applied sciences

MDPI

Article

Enhanced Search-and-Rescue Optimization-Enabled Secure Route Planning Scheme for Internet of Drones Environment

Fatma S. Alrayes [1], Sami Dhahbi [2,3], Jaber S. Alzahrani [4], Amal S. Mehanna [5], Mesfer Al Duhayyim [6,*], Abdelwahed Motwakel [7], Ishfaq Yaseen [7] and Amgad Atta Abdelmageed [7]

[1] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[2] Department of Information Systems, College of Science & Art at Mahayil, King Khalid University, Abha 62529, Saudi Arabia
[3] Research Team on Intelligent Systems in Imaging and Artificial Vision (SIIVA)—Lab LIMTIC, Higher Institute of Computer, University of Tunis EL Manar, Aryanah 2036, Tunisia
[4] Department of Industrial Engineering, College of Engineering at Alqunfudah, Umm Al-Qura University, Mecca 24382, Saudi Arabia
[5] Department of Digital Media, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo 11845, Egypt
[6] Department of Computer Science, College of Sciences and Humanities—Aflaj, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia
[7] Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia
* Correspondence: m.alduhayyim@psau.edu.sa

check for updates

Citation: S. Alrayes, F.; Dhahbi, S.; S. Alzahrani, J.; Mehanna, A.S.; Al Duhayyim, M.; Motwakel, A.; Yaseen, I.; Atta Abdelmageed, A. Enhanced Search-and-Rescue Optimization-Enabled Secure Route Planning Scheme for Internet of Drones Environment. *Appl. Sci.* **2022**, *12*, 7950. https://doi.org/10.3390/app12157950

Academic Editors: Mingcong Deng, Augusto Ferrante, Mihaiela Iliescu and Tai Yang

Received: 25 May 2022
Accepted: 30 July 2022
Published: 8 August 2022

Abstract: The Internet of Drones (IoD) is greatly developed and promotes many civil applications. However, it can still be prone to several security problems which threaten public safety. The issue of security poses further problems upon linking the IoD to the Internet, as its data stream is exposed to attack. For secure communication between drones, an effective route planning scheme with a major intention of accomplishing security is needed. With this aim, this study develops an enhanced search-and-rescue optimization-enabled secure route planning (ESRO-SRP) scheme for the IoD environment. The presented ESRO-SRP technique mainly aims to derive a set of optimal routes to the destination. In addition, the ESRO-SRP algorithm is derived by the integration of the quasi-oppositional-based learning (QOBL) concept with the conventional SRO algorithm. Moreover, the presented ESRO-SRP technique derived a fitness function encompassing different input parameters such as residual energy, distance, and degree of trust. The experimental validation of the ESRO-SRP technique is carried out under several aspects, and the results demonstrated the enhancements of the ESRO-SRP model over recent approaches. The ESRO-SRP model has provided an increased packet delivery ratio (PDR) of 86%, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm approaches have accomplished a minimal PDR of 79.60%, 73.60%, 67.60%, and 63.20%, respectively.

Keywords: Internet of Drones; search-and-rescue optimization; metaheuristics; security; route planning

1. Introduction

The use of unmanned aerial vehicles (UAVs), also termed drones, is anticipated to incline at exceptional rates because of growing curiosity from investors, hobbyists, and researchers; the quantity of drones is quickly rising, and the Internet of Drones (IoD) environment and number of related applications are expanding rapidly, in which an infinite number of multi-sized drones flawlessly communicate with one another via area service providers whose objective it is to understand and align the accessibility of drones to a controlled airspace and operate a navigation service [1]. The economic development of drone industries in the United States, involving military scouting, traffic, wildlife surveillance, urban safety scrutiny of infrastructure, on-demand package supply, aerial photography, etc., is reported to be substantial for industries or business operations [2,3]. Figure 1 depicts the procedure of IoD.

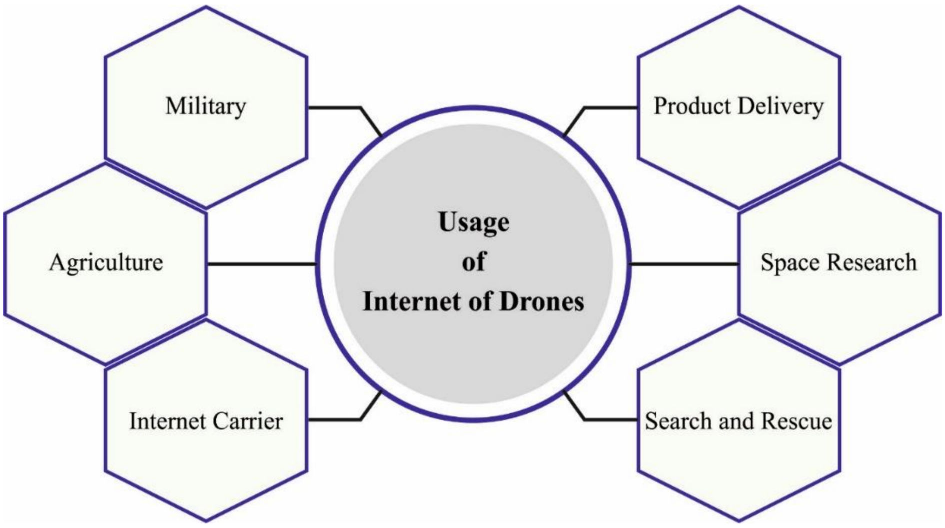

Figure 1. Application areas of IoD.

Even though the IoD network offers numerous benefits, it also carries numerous susceptibilities which should be handled, the most important criteria of which are privacy and security problems [4]. However, the IoD network system is commonly placed for real-time application zones where end users need to obtain real-time information from UAVs which are connected to a particular area. So, there are high chances of security assaults occurring, leading to the colossal ruin of the data exchange functions inside the network [5–7]. An attacker can gain access to the keys and block transmissions. For the accessibility of keys, the intruder can abuse a susceptibility in the IoD network and its application zones. The intruder might alter this information, resulting in the misguidance of the receivers. However, IoD access management is a significant variable, and security problems regarding authorization and accessibilities must be emphasized [8,9]. This applies to the data in transfer, which should be protected for confidentiality, authenticity, and integrity.

Most of the privacy and security methods advanced by authors were intended to ensure security measures on the IoD network [10,11]. The approaches focused on mitigating problems which influence the secure localization of drones or privacy and security necessities linked with the IoD network system. Localization fault assaults impede the reliability position of UAVs, leading to distressing costs for the overall functionality of the IoD network [12]. Additionally, privacy and security necessities are the objectives that decide the functions and capacities of the IoD network attained in justifying certain privacy and security measures [13]. The privacy and security needs of the IoD network involve authenticity, integrity, availability, privacy preservation, and confidentiality [14].

Tian et al. [15] suggested a powerful privacy-preserving validation architecture. With the help of a lightweight online/offline signature model, this architecture guarantees verification effectiveness while placing resource constraints on small-scale UAVs. Considering the high mobility of UAVs, a prediction validation model is explored by using mobile edge computing (MEC) in this architecture for reducing the verification expenses for possible verification activity. Allouch et al. [16] developed an Unmanned Traffic Management (UTM)-Chain, a light-weight blockchain-related security model with hyper ledger fabric for UTM of lower-altitude UAV that fits the storage and computation resource constraints of UAV. Furthermore, UTM-Chain offers secured and unchangeable traffic information among their ground control stations and the UAVs. In [8], a blockchain-related security model for cyber-physical systems is introduced for ensuring secured transmission of datasets amongst drones. In this model, the miner node is chosen by deep learning (DL)-based technique, that is, a deep Boltzmann machine, with features such as flight time of the drone, computation resource, and the available battery power.

The authors in [17] developed a lightweight user verification system where the client in the IoD environments needs to directly access information from a drone to show that the client is authorized for accessing the dataset from that drone. The formal security validation with the generally recognized automatic confirmation of Internet security protocol and application tool alongside informal security investigation shows that the suggested technique is secured against well-known attacks. In [18], the authors developed a Drone-map organizer, viz., a service-related fog-based drone managing scheme that monitors, communicates, and controls with drones through the networks. The suggested technique enables interaction with various drones through the internet that allows drones to be controlled anyplace and anywhere, with no long-distance restrictions. This model offers drones access to fog computational resources for drones to perform heavyweight load computation. Though existing works have focused on the IoD environment, it is still necessary to design energy-efficient and security-based solutions for the IoD environment with the inclusion of multiple input parameters of the drones.

This study develops an enhanced search-and-rescue optimization-enabled secure route planning (ESRO-SRP) scheme for the IoD environment. The presented ESRO-SRP technique mainly aims to derive a set of optimal routes to the destination. In addition, the ESRO-SRP algorithm is derived by the integration of the quasi-oppositional-based learning (QOBL) concept with the conventional SRO algorithm. Moreover, the presented ESRO-SRP technique derived a fitness function encompassing different input parameters such as residual energy (RE), distance, and trust degree. The experimental validation of the ESRO-SRP technique is carried out under several aspects. In short, the major contributions are summarized as follows.

- To the best of our knowledge, the ESRO-SRP technique for the IoD environment does not exist in the literature.
- Develop a new ESRO-SRP technique for a secure route selection process in the IoD environment.
- Derive an ESRO-SRP algorithm using the combination of QOBL with the traditional SRO algorithm and derive a fitness function involving multiple input parameters.
- Simulate the performance of the ESRO-SRP technique under varying levels of energy consumption in the IoD environment.

The rest of the paper is organized as follows. Section 2 offers a detailed discussion of the proposed model and Section 3 validates the experimental results of the proposed model. Finally, Section 4 concludes the study with key findings and possible future enhancements.

2. Materials and Methods

In this study, a novel ESRO-SRP technique has been developed for secure communication among drones in the IoD environment. The presented ESRO-SRP technique mainly aims to derive a set of optimal routes to the destination. In addition, the ESRO-SRP algorithm is derived by the integration of the QOBL concept with the conventional SRO algorithm. Moreover, the presented ESRO-SRP technique derived a fitness function encompassing different input parameters such as RE, distance, and trust degree.

2.1. Overview of ESRO-SRO Algorithm

In the SRO approach, the human position is equal to the resolution of the optimization issues, and the clue quantity accomplished in the location characterizes the objective function. The group members gather clue information in the search. Few clues are absent in the event of gaining optimal clues in another position, but the dataset is exploited for optimizing the searching technique [19]. Here, the position of the left clue can be stored in the (M memory matrix), where the position of the human is stored in the (X position matrix). The M matrix dimension is the same as X. They are $N \times D$ matrices, whereas D symbolizes problem dimension and N embodies human count. The clue matrixes have the attained clue position. The M and C matrixes are upgraded in all human searching processes [19]:

$$C = \left\{ \begin{matrix} X \\ M \end{matrix} \right\} = \left\{ \begin{matrix} X_{11} & \cdots & X_{1D} \\ \vdots & \ddots & \vdots \\ X_{N1} & \cdots & X_{ND} \\ M_{11} & \cdots & M_{1D} \\ \vdots & \ddots & \vdots \\ M_{N1} & \cdots & M_{ND} \end{matrix} \right\}, \tag{1}$$

In Equation (1), X and M represent the position of human and memory matrixes; correspondingly, X_{N1} embodies the position of initialized dimension for N^{th} human, and M_{1D} characterizes D^{th} dimensional position for the preliminary memory. Given the description presented in the previous section, in addition to an arbitrary clue amid accomplished clues, the search path is described as follows:

$$\mathrm{SD}_i = (\mathrm{X}_i - \mathrm{C}_k)\ ,\ k \neq i, \tag{2}$$

In Equation (2), X_i, C_k, and SD_i correspondingly symbolize j^{th} human location, the k^{th} clue location, and j^{th} human searching direction; k suggests arbitrary numbers within 1 and $2N$ and appropriately chosen $k \neq i$. It is important to emphasize that human usually seeks accordingly, and some repetitious positions could not be searched another time. Henceforth, the search should be generated if the group member is restrained. Therefore, X_j dimension could not be rehabilitated.

For applying this constraint, the binomial crossover operator has been exploited when the clue is larger than that of the clue associated with the present position, an SD_j direction and the position of that search clue; next, the searching method undergoes the present location beside the SD_i direction [16].

$$X'_{i,j=} \left\{ \begin{matrix} \left\{ \begin{matrix} \mathrm{C}_{k,j} + r\mathrm{l} \times \left(\mathrm{X}_{i,j} - \mathrm{C}_{k,j}\right), if\ f(\mathrm{C}_k) >, f(\mathrm{X}_i) \\ \mathrm{X}_{\mathrm{i},j} + r\mathrm{l} \times \left(\mathrm{X}_{i,j} - \mathrm{C}_{k,j}\right), otherwise \end{matrix} \right. & \begin{matrix} if\ r2 < \mathrm{SEor}\ j = j_{rand}, \\ otherwise, \end{matrix} (j = 1,\ \ldots,\ D), \\ \mathrm{X}_{i,j} & \end{matrix} \right. \tag{3}$$

where the following are defined: $X'_{i,j}$ symbolizes the novel place of j^{th} parameters of i^{th} humans; $C_{k,\ j}$ specifies place of j^{th} parameter for the k^{th} accomplished clues; $f(C_k)$ and $f(X_i)$ correspondingly imply an objective function for the C_k and X_i solution; $r\mathrm{l}$ and $r2$ epitomize arbitrary value; j_{rand} symbolizes arbitrary value within 1 and D that assures that 1D of $X'_{i,j}$ is varied from $X_{i,j}$. Equation (3) is applied to accomplish a new place of j^{th} human in all dimensions.

Next, humans search nearby the current place, and the concept of related discrete clues applied in the social phase is exploited for searching. In conflict with the social phase, X_i dimension is attuned in the separation phase. The novel place of j^{th} human can be accomplished as follows [16]:

$$X'_i = X_j + r3 \times (C_k - C_m)\ ,\ i \neq k \neq m, \tag{4}$$

In Equation (4), k and m characterize arbitrary numbers within 1 and $2N$. To evade motion besides another clue, k and m are designated in this manner, such that $i \neq k \neq m$. $r3$ symbolizes an arbitrary value between zero and one. In the metaheuristic method, each solution should be positioned in the solution region, and when they are farther from the permitted solution region, they should be altered. If the novel place of a human is farther from the solution region, the succeeding equation is exploited for altering the novel place:

$$X'_{i,j}=\begin{cases} \frac{\left(X_{i,j}+X_j{}^{max}\right)}{2}, if\ X'_{i,j} > x_j^{max}, \\ \frac{\left(X_{i,j}+X_j{}^{min}\right)}{2}, if\ X'_{i,j} < x_j^{min}, \end{cases} \begin{pmatrix} j \\ = 1, \ldots,\ D \end{pmatrix} \tag{5}$$

The process involved in the SRO algorithm is given in Algorithm 1.

Next, in all iterations, the member of the group searched according to the two phases, and after each stage, once the value of the main function is in position, $X'_i(f(X'_i))$ is greater than that of the preceding one $(f\ (X_i))$, thus the earlier position (X_i) would be stored in an arbitrary place of the M memory matrix and it would be adopted as a novel place. If not, the position is left and memory is not improved:

$$M_n = \begin{cases} X_i, if\ f\ (X'_i) >, f(X_i) \\ M_n,\ \text{otherwise} \end{cases} \tag{6}$$

$$X_i = \begin{cases} X'_i, if\ f\ (X'_i) >, f(X_i) \\ X_i,\ \text{otherwise,} \end{cases} \tag{7}$$

where M_n indicates the location of n^{th} clue saved in the M, and n represents arbitrary numbers within 1 and N. With that memory, upgrading increases the different kinds of techniques and the ability of methods for detecting a globally optimum solution. Firstly, the unsuccessful search number (USN) is fixed as zero for all human beings. Once the human discovers an optimal clue in the first and second stages of the searching technique, the USN is fixed as zero for that human; if not, it raises it by one point as follows [16]:

$$\text{USN}_i = \begin{cases} \text{USN}_i + 1, if\ f(X'_i) <, f(X_j) \\ 0, or\ else \end{cases} \tag{8}$$

The arbitrary place from the search region is represented in the following equation and USN$_i$ is fixed as zero for that human:

$$X_{i,j} = X_j^{\text{min}} + r4 \times \left(X_j^{\text{max}} - X_j{}^{\text{min}}\right) j = 1,\ \ldots,\ D, \tag{9}$$

In Equation (9), $r4$ designates an arbitrary value and is discrete for each dimension. Tizhoosh proposed the concept of oppositional-based learning (OBL) that includes opposite numbers having the highest possibility of accomplishing a solution compared to arbitrary numbers. The incorporation of OBL with the SRO method leads to an improved convergence rate and effective result of the presented ESRO-SRP algorithm. The QOBL method applies quasi-opposite value efficiently through the opposite number in the global optimal outcome. Assume χ represents a real number in I-dimensional region. The x^o and x^{qo}(of x) opposite and quasi-opposite numbers are shown in the following [20]:

$$x^0 = a + b - x \tag{10}$$

In which $x \in \mathbb{R}$ and $\in b]$.

$$x^{qo} = rand\left(\frac{a+b}{2},\ x^0\right) \tag{11}$$

Let $X(x_1,\ x_2,\ \ldots,\ x_n)$ be a point from the n-dimensional region. The opposite point, $X^o\left(x_1^o,\ x_2^o,\ \ldots,\ x_n^0\right)$ and quasi-opposite point, $X^{qo}\left(x_1^{qo},\ x_2^{qo},\ \ldots,\ x_n^{qo}\right)$ are shown in the following.

$$x_i^o = a_i + b_i - x_i \tag{12}$$

Algorithm 1: Pseudo-code of the SRO algorithm

```
Begin
Initialize parameters : Arbitrary population initialization of 2N solutions, $\left[X_j^{min}, X_j^{max}\right]$, $j = 1, \ldots, D$
Organize the solution in a decreasing manner and decide the optimal location (Xbest)
Exploit the 1st half of the organized outcome for $X$ and the remaining for $M$
Represent variables (SE, MU) and set the $\mathrm{USN}_i = 0$ where $i = 1, \ldots, N$
While end criteria are not met do
    For $i = 1$ to $N$ do
        $\mathrm{C} = \left\{ \begin{matrix} X \\ M \end{matrix} \right\}$   //Social Phase
        $\mathrm{SD}_j = \left(X_j - \mathrm{C}_k\right)$, $k$ was chosen arbitrarily that $i \neq k$
        $j_{\mathrm{rand}} =$ rand int $[1, D]$
        $r1 =$ rand $[-1, 1]$
        For $j = 1$ to $D$ do
            $X'_{i,j} = \left\{ \begin{cases} \mathrm{C}_{k,j} + r1 \times SD_{i,j}, & if\ f(\mathrm{C}_k) > f(X_i), \\ X_{i,j} + r1 \times SD_{i,j}, & otherwise \end{cases} \right.$
            $X'_{i,j} = \begin{cases} \left(X_{i,j} + X_j^{max}\right)/2, & \text{if } X'_{i,j} > X_j^{max} \\ \left(X_{i,j} + X_j^{min}\right)/2, & \text{if } X'_{i,j} < X_j^{min} \end{cases}$
        End For
        $M_n = \begin{cases} X_i, & \text{if } f\left(X'_i\right) > f(X_i), \\ M_n, & otherwise \end{cases}$
        $X_i = \begin{cases} X'_i, \text{ if } f\left(X'_i\right) > f(X_i) \\ X_i,\ otherwise \end{cases}$
        $\mathrm{USN}_i = \begin{cases} \mathrm{USN}_i + 1, \text{ if} f\left(X'_i\right) < f(X_i) \\ 0,\ otherwise \end{cases}$
        $\mathrm{C} = \left\{ \begin{matrix} X \\ M \end{matrix} \right\}$   //Individual Stage
        $X'_i = X_i +$ rand $[0, 1] \times (\mathrm{C}_k - \mathrm{C}_m)$,
        For $j = l$ to $D$ do
            $X'_{i,j} = \begin{cases} \left(X_{i,j} + X_j^{max}\right)/2, & \text{if } X'_{i,j} > X_j^{max} \\ \left(X_{i,j} + X_j^{min}\right)/2, & \text{if } X'_{i,j} > X_j^{min} \end{cases}$
        End For
        $M_n = \begin{cases} X_i, & \text{if } f\left(X'_i\right) > f(X_i), \\ M_n, & otherwise \end{cases} n\ randomly\ chosen$
        $X_i = \begin{cases} X_i \text{ if } f\left(X'_j\right) > f(X_i) \\ X_i \text{ otherwise} \end{cases}$
        $\mathrm{USN}_i = \begin{cases} \mathrm{USN}_i + 1, \text{ if } f\left(X'_i\right) < f(X_i) \\ 0, otherwise \end{cases}$
        If the $\mathrm{USN}_i >$ MU do
            For $j = l$ to $D$ do
                $X_{i,j} = X_j^{mini} +$ rand $[0, 1] \times \left(X_j^{maxi} - X_j^{mini}\right)$
            End for
            $\mathrm{USN}_i = 0$
        End If
    End for
    Decide the existing finest place and upgrade Xbest
End while
Return Xbest
End
```

Here, $x_i \in \mathbb{R}$ and $x_i \in [a_i,\ b_i] \forall i \in 1,\ 2,\ \ldots,\ n$.

$$x_i^{qo} = rand\left(\frac{a_i + b_i}{2},\ x_i^o\right) \tag{13}$$

In QOBL is exploited to the SRO algorithm to initialize the population as well as creation jumping. It generates a group of optimum outcomes for population initialization [8]. Algorithm 2 defines the QOBL pseudo-code to the novel population.

Algorithm 2: Pseudo-code of QOBL

```
for $i = 1 :\ Eco\_size$
    for $j = 1 :\ D$
        $X_{i,j}^o = lb_j + up_j - X_{i,j};$
        $C_{i,j} = \left(lb_j + up_j\right)/2;$
        if $(X_{i,j} < C_{i,j})$
                $X_{i,j}^{qo} = C_{i,j} + \left(X_{i,j}^o - C_{i,j}\right) \times rand;$
        else
                $X_{i,j}^{qo} = X_{i,j}^o + \left(C_{i,j} - X_{i,j}^o\right) \times rand;$
        end if
    end for
end for
```

2.2. Process Involved in ESRO-SRP Technique

To define an optimum group of routes, an offered function was employed to determine the following hop to destination and is represented by:

$$f(x) = \left\{i,\ for\ which\left|\left(\frac{i}{k} - X_{i_{fj}}\right)\right| is\ minimum,\ \forall_i 1 \le i \le k \right. \tag{14}$$

The drive is to determine an optimum group of routes from the cluster heads (CHs) to the base station (BS), employing a fitness function (FF) comprising 2 parameters such as energy and distance. Primarily, the RE of the next-hop node is determined, and a node with higher energy was provided as a relay node. To transfer data, the source node sends it to the relay node, which is further forwarded to BS utilizing inter CHs. Thus, the node with higher RE is provided as the next-hop node. A primary sub-objective $f1$ was offered as:

$$f1 = E_{CH} \tag{15}$$

In addition, the Euclidean distance was executed to define the distance from CH to BS. The minimized energy dissipation was frequently dependent on the broadcast distances. With a lesser distance, the energy was retained significantly [21]. Once the distance is improved, a further count of energy is spent. Hence, the node with lesser distances is chosen to relay nodes. So, the next sub-objective using distance is $f2$ which is formulated as:

$$f2 = \frac{1}{\sum_{i=1}^{m} d\ is(CH_i,\ NH) + dis(NH,\ BS)} \tag{16}$$

The present research work utilized direct trust values (TVs) amongst drones, and their mathematical process was signified as:

$$f3 = Trust \tag{17}$$

$$Tr_{i,j} = \left(Tr_{ij}^{Dir} + Tr_{ij}^{Indir}\right)/2. \tag{18}$$

Here, Tr_{ij}^{dir} and Tr_{ij}^{indir} denotes the direct as well as indirect TVs of one node to another node correspondingly. The count of trust nodes from the cluster is attained in the group with maximal TVs, and their state value was provided by the level of confidence values suggested in one node to another node. The TV of BS was computed as:

$$Tr_C = \sum_{j=1}^{S-1} Tr_{C(i,j)}/(S-1). \tag{19}$$

In the above formula, Tr_C refers to the trusted value and S represents the amount of drones. If the path trust was smaller than the trust requirement value, the path trust alert occurrence was triggered.

The above-mentioned sub-objective was revised as to FF as offered in that α_1 and α_2 denotes the weight assigned to every sub-objective.

$$Fitness = \alpha_1(f1) + \alpha_2(f2) + \alpha_1(f3),\ where \sum_{i=1}^{3} \alpha_i = 1\alpha_i\varepsilon(0,1); \tag{20}$$

3. Results and Discussion

In this section, the performance validation of the ESRO-SRP model is examined under distinct levels of energy consumption (EC). The EC is varied from 5% to 100% with a step size of 5%. Table 1 and Figure 2 report a comparative throughput (THRP) inspection of the ESRO-SRP model with recent models under distinct levels of energy [22–25]. The results portrayed that the ESRO-SRP model has accomplished maximum values of THRP under all energy levels. For instance, with an EC of 5%, the ESRO-SRP model has provided an increased THRP of 33.95 bytes/s, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm models have accomplished a reduced THRP of 14.54 bytes/s, 14.54 bytes/s, 9.69 bytes/s, and 7.75 bytes/s, respectively. Moreover, with an EC of 100%, the ESRO-SRP system has offered a maximal THRP of 189.20 bytes/s, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm techniques have accomplished a lower THRP of 165.91 bytes/s, 140.68 bytes/s, 110.60 bytes/s, and 99.93 bytes/s, respectively.

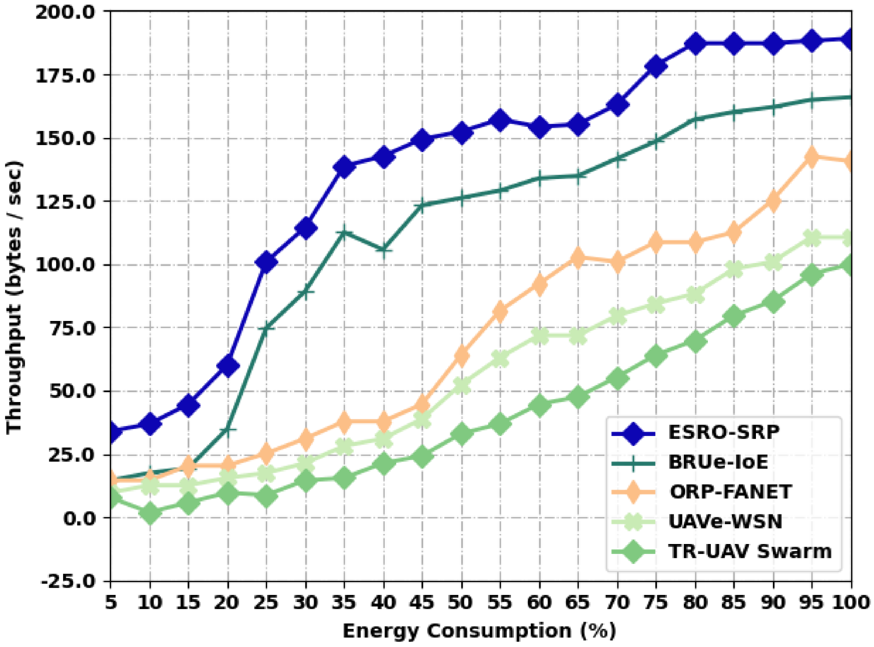

Figure 2. Throughput analysis of ESRO-SRP technique under distinct levels of energy.

Table 1. Throughput analysis of ESRO-SRP technique with existing algorithms under distinct levels of energy.

Throughput (bytes/s)					
EC (%)	**ESRO-SRP**	**BRUe-IoE**	**ORP-FANET**	**UAVe-WSN**	**TR-UAV Swarm**
5	33.95	14.54	14.54	9.69	7.75
10	36.86	17.45	14.54	12.60	1.93
15	44.62	19.39	20.36	12.60	5.81
20	60.15	34.92	20.36	15.51	9.69
25	100.90	74.70	25.21	17.45	8.72
30	114.48	89.26	31.04	21.33	14.54
35	138.74	112.54	37.83	28.12	15.51
40	142.62	105.75	37.83	31.04	21.33
45	149.42	123.22	44.62	38.80	24.24
50	152.33	126.13	64.03	52.38	32.98
55	157.18	129.04	81.49	63.06	36.86
60	154.27	133.89	92.17	71.79	44.62
65	155.24	134.86	102.84	71.79	47.53
70	163.00	141.65	100.90	79.55	55.29
75	178.53	148.45	108.66	84.40	64.03
80	187.26	157.18	108.66	88.28	69.85
85	187.26	160.09	112.54	97.99	79.55
90	187.26	162.03	125.16	100.90	85.37
95	188.23	164.94	142.62	110.60	96.05
100	189.20	165.91	140.68	110.60	99.93

Table 2 and Figure 3 define a comparative PDR examination of the ESRO-SRP approach with recent models under distinct levels of energy. The results exposed that the ESRO-SRP model has accomplished maximal values of PDR under all energy levels. For example, with an EC of 5%, the ESRO-SRP model has provided an increased PDR of 65.20%, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm systems have accomplished a decreased PDR of 58.40%, 49.60%, 40.80%, and 39.20%, respectively. Additionally, with an EC of 100%, the ESRO-SRP model has provided an increased PDR of 86%, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm approaches have accomplished a minimal PDR of 79.60%, 73.60%, 67.60%, and 63.20%, respectively.

Table 3 and Figure 4 demonstrate a comparative average HOPS (AHOPS) analysis of the ESRO-SRP system with recent models under distinct levels of energy. The results depicted that the ESRO-SRP approach has accomplished higher AHOPS values under all energy levels. For instance, with an EC of 5%, the ESRO-SRP model has provided an increased AHOPS of 9%, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm algorithms have accomplished a minimal AHOPS of 7%, 5%, 5%, and 2%, respectively. Finally, with an EC of 100%, the ESRO-SRP model has offered superior AHOPS of 23%, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm methodologies have accomplished a lower AHOPS of 22%, 21%, 11%, and 7% correspondingly.

Table 2. PDR analysis of ESRO-SRP technique with existing algorithms under distinct levels of energy.

Packet Delivery Ratio (%)					
EC (%)	**ESRO-SRP**	**BRUe-IoE**	**ORP-FANET**	**UAVe-WSN**	**TR-UAV Swarm**
5	65.20	58.40	49.60	40.80	39.20
10	64.80	60.00	50.00	42.00	39.60
15	66.00	60.00	53.20	46.80	39.60
20	70.80	61.60	54.00	46.40	42.00
25	72.40	64.00	56.00	47.60	43.60
30	73.20	66.40	56.40	50.00	44.80
35	74.40	66.40	57.60	51.60	46.40
40	74.40	66.40	59.20	53.60	48.00
45	75.20	66.00	60.00	54.00	50.80
50	76.40	67.20	61.60	54.40	50.00
55	76.00	68.00	61.60	54.40	50.80
60	76.40	69.60	64.40	55.20	51.60
65	78.40	72.80	64.80	58.40	52.80
70	80.40	73.60	66.80	59.20	54.00
75	83.20	75.20	70.00	61.20	54.40
80	81.60	76.80	71.60	62.80	56.40
85	86.00	77.60	71.60	64.00	59.20
90	85.60	79.20	72.80	64.80	61.20
95	89.20	80.40	73.20	65.60	60.00
100	86.00	79.60	73.60	67.60	63.20

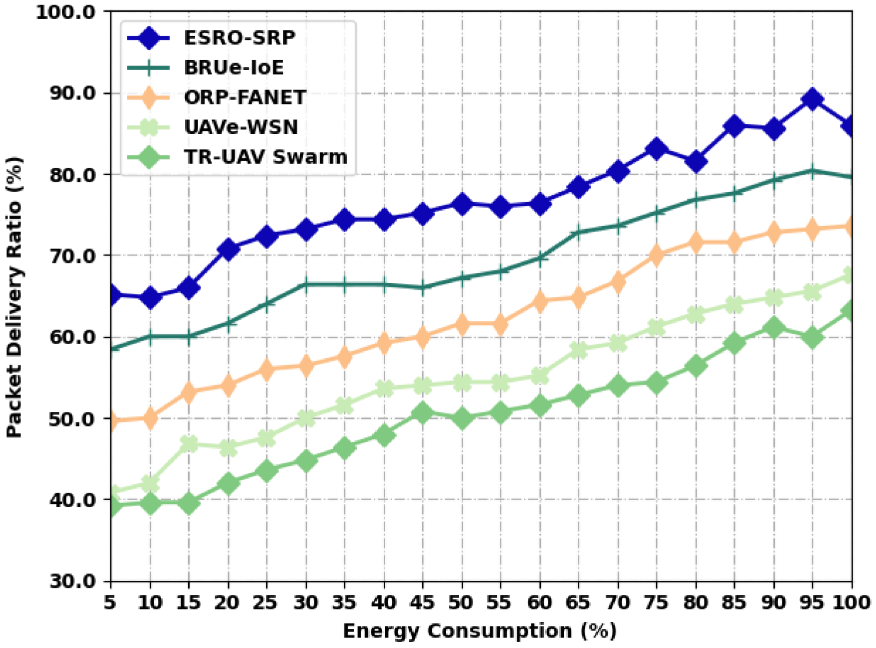

Figure 3. PDR analysis of ESRO-SRP technique under distinct levels of energy.

Table 3. Average HOPS analysis of ESRO-SRP technique with existing algorithms under distinct levels of energy.

Average HOPS (%)					
EC (%)	**ESRO-SRP**	**BRUe-IoE**	**ORP-FANET**	**UAVe-WSN**	**TR-UAV Swarm**
5	9	7	5	5	2
10	9	7	6	5	2
15	10	7	6	5	2
20	11	8	6	5	2
25	14	10	8	5	2
30	16	12	9	5	3
35	16	12	10	6	3
40	16	13	10	6	4
45	17	14	11	6	4
50	17	14	11	7	3
55	18	15	11	7	4
60	20	15	12	8	4
65	20	15	12	8	5
70	21	16	12	9	6
75	21	18	13	9	6
80	21	18	15	9	6
85	22	19	18	10	7
90	24	20	18	10	7
95	24	22	20	10	6
100	23	22	21	11	7

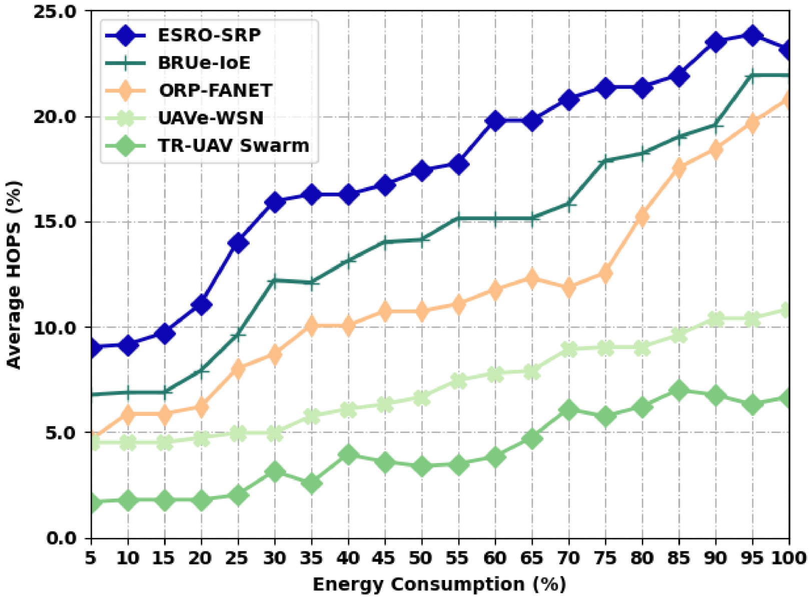

Figure 4. AHOPS analysis of ESRO-SRP technique under distinct levels of energy.

Table 4 and Figure 5 illustrate a comparative coverage inspection of the ESRO-SRP approach with recent models under distinct levels of energy. The outcomes represented that the ESRO-SRP model has accomplished improved values of coverage under all energy levels.

For instance, with an EC of 5%, the ESRO-SRP model has provided a maximal coverage of 97.69%, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm methods have accomplished a decreased coverage of 91.18%, 83.58%, 81.41%, and 73.26%, respectively. Finally, with an EC of 100%, the ESRO-SRP model has provided an enhanced coverage of 48.29%, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm models have accomplished minimal coverage of 33.63%, 16.26%, 15.18%, and 3.24%, respectively.

Table 4. Coverage analysis of ESRO-SRP technique with existing algorithms under distinct levels of energy.

Coverage (%)					
EC (%)	**ESRO-SRP**	**BRUe-IoE**	**ORP-FANET**	**UAVe-WSN**	**TR-UAV Swarm**
5	97.69	91.18	83.58	81.41	73.26
10	98.78	92.81	81.41	75.43	70.01
15	96.61	90.09	79.23	73.26	66.21
20	92.81	89.01	75.98	71.63	65.12
25	89.01	85.21	72.18	71.63	58.61
30	86.83	82.49	70.01	64.03	53.18
35	86.83	77.06	59.15	65.66	43.95
40	77.61	68.38	56.43	55.35	42.32
45	75.98	67.83	56.98	51.01	39.06
50	65.12	60.78	49.92	47.21	36.35
55	62.41	54.26	45.03	42.32	35.26
60	61.32	50.46	42.86	39.61	28.21
65	60.78	47.75	38.52	36.35	26.03
70	58.61	46.66	36.35	31.46	25.49
75	55.89	43.95	30.92	27.66	23.86
80	52.09	40.69	30.38	27.66	21.15
85	51.01	38.52	27.66	19.52	16.81
90	51.01	37.43	21.69	19.52	13.01
95	51.01	35.26	18.98	15.18	3.24
100	48.29	33.63	16.26	15.18	3.24

Table 5 and Figure 6 depict a comparative lifetime analysis of the ESRO-SRP algorithm with recent methodologies under distinct levels of energy. The results outperformed in that the ESRO-SRP model has accomplished maximum values of a lifetime under all energy levels. For instance, with an EC of 5, the ESRO-SRP system has provided a higher lifetime of 57 rounds, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm algorithms have accomplished a minimal lifetime of 41, 25, 10, and 1 round, respectively. Moreover, with an EC of 100, the ESRO-SRP model has an obtainable increased lifetime of 176 rounds, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm approaches have accomplished a decreased lifetime of 157, 144, 124, and 107 rounds, respectively.

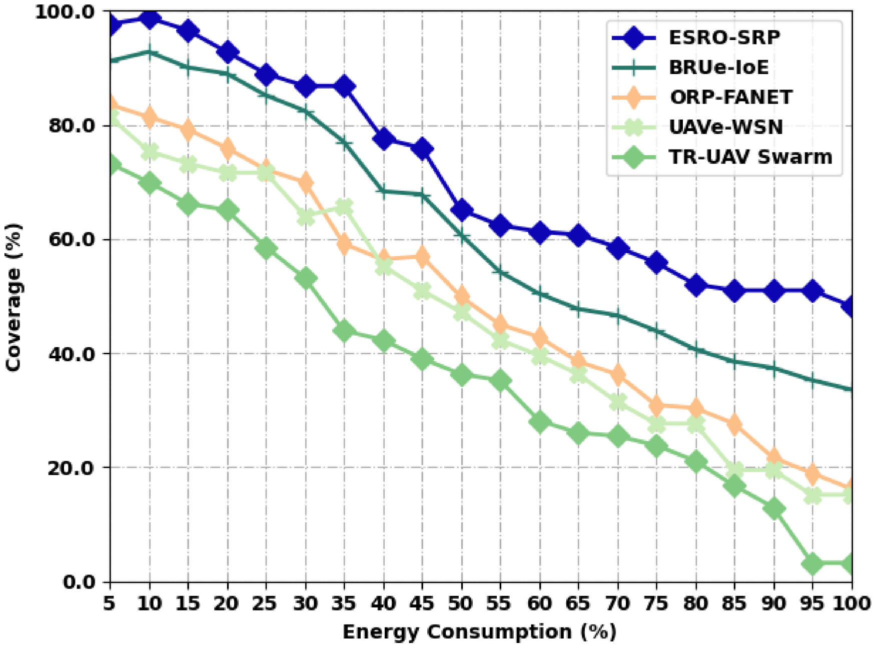

Figure 5. Coverage analysis of ESRO-SRP technique under distinct levels of energy.

Table 5. Lifetime analysis of ESRO-SRP technique with existing algorithms under distinct levels of energy.

Lifetime (No. of Rounds)					
EC (%)	**ESRO-SRP**	**BRUe-IoE**	**ORP-FANET**	**UAVe-WSN**	**TR-UAV Swarm**
5	57	41	25	10	1
10	65	48	38	15	6
15	65	53	40	35	14
20	75	56	48	41	15
25	75	62	52	43	19
30	88	65	58	43	22
35	94	72	66	52	30
40	113	96	73	51	32
45	124	110	80	58	37
50	130	108	93	60	40
55	142	121	96	66	39
60	148	124	105	72	44
65	149	130	107	75	44
70	157	139	120	78	58
75	163	147	119	95	78
80	167	147	117	94	86
85	170	151	124	102	90
90	174	154	135	104	94
95	175	157	136	119	100
100	176	157	144	124	107

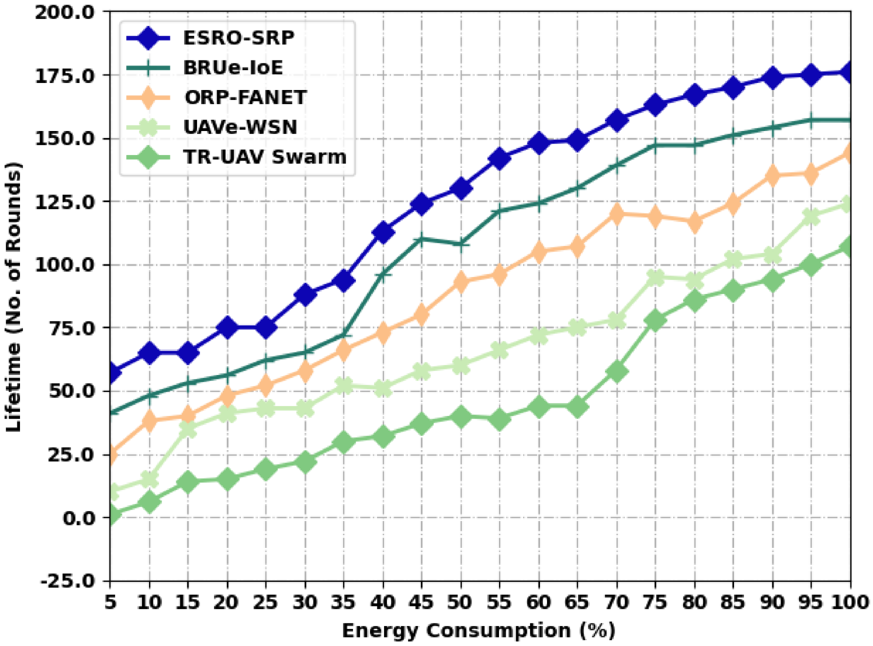

Figure 6. Lifetime analysis of ESRO-SRP technique under distinct levels of energy.

The experimental results ensured the superior outcomes of the proposed model over other models in the IoD environment.

4. Conclusions

In this study, a novel ESRO-SRP technique was established for secure communication among the drones in the IoD environment. The presented ESRO-SRP technique mainly aims to derive a set of optimal routes to the destination. In addition, the ESRO-SRP algorithm is derived by the integration of the QOBL concept with the conventional SRO algorithm. Moreover, the presented ESRO-SRP technique derived a fitness function encompassing different input parameters such as RE, distance, and trust degree. The experimental validation of the ESRO-SRP technique is carried out under several aspects, and the results demonstrated the enhancements of the ESRO-SRP model over recent approaches. The ESRO-SRP model has provided an increased PDR of 86%, whereas the BRUe-IoE, ORP-FANET, UAVe-WSN, and TR-UAV Swarm approaches have accomplished a minimal PDR of 79.60%, 73.60%, 67.60%, and 63.20%, respectively. Therefore, the ESRO-SRP technique can be exploited as an effective tool to improve security and network efficiency. In the future, the performance of the ESRO-SRP algorithm will be extended to the integration of lightweight cryptographic techniques.

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

Funding: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through the Large Groups Project under grant number (142/43). 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: (22UQU4340237DSR31).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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 that they have no conflict of interest. The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript.

References

1. Singh, M.; Aujla, G.S.; Bali, R.S. A Deep Learning-Based Blockchain Mechanism for Secure Internet of Drones Environment. *IEEE Trans. Intell. Transport. Syst.* **2021**, *22*, 4404–4413. [CrossRef]
2. Lin, C.; He, D.; Kumar, N.; Choo, K.-K.R.; Vinel, A.; Huang, X. Security and Privacy for the Internet of Drones: Challenges and Solutions. *IEEE Commun. Mag.* **2018**, *56*, 64–69. [CrossRef]
3. Alsamhi, S.H.; Ma, O.; Ansari, M.S.; Almalki, F.A. Survey on Collaborative Smart Drones and Internet of Things for Improving Smartness of Smart Cities. *IEEE Access* **2019**, *7*, 128125–128152. [CrossRef]
4. Chatterjee, S.; Perumalla, S.; Siva Kumar, A.P. Design and Implementation of Novel Secure User Authentication System over Internet of Drones. *Int. J. Syst. Syst. Eng.* **2021**, *11*, 105–120. [CrossRef]
5. Putranto, D.S.C.; Aji, A.K.; Wahyudono, B. Design and Implementation of Secure Transmission on Internet of Drones. In Proceedings of the 2019 IEEE 6th Asian Conference on Defence Technology (ACDT), Bali, Indonesia, 13–15 November 2019; pp. 128–135. [CrossRef]
6. Al-Wesabi, F.N.; Obayya, M.; Hamza, M.A.; Alzahrani, J.S.; Gupta, D.; Kumar, S. Energy Aware Resource Optimization using Unified Metaheuristic Optimization Algorithm Allocation for Cloud Computing Environment. *Sustain. Comput. Informatics Syst.* **2022**, *35*, 100686. [CrossRef]
7. Fitwi, H.; Nagothu, D.; Chen, Y.; Blasch, E. A Distributed Agent-Based Framework for a Constellation of Drones in a Military Operation. In Proceedings of the 2019 Winter Simulation Conference (WSC), National Harbor, MD, USA, 8–11 December 2019; pp. 2548–2559. [CrossRef]
8. Abunadi, I.; Althobaiti, M.M.; Al-Wesabi, F.N.; Hilal, A.M.; Medani, M.; Hamza, M.A.; Rizwanullah, M.; Zamani, A.S. Federated Learning with Blockchain Assisted Image Classification for Clustered UAV Networks. *Comput. Mater. Contin.* **2022**, *72*, 1195–1212. [CrossRef]
9. Sirohi, P.; Al-Wesabi, F.N.; Alshahrani, H.M.; Maheshwari, P.; Agarwal, A.; Dewangan, B.K.; Hilal, A.M.; Choudhury, T. Energy-Efficient Cloud Service Selection and Recommendation Based on QoS for Sustainable Smart Cities. *Appl. Sci.* **2021**, *11*, 9394. [CrossRef]
10. Alrowais, F.; Almasoud, A.S.; Marzouk, R.; Al-Wesabi, F.N.; Hilal, A.M.; Rizwanullah, M.; Motwakel, A.; Yaseen, I. Artificial Intelligence Based Data Offloading Technique for Secure MEC Systems. Comput. *Mater. Contin.* **2022**, *72*, 2783–2795. [CrossRef]
11. Singh, M.; Aujla, G.S.; Bali, R.S. ODOB: One Drone One Block-based Lightweight Blockchain Architecture for Internet of Drones. In Proceedings of the IEEE INFOCOM 2020—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, 6–9 July 2020; pp. 249–254. [CrossRef]
12. Guerber, C.; Royer, M.; Larrieu, N. Machine Learning and Software Defined Network to secure communications in a swarm of drones. *J. Inf. Secur. Appl.* **2021**, *61*, 102940. [CrossRef]
13. Kuzmin, A.; Znak, E. Blockchain-base structures for a secure and operate network of semi-autonomous Unmanned Aerial Vehicles. In Proceedings of the 2018 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), Singapore, 31 July–2 August 2018; pp. 32–37. [CrossRef]
14. Ravi, N.; Chitanvis, R.; El-Sharkawy, M. Applications of Drones using Wireless Sensor Networks. In Proceedings of the 2019 IEEE National Aerospace and Electronics Conference (NAECON), Dayton, OH, USA, 15–19 July 2019; pp. 513–518. [CrossRef]
15. Tian, Y.; Yuan, J.; Song, H. Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones. *J. Inf. Secur. Appl.* **2019**, *48*, 102354. [CrossRef]
16. Allouch, A.; Cheikhrouhou, O.; Koubâa, A.; Toumi, K.; Khalgui, M.; Gia, T.N. UTM-Chain: Blockchain-Based Secure Unmanned Traffic Management for Internet of Drones. *Sensors* **2021**, *21*, 3049. [CrossRef] [PubMed]
17. Wazid, M.; Das, A.K.; Kumar, N.; Vasilakos, A.V.; Rodrigues, J.J.P.C. Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment. *IEEE Internet Things J.* **2018**, *6*, 3572–3584. [CrossRef]
18. Gorrepati, R.R.; Guntur, S.R. DroneMap: An IoT Network Security in Internet of Drones. In *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*; Springer: Cham, Switzerland, 2021; pp. 251–268. [CrossRef]
19. Jain, D.K.; Tyagi, S.K.S.; Neelakandan, S.; Prakash, M.; Natrayan, L. Metaheuristic Optimization-Based Resource Allocation Technique for Cybertwin-Driven 6G on IoE Environment. *IEEE Trans. Ind. Inform.* **2021**, *18*, 4884–4892. [CrossRef]
20. Goswami, P.; Mukherjee, A.; Maiti, M.; Tyagi, S.K.S.; Yang, L. A Neural-Network-Based Optimal Resource Allocation Method for Secure IIoT Network. *IEEE Internet Things J.* **2021**, *9*, 2538–2544. [CrossRef]
21. Padmaa, M.; Jayasankar, T.; Venkatraman, S.; Dutta, A.K.; Gupta, D.; Shamshirband, S.; Rodrigues, J.J. Oppositional chaos game optimization based clustering with trust based data transmission protocol for intelligent IoT edge systems. *J. Parallel Distrib. Comput.* **2022**, *164*, 142–151. [CrossRef]

22. Ahmad, M.; Ullah, F.; Wahid, I.; Khan, A.; Uddin, M.I.; Alharbi, A.; Alosaimi, W. A Bio-inspired Routing Optimization in UAV-enabled Internet of Everything. *Comput. Mater. Contin.* **2021**, *67*, 321–336. [CrossRef]
23. Liu, B.; Zhang, W.; Chen, W.; Huang, H.; Guo, S. Online computation ofoading and trafc routing for UAV swarms in edge-cloud computing. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8777–8791. [CrossRef]
24. Baek, J.; Han, S.I.; Han, Y. Energy-efficient UAV routing for wireless sensor networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 1741–1750. [CrossRef]
25. Yang, H.; Liu, Z. An optimization routing Protocol for FANETs. *EURASIP J. Wirel. Commun. Netw.* **2019**, *2019*, 2–8. [CrossRef]