaders named stallions, several mares, and their offspring. The part of stallion is to lead the group and connect with mares, as the foals start their lives with grazing performance. In addition, if the foals exceed the age of puberty, they can leave their group and integrate into other groups. The process of the WHO technique was outlined in the subsequent steps:

2.3.1. Population Initialization

During this stage, the parameter needed for the WHO technique was established for evaluating the primary solution, afterward upgraded based on the technique process. The horses were separated into many groups and all the groups have one stallion. This division was estimated employing in Equation (14) as follows:

$$H = Q \times SR \tag{14}$$

where H denotes the entire amount of groups, Q refers to the population size, and SR signifies the number of stallions from the population.

2.3.2. Grazing Behavior

This step presents the grazing performance of foals before they can obtain puberty. The stallion was considered at the center of the grazing region, whereas the residual group members were adjacent to the center of the region. This performance is demonstrated employing in Equation (15):

$$X^{j}_{i+1,H} = 2A \times cos(2\pi RA) \times \left(S^{j} - X^{j}_{i,H}\right) + S^{j} \tag{15}$$

In which i signifies the number of group members, j denotes the number of stallions, $X^{j}_{\imath+1,H}$, $X^{j}_{i,H}$ stands for the place of group members from the next and present iteration correspondingly, A has an arbitrarily selective adaptive process, R represents the arbitrary number in -2 and 2, and S^{j} denotes the stallion place.

2.3.3. Horse Mating Behavior

This phase offers the performance of foals afterward obtaining puberty age. As previously noted, foals leave their groups and combine with another group for mating and for preventing fathers from marrying their daughters and sisters. Besides, this performance was demonstrated in employing Equation (16):

$$X^{t}_{H,l} = Mean\left(X^{u}_{H,i},\ X^{w}_{H,j}\right) and\ i \neq j \neq l \tag{16}$$

where $X^{t}_{H,l}$ signifies the place of horse t of group l, $X^{u}_{H,i}$ refers to the place of foals u of group i, and $X^{w}_{H,j}$ signifies the place of foal w of group j, in which the foal u mate with foal w from the group l. Therefore, an essential state to mate was obtained. Algorithm 1 demonstrates the working of the WHO algorithm.

2.3.4. Group Leadership

During this stage, the group stallion leads the members of the group to the waterhole for food. Likewise, the stallion fights with another stallion for dominating the waterhole. This performance is defined utilizing Equation (17):

$$S_{\imath+1,G} = \begin{cases} 2A \times cos(2\pi RA) \times (WP - S_{i,G}) + WP\ if\ r_1 > 0.5 \\ 2A \times cos(2\pi RA) \times (WP - S_{i,G}) - WP\ if\ r_1 \leq 0.5 \end{cases} \tag{17}$$

In which $S_{\imath+1,G}$, $S_{\imath,G}$ demonstrates the next and present place of leaders correspondingly, WP implies the place of waterholes and r_1 is a random vector among zero and one.

2.3.5. Leaders' Exchange and Selection

At last, the group leader was chosen for obtaining an optimum fitness value. During all the iterations, the group leader was selected, whereas an optimum leader is obtained amongst the entire leaders from the iterations. This step is demonstrated by Equation (18):

$$S_{i,G} = \begin{cases} X_{i,G} if\ \cos t(X_{i,G}) < \ \cos t(S_{i,G}) \\ S_{i,G} if\ \cos t(X_{i,G}) > \ \cos t(S_{i,G}) \end{cases} \tag{18}$$

During this work, the ending condition is for performing the optimized procedure up to the maximal count of iterations (Max. It). The optimized approach was computed employing 100 iterations, with a population size of 30.

Algorithm 1: Pseudocode of WHO algorithm

```
Arbitrary initiation of the primary horse population
Parameter initiatin
Determine fitness of Horses
Produce Foal groups and elect Stallions
Determine optimum horse
While the stopping criteria were unsatisfied
Determine TDR
For the number of Stallions
    Find $Z$
    For the number of Foals under various groups
        If rand $> PC$
            Update foal position
        End
    End
    If rand > 0.5
        Update $\overline{Stallion_G}$ position
    Else
        Update $\overline{Stallion_{Gi}}$ b position
    End
    If cost$\left(\overline{Stallion_{\ Gi}}\right) < cost$(Stallion)
        Stallion $= \overline{Stallion_{Gi}}$
    End
    Arrange Foals of the group by cost
    Elect Foal with the least cost
    If the cost (Foa1) < cos (Stallion)
        Swap Foal and Stallion position
    End
End
Upgrade optimal
End
```

An important objective of the WHOMHR approach is maximizing network lifespan and minimizing energy consumption of all drones [21]. Assuming that $h1$ is a most main function such that CHs select next-hop CHs with superior RE to route the data such that for maximizing the network lifespan viz., $h1$ is maximized. Consider $h2$ to be another objective function that is minimal distance amongst CHs to next-hop CHs and next-hop CHs to BS. Decreasing the energy consumption of networks requires minimizing the $h2$. Assume that $h3$ is the 3rd objective function such that CHs are select as the next-hop CHs with lesser node degree. To enhance the network, lifespan requires minimizing h_3. Let b_{ij} be a Boolean variable determined as:

$$b_{\text{ ij}} = \begin{cases} 1\ if\ next - hop(CH_i) = CH_j, & \forall_{i,j} 1 \le i,\ j \le m \\ 0 & Otherwise \end{cases} \tag{19}$$

$$Minimize\ F = 1/h_1 \times \beta_1 + h_2 \times \beta_2 + h_2 \times \beta_3 \tag{20}$$

subject to,

$$dis\left(CH_i,\ CH_j\right) \times \le d_{\text{ max}}\ CH_j \in \{C + BS\} \tag{21}$$

$$\sum_{j=1}^{m} b_{ij} = 1\ and\ 1 \ne j \tag{22}$$

$$0 < \beta_1,\ \beta_2,\ \beta_3 < 1 \tag{23}$$

3. Results and Discussion

In this section, the secure communication performance of the DMOSC-MHRS model is investigated in detail. The proposed model is simulated using MATLAB under three different scenarios based on grid size.

- Scenario-1: Grid size of 1000 × 1000 m^2
- Scenario-2: Grid size of 2000 × 2000 m^2
- Scenario-3: Grid size of 3000 × 3000 m^2

Table 1 and Figure 2 highlight the cluster building time (CBT) of the DMOSC-MHRS approach under varying drones with existing methods such as the hybrid self-organized clustering scheme (HSCS), bio-inspired clustering scheme for FANET (BICSF), and SCA-ITV [22]. The experimental values indicated that the DMOSC-MHRS algorithm has demonstrated enhanced results under all drones. For example, with 15 drones, the DMOSC-MHRS model offered a lower CBT of 0.33 s whereas the SCA-ITV, BICSF, and HSCS algorithms obtained higher CBT of 0.61 s, 0.44 s, and 0.44 s, correspondingly. In line, with 20 drones, the DMOSC-MHRS approach presented a lower CBT of 0.47 s whereas the SCA-ITV, BICSF, and HSCS methods acquired higher CBT of 0.84 s, 0.70 s, and 0.59 s, correspondingly. Along with 25 drones, the DMOSC-MHRS technique has presented a lower CBT of 0.62 s whereas the SCA-ITV, BICSF, and HSCS algorithms gained higher CBT of 1.05 s, 0.86 s, and 0.79 s, correspondingly.

Table 1. CBT analysis of DMOSC-MHRS approach with existing algorithms under distinct drones.

Cluster Building Time (s)				
No. of Drones	**SCA-ITV**	**BICSF**	**HSCS**	**DOC-MHRS**
15	0.61	0.44	0.44	0.33
20	0.84	0.70	0.59	0.47
25	1.05	0.86	0.79	0.62
30	1.19	1.06	0.92	0.73
35	1.25	1.14	1.11	0.89

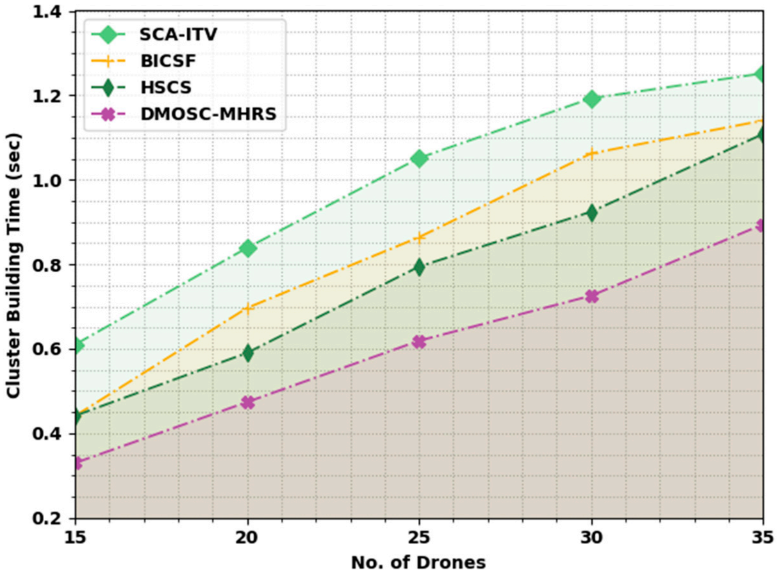

Figure 2. CBT analysis of DMOSC-MHRS approach under distinct drones.

Table 2 presents an overall energy consumption (ECM) inspection of the DMOSC-MHRS algorithm with recent models on different scenarios. Figure 3 reports a comparative ECM assessment of the DMOSC-MHRS technique with existing models on Scenario-1.

Table 2. ECM analysis of DMOSC-MHRS approach with existing algorithms under distinct scenarios.

	Energy Consumption (J)			
No. of Drones	**SCA-ITV**	**BICSF**	**HSCS**	**DMOSC-MHRS**
		Scenario-1		
15	0.61	0.44	0.44	0.33
20	0.84	0.70	0.59	0.47
25	1.05	0.86	0.79	0.62
30	1.19	1.06	0.92	0.73
35	1.25	1.14	1.11	0.89
		Scenario-2		
15	1.73	1.66	1.39	1.07
20	2.81	2.49	2.25	1.47
25	3.57	3.30	2.91	2.11
30	4.37	3.90	3.20	2.76
35	4.66	4.14	3.77	3.02
		Scenario-3		
15	2.78	2.03	1.77	1.23
20	3.38	2.74	2.58	1.95
25	3.95	3.52	3.18	2.55
30	4.52	4.04	3.66	2.91
35	4.66	4.46	3.95	3.45

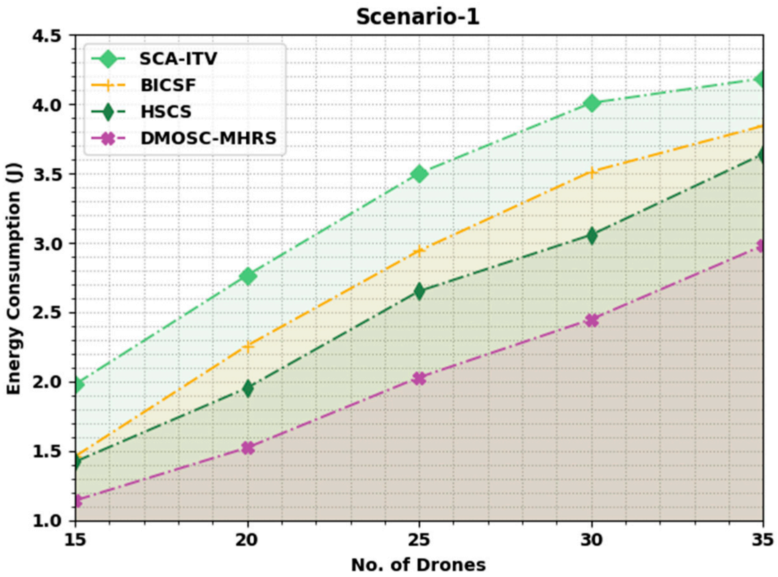

Figure 3. ECM analysis of DMOSC-MHRS approach under Scenario-1.

The figure indicates that the DMOSC-MHRS approach shows enhanced results with minimal ECM values. For instance, with 15 drones, the DMOSC-MHRS model gained the least ECM of 0.33 J whereas the SCA-ITV, BICSF, and HSCS models obtained higher ECM of 0.61 J, 0.44 J, and 0.44 J, respectively. In the meantime, with 20 drones, the DMOSC-MHRS approach has achieved the least ECM of 0.47 J whereas the SCA-ITV, BICSF, and HSCS methodologies obtained higher ECM of 0.84 J, 0.70 J, and 0.59 J, correspondingly. In due course, with 25 drones, the DMOSC-MHRS method acquired the least ECM of 0.62 J whereas the SCA-ITV, BICSF, and HSCS algorithms reached higher ECM of 1.05 J, 0.86 J, and 0.79 J, correspondingly.

Figure 4 reports a brief ECM assessment of the DMOSC-MHRS methodology with existing models in Scenario-2. The figure denoting the DMOSC-MHRS approach shows enhanced results with minimum ECM values. For example, with 15 drones, the DMOSC-MHRS approach gained least ECM of 1.07 J whereas the SCA-ITV, BICSF, and HSCS models obtained higher ECM of 1.73 J, 1.66 J, and 1.39 J, correspondingly. Simultaneously with 20 drones, the DMOSC-MHRS approach attained the least ECM of 1.47 J whereas the SCA-ITV, BICSF, and HSCS techniques obtained higher ECM of 2.81 J, 2.49 J, and 2.25 J, correspondingly. Eventually, with 25 drones, the DMOSC-MHRS method acquired the least ECM of 2.11 J whereas the SCA-ITV, BICSF, and HSCS algorithms reached higher ECM of 3.57 J, 3.30 J, and 2.91 J, correspondingly.

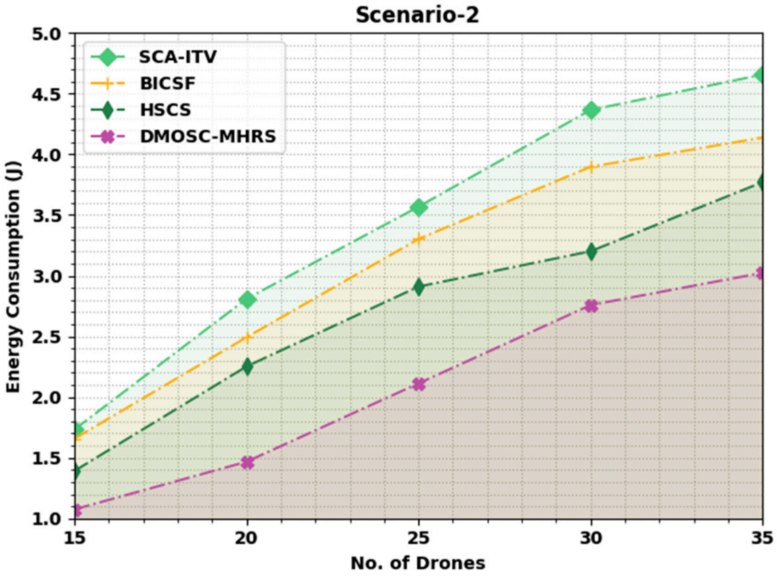

Figure 4. ECM analysis of DMOSC-MHRS approach under Scenario-2.

Figure 5 reports a comprehensive ECM assessment of the DMOSC-MHRS approach with existing models on Scenario-3. The figure representing the DMOSC-MHRS technique exhibits enhanced results with minimal ECM values. For example, with 15 drones, the DMOSC-MHRS model gained the least ECM of 1.23 J whereas the SCA-ITV, BICSF, and HSCS approaches reached higher ECM of 2.78 J, 2.03 J, and 1.77 J, correspondingly. Concurrently, with 20 drones, the DMOSC-MHRS approach attained the least ECM of 1.95 J whereas the SCA-ITV, BICSF, and HSCS methodologies obtained higher ECM of 3.38 J, 2.74 J, and 2.58 J, correspondingly. Similarly, with 25 drones, the DMOSC-MHRS model gained the least ECM of 2.55 J whereas the SCA-ITV, BICSF, and HSCS approaches reached higher ECM of 3.95 J, 3.52 J, and 23.18 J, correspondingly.

A comprehensive cluster lifetime (CLT) inspection of the DMOSC-MHRS model with other models is performed on different scenarios in Table 3. Figure 6 performs a comparative analysis of the DMOSC-MHRS technique with recent models in Scenario-1. The figure highlights that the DMOSC-MHRS algorithm displays enhanced performance with maximal CLT values under all drones. For example, with 15 drones, the DMOSC-MHRS methodology attained enhanced results with improved CLT of 52.34 s whereas the SCA-ITV, BICSF, and HSCS models obtained reduced CLT of 36.73 s, 46.37 s, and 48.67 s, respectively. Also, with 25 drones, the DMOSC-MHRS approach reached enhanced results with improved CLT of 50.35 s whereas the SCA-ITV, BICSF, and HSCS approaches gained reduced CLT of 32.60 s, 40.41 s, and 44.54 s, correspondingly. Along with 35 drones, the DMOSC-MHRS technique reached enhanced results with improved CLT of 48.36 s whereas the SCA-ITV, BICSF, and HSCS models obtained reduced CLT of 28.78 s, 34.74 s, and 37.65 s, correspondingly.

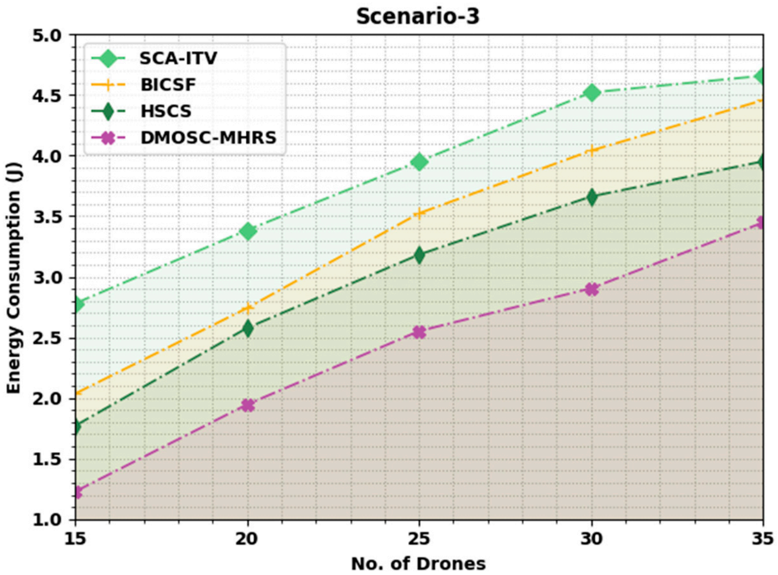

Figure 5. ECM analysis of DMOSC-MHRS approach under Scenario-3.

Table 3. CLT analysis of DMOSC-MHRS approach with existing algorithms under distinct scenarios.

		Cluster Life Time (s)		
No. of Drones	**SCA-ITV**	**BICSF**	**HSCS**	**DMOSC-MHRS**
		Scenario-1		
15	36.73	46.37	48.67	52.34
20	34.90	44.08	47.75	52.49
25	32.60	40.41	44.54	50.35
30	30.31	38.72	41.78	49.13
35	28.78	34.74	37.65	48.36
		Scenario-2		
15	43.85	50.78	52.78	55.71
20	40.78	48.63	51.09	54.78
25	37.70	44.78	47.86	53.24
30	36.00	42.62	46.16	50.32
35	32.77	38.77	41.39	49.70
		Scenario-3		
15	48.78	55.01	56.26	58.59
20	43.48	50.65	54.08	57.50
25	38.81	45.51	50.49	56.26
30	35.85	44.88	46.75	52.83
35	35.69	40.83	43.79	52.83

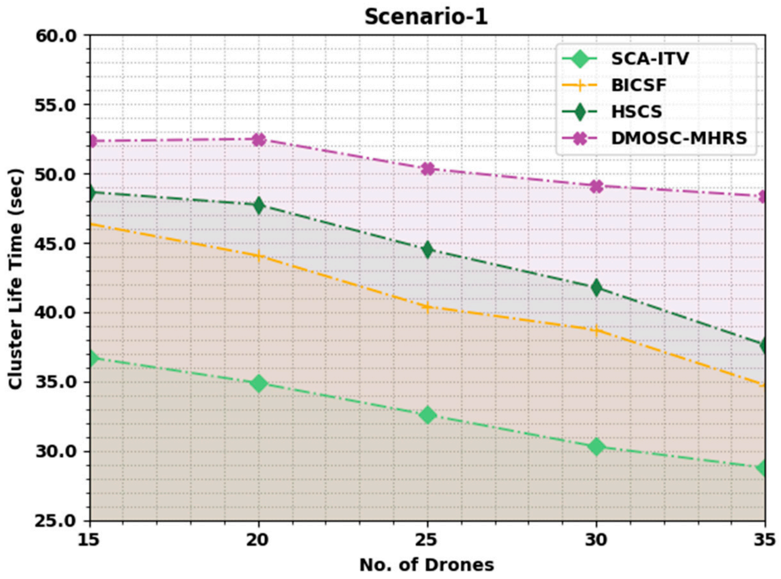

Figure 6. CLT analysis of DMOSC-MHRS approach under Scenario-1.

Figure 7 portrays a comparative analysis of the DMOSC-MHRS algorithm with recent models in Scenario-2. The figure highlights that the DMOSC-MHRS methodology shows enhanced performance with maximal CLT values under all drones. For example, with 15 drones, the DMOSC-MHRS approach attained enhanced results with an improved CLT of 55.71 s whereas the SCA-ITV, BICSF, and HSCS methodologies reached reduced CLT of 43.85 s, 50.78 s, and 52.78 correspondingly. Besides, with 25 drones, the DMOSC-MHRS model attained enhanced results with improved CLT of 53.24 s whereas the SCA-ITV, BICSF, and HSCS models obtained reduced CLT of 37.70 s, 44.78 s, and 47.86 s, correspondingly. Further, with 35 drones, the DMOSC-MHRS approach achieved enhanced results with improved CLT of 49.70 s whereas the SCA-ITV, BICSF, and HSCS models obtained reduced CLT of 32.77 s, 38.77 s, and 41.39 s, correspondingly.

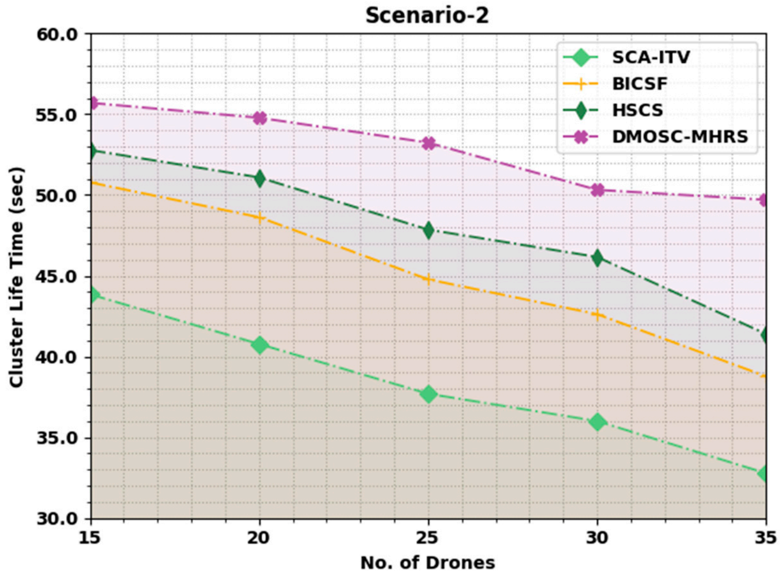

Figure 7. CLT analysis of DMOSC-MHRS approach under Scenario-2.

Figure 8 depicts a detailed study of the DMOSC-MHRS technique with recent models in Scenario-3. The figure points out that the DMOSC-MHRS approach displays enhanced performance with maximum CLT values under all drones. For example, with 15 drones, the DMOSC-MHRS approach attained enhanced results with an improved CLT of 58.59 s whereas the SCA-ITV, BICSF, and HSCS algorithms reached reduced CLT of 48.78 s, 55.01 s, and 56.26 s, correspondingly. Besides, with 25 drones, the DMOSC-MHRS technique gained enhanced results with improved CLT of 56.26 s whereas the SCA-ITV, BICSF, and HSCS techniques achieved reduced CLT of 38.81 s, 45.51 s, and 50.49 s, correspondingly. Along with 35 drones, the DMOSC-MHRS approach gained enhanced results with improved CLT of 52.83 s whereas the SCA-ITV, BICSF, and HSCS models obtained reduced CLT of 35.69 s, 40.83 s, and 43.79 s, correspondingly.

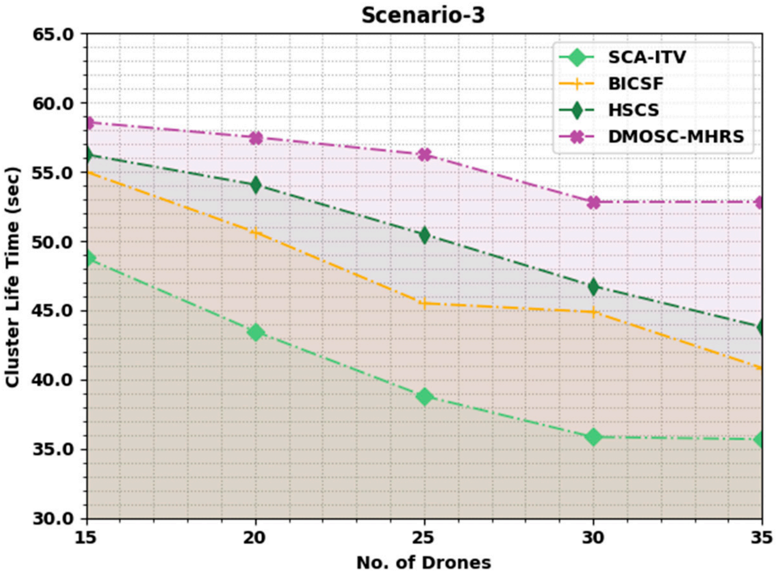

Figure 8. CLT analysis of DMOSC-MHRS approach under Scenario-3.

Table 4 and Figure 9 highlight the reliability (REL) of the DMOSC-MHRS model under varying drones. The experimental values indicate that the DMOSC-MHRS model has demonstrated enhanced results under all drones. For instance, with 15 drones, the DMOSC-MHRS model offered a higher REL of 94.29% whereas the SCA-ITV, BICSF, and HSCS techniques obtained lower REL of 87.36%, 89.13%, and 90.43%, respectively. Concurrently, with 20 drones, the DMOSC-MHRS approach presented a higher REL of 94.90% whereas the SCA-ITV, BICSF, and HSCS algorithms attained lower REL of 88.05%, 89.60%, and 91.06%, correspondingly. Concurrently, with 25 drones, the DMOSC-MHRS method rendered a higher REL of 94.98% whereas the SCA-ITV, BICSF, and HSCS approaches attained lower REL of 89.56%, 90.91%, and 92.52%, correspondingly. Finally, the experimental values demonstrated the enhanced performance of the DMOSC-MHRS model compared to recent models.

Table 4. Reliability analysis of DMOSC-MHRS approach with existing algorithms under distinct drones.

	Reliability (%)			
No. of Drones	**SCA-ITV**	**BICSF**	**HSCS**	**DMOSC-MHRS**
15	87.36	89.13	90.43	94.29
20	88.05	89.60	91.06	94.90
25	89.56	90.91	92.52	94.98
30	90.63	92.05	93.77	95.56
35	91.90	93.66	95.11	96.99

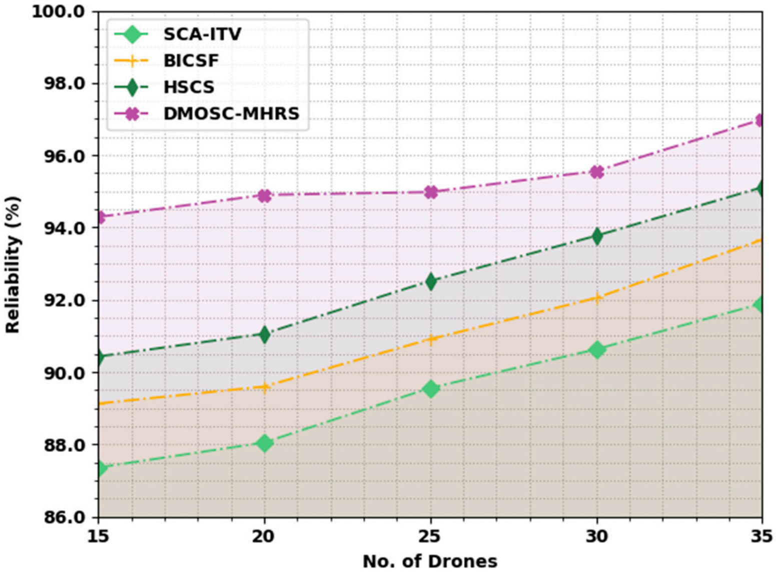

Figure 9. Reliability analysis of DMOSC-MHRS approach under distinct drones.

4. Conclusions

In this study, a new DMOSC-MHRS algorithm was devised for secure cluster-based communication in the IoD environment. The DMOSC-MHRS technique proficiently chooses CHs and optimal routes to a destination. In the presented DMOSC-MHRS approach, a new DMOSC technique is utilized to choose CHs and create clusters. A FF involving trust as a major factor is included to accomplish security. Besides, the DMOSC-MHRS technique designs a WHOMHR scheme for the optimal route selection process. To demonstrate the enhanced performance of the DMOSC-MHRS model, a comprehensive experimental assessment is made. Extensive comparison studies illustrate the better performance of the DMOSC-MHRS model over other approaches, with maximum reliability of 96.99%. Therefore, the proposed model can be employed in future real-time applications such as environmental monitoring, forest fire detection, disaster management, search and rescue, and smart cities. In the future, the performance of the DMOSC-MHRS algorithm can be enhanced by the utilization of data aggregation approaches, thereby enhancing overall network efficiency. In addition, the overall network performance can be improved by the use of unequal clustering techniques to mitigate hot spot problems.

Author Contributions: Conceptualization, F.S.A. and J.S.A.; methodology, K.A.A.; software, A.M.H.; validation, H.A., M.A.E. and A.Y.; formal analysis, A.Y.; investigation, A.M.; resources, A.M.; data curation, A.M.H.; writing—original draft preparation, F.S.A., A.A., J.S.A. and H.A.; writing—review and editing, K.A.A. and A.A.; visualization, A.M.; supervision, A.M.H.; project administration, J.S.A.; funding acquisition, F.S.A. and A.A. All authors have read and agreed to the published version of the manuscript.

Funding: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: 22UQU4340237DSR47. Research Supporting Project number (RSP2022R444), King Saud University, Riyadh, Saudi Arabia.

Data Availability Statement: Data sharing is not applicable to this article as no datasets were generated during the current study.

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

References

1. Rovira-Sugranes, A.; Razi, A.; Afghah, F.; Chakareski, J. A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook. *Ad Hoc Netw.* **2022**, *130*, 102790. [CrossRef]
2. Nazib, R.A.; Moh, S. Routing protocols for unmanned aerial vehicle-aided vehicular ad hoc networks: A survey. *IEEE Access* **2020**, *8*, 77535–77560. [CrossRef]
3. Gupta, V.; Seth, D. Design issues for developing routing protocols for flying ad hoc network. *Multimed. Technol. Internet Things Environ.* **2022**, *3*, 135–145.
4. Lagkas, T.; Argyriou, V.; Bibi, S.; Sarigiannidis, P. UAV IoT framework views and challenges: Towards protecting drones as "Things". *Sensors* **2018**, *18*, 4015. [CrossRef] [PubMed]
5. Alsamhi, S.H.; Shvetsor, A.V.; Shvetsova, S.V.; Hawbani, A.; Guizan, M.; Alhartomi, M.A.; Ma, O. Blockchain-Empowered Security and Energy Efficiency of Drone Swarm Consensus for Environment Exploration. *IEEE Trans. Green Commun. Netw.* **2022**. [CrossRef]
6. Gopi, S.P.; Magarini, M.; Alsamhi, S.H.; Shvetsov, A.V. Machine learning-assisted adaptive modulation for optimized drone-user communication in b5g. *Drones* **2021**, *5*, 128. [CrossRef]
7. Sharma, B.; Obaidat, M.S.; Sharma, V.; Hsiao, K.F. Routing and collision avoidance techniques for unmanned aerial vehicles: Analysis, optimal solutions, and future directions. *Int. J. Commun. Syst.* **2020**, *33*, e4628. [CrossRef]
8. Arafat, M.Y.; Moh, S. A survey on cluster-based routing protocols for unmanned aerial vehicle networks. *IEEE Access* **2018**, *7*, 498–516. [CrossRef]
9. Semiz, F.; Polat, F. Solving the area coverage problem with UAVs: A vehicle routing with time windows variation. *Robot. Auton. Syst.* **2020**, *126*, 103435. [CrossRef]
10. Wang, H.; Fang, H.; Wang, X. Safeguarding cluster heads in UAV swarm using edge intelligence: Linear discriminant analysis-based cross-layer authentication. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1298–1309. [CrossRef]
11. Fatemidokht, H.; Rafsanjani, M.K.; Gupta, B.B.; Hsu, C.H. Efficient and secure routing protocol based on artificial intelligence algorithms with UAV-assisted for vehicular ad hoc networks in intelligent transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4757–4769. [CrossRef]
12. Fu, Z.; Mao, Y.; He, D.; Yu, J.; Xie, G. Secure multi-UAV collaborative task allocation. *IEEE Access* **2019**, *7*, 35579–35587. [CrossRef]
13. Namdev, M.; Goyal, S.; Agarwal, R. An optimized communication scheme for energy efficient and secure flying ad-hoc network (FANET). *Wirel. Pers. Commun.* **2021**, *120*, 1291–1312. [CrossRef]
14. Zhao, L.; Saif, M.B.; Hawbani, A.; Min, G.; Peng, S.; Lin, N. A novel improved artificial bee colony and blockchain-based secure clustering routing scheme for FANET. *China Commun.* **2021**, *18*, 103–116. [CrossRef]
15. Ever, Y.K. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Comput. Commun.* **2020**, *155*, 143–149. [CrossRef]
16. Bhardwaj, V.; Kaur, N.; Vashisht, S.; Jain, S. SecRIP: Secure and reliable intercluster routing protocol for efficient data transmission in flying ad hoc networks. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4068. [CrossRef]
17. Khan, I.U.; Shah, S.B.H.; Wang, L.; Aziz, M.A.; Stephan, T.; Kumar, N. Routing protocols & unmanned aerial vehicles autonomous localization in flying networks. *Int. J. Commun. Syst.* **2021**, e4885. [CrossRef]
18. Aldosari, F.; Abualigah, L.; Almotairi, K.H. A Normal Distributed Dwarf Mongoose Optimization Algorithm for Global Optimization and Data Clustering Applications. *Symmetry* **2022**, *14*, 1021. [CrossRef]
19. Veerabadrappa, K.; Lingareddy, S.C. Secure Routing using Multi-Objective Trust Aware Hybrid Optimization for Wireless Sensor Networks. *Int. J. Intell. Eng. Syst.* **2022**, *15*, 540–548.
20. Ali, M.H.; Kamel, S.; Hassan, M.H.; Tostado-Véliz, M.; Zawbaa, H.M. An improved wild horse optimization algorithm for reliability based optimal DG planning of radial distribution networks. *Energy Rep.* **2022**, *8*, 582–604. [CrossRef]
21. Rao, P.C.; Lalwani, P.; Banka, H.; Rao, G. Competitive swarm optimization based unequal clustering and routing algorithms (CSO-UCRA) for wireless sensor networks. *Multimed. Tools Appl.* **2021**, *80*, 26093–26119. [CrossRef]
22. Aftab, F.; Khan, A.; Zhang, Z. Hybrid self-organized clustering scheme for drone based cognitive Internet of Things. *IEEE Access* **2019**, *7*, 56217–56227. [CrossRef]