applied sciences

MDPI

Article

An Enhanced and Secure Trust-Aware Improved GSO for Encrypted Data Sharing in the Internet of Things

Prabha Selvaraj [1,†], Vijay Kumar Burugari [2,†], S. Gopikrishnan [1,†], Abdullah Alourani [3,*,†], Gautam Srivastava [4,5,6,†] and Mohamed Baza [7,†]

1 School of Computer Science and Engineering, VIT-AP University, Amaravati-522237, Andhra Pradesh, India
2 Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram 522302, Andhra Pradesh, India
3 Department of Computer Science and Information, College of Science in Zulfi, Majmaah University, Al-Majmaah 11952, Saudi Arabia
4 Department of Math and Computer Science, Brandon University, Brandon, MB R7A 6A9, Canada
5 Research Centre for Interneural Computing, China Medical University, Taichung 40402, Taiwan
6 Department of Computer Science and Math, Lebanese American University, Beirut 1102, Lebanon
7 Department of Computer Science, College of Charleston, Charleston, SC 29424, USA
* Correspondence: a.alourani@mu.edu.sa
† These authors contributed equally to this work.

Abstract: Wireless sensors and actuator networks (WSNs) are the physical layer implementation used for many smart applications in this decade in the form of the Internet of Things (IoT) and cyber-physical systems (CPS). Even though many research concerns in WSNs have been answered, the evolution of the WSN into an IoT network has exposed it to many new technical issues, including data security, multi-sensory multi-communication capabilities, energy utilization, and the age of information. Cluster-based data collecting in the Internet of Things has the potential to address concerns with data freshness and energy efficiency. However, it may not offer reliable network data security. This research presents an improved method for data sharing and cluster head (CH) selection using the hybrid Vlsekriterijumska Optimizacija I Kompromisno Resenje (VIKOR) method in conjunction with glowworm swarm optimization (GSO) strategies based on the energy, trust value, bandwidth, and memory to address this security-enabled, cluster-based data aggregation in the IoT. Next, we aggregate the data after the cluster has been built using a genetic algorithm (GA). After aggregation, the data are encrypted and delivered securely using the TIGSO-EDS architecture. Cuckoo search is used to analyze the data and choose the best route for sending them. The proposed model's analysis of the results is analyzed, and its uniqueness has been demonstrated via comparison with existing models. TIGSO-EDS reduces energy consumption each round by 12.71–19.96% and increases the percentage of successfully delivered data packets from 2.50% to 5.66%.

Keywords: security; encryption; cyber-physical systems; GSO; Internet of Things

check for updates

Citation: Selvaraj, P.; Burugari, V.K.; Gopikrishnan, S.; Baza, M.; Srivastava, G. An Enhanced and Secure Trust-Aware Improved GSO for Encrypted Data Sharing in the Internet of Things. *Appl. Sci.* **2022**, *13*, 831. https://doi.org/10.3390/app13020831

Academic Editor: Wenfeng Zheng

Received: 27 October 2022
Revised: 23 December 2022
Accepted: 26 December 2022
Published: 7 January 2023

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

1. Introduction

Wireless sensor networks (WSNs) contain two types of nodes, which are the sensor nodes and the base station. Sensor nodes (SNs) are deployed very close to each other in a specific environment(s). A typical representation of WSN network architecture is depicted in Figure 1. An SN is capable of transferring and receiving collected data and then forwarding them to the gateway for further processing. Each sensor contains a transceiver, microcontroller, memory, sensor units, and power.

WSNs have a base station (BS) with no energy constraint which is far off from the region of the sensor nodes. To communicate with the BS, the sensor nodes either employ direct transmission or multi-hop transmission since they are fixed. In a WSN, clustering is introduced to overcome the aforementioned issues due to the scalability of networks, considering attributes related to energy-saving and the stability of the network topology. The

sensor nodes are combined into the clusters, and this has been followed by the community of research to reach the network scalability objective [1]. The entire cluster has a head. Even though there are more clustering algorithms proposed for ad hoc networks in the literature, the main aim is to form stable clusters of mobile nodes [2]. Different methodologies are applied for the stability of a node and its reachability without considering issues such as network longevity and coverage in the design goals of WSNs. Now, different techniques for clustering have been particularly modeled for WSNs, as discussed in [3].

Based on the node deployment and bootstrapping methodology, the proposed clustering methodology varies, and it is used in the network's structural and operational design and its features [4]. In a cluster, the sensor can select the cluster head (CH) or be pre-assigned by the network designer. The CH is the one with higher resources. The membership of a cluster may change or be fixed. The cluster head can act as a next tier, or it may transfer the data to the base station or command center [5].

Furthermore, clustering has an advantage in terms of network scalability. It can restrict the route set up inside the cluster, which is noted for each node to reduce the routing table size [6]. The bandwidth used for communication can be preserved by clustering through restricting the inter-cluster communication and communicating redundant messages between sensor nodes. Clustering applied at the sensor level stabilizes the network topology and also reduces the maintenance overhead. Even though the cluster head and sensors nodes are linked, when there is a change in the inter-cluster tier level, it does not cause any effect on the cluster construction, as explained in [7]. The optimal cluster head can improve and optimize the network operation as well as the sensor's battery lifetime, which in turn improves the lifetime of the network, as stated by Rodríguez et al. [8] and Zhao et al. [9].

The Internet of Things (IoT), which is built on a layered architecture, permits Internet communication between physical items that are connected to different types of networks [10]. The layers in this design accommodate each other's requirements, and the way in which they communicate with one another influences not just their own performance but also that of the entire network [11]. To a considerable extent, the actualization of the Internet of Things will be determined by a variety of factors, including system design, networks and communications, data processing and ubiquitous computing technologies, dependability, and both physical and cyber linkages [12]. Networking, and more specifically network routing, is the primary power behind the Internet of Things and is what makes it possible for devices to connect with one another [10]. This comprises the creation of traffic routes as well as the movement of packets across the network from their point of origin to their eventual destination.

In the Internet of Things, the physical layer is responsible for providing support to the sensor networks. Because of this, the need for communication between the many IoT devices and the wireless sensor network is one of the challenges of the IoT. Self-organizing wireless sensor networks are networks that have a high number of nodes which are dispersed throughout a single place. These nodes are accountable for obtaining the required data and sending them to a node in the network, which is known as a base station.

Sensor networks, the most important subset of the Internet of Things sets, are unique from other distributed systems because of the limits and problems involved in routing. In the Internet of Things ecosystem, one of the issues is minimizing the amount of power that is consumed across the network while simultaneously routing data between devices. Therefore, in most Internet of Things networks, various protocols such as hierarchical protocols can be employed to limit the amount of energy that is consumed. Clustering techniques have also been utilized in these networks.

In this study, an attempt is made to treat the challenge of energy-conscious routing among WSN-based Internet of Things devices as an optimization problem, and an effective optimization method is employed to provide a solution to the problem. The algorithm that was ultimately chosen was a tweaked version of the GSO optimization algorithm. In this particular approach, an effort has been made to reduce the likelihood of the algorithm becoming stuck in a cycle of local optimizations.

The current article is divided into five sections, the first of which introduces the IoT and its architecture before looking at IoT routing. After analyzing the prior studies, the following will provide a presentation of the proposed strategy, as well as an analysis of how effective it is. The conclusions drawn from this article are presented and discussed at the end.

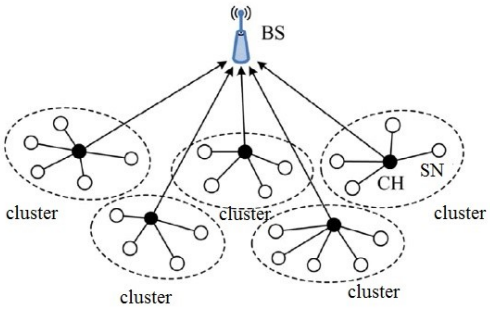


Figure 1. Wireless sensor network architecture.

2. Literature Survey

The term GSO refers to two variants of swarm-based optimizations, namely genetic swarm optimization and glowworm swarm optimization. The combination of the famous particle swarm optimization (PSO) and a genetic algorithm (GA) is treated as a hybrid evolutionary algorithm, and it is named genetic swarm optimization. Sampathkumar et al. [13] proposed glowworm swarm optimization. This behavior is replicated in such a way that the glowworm holds a luminescence quantity, called luciferin, to swap the information that has been carried along with it to other companions. The work suggested by the author uses glowworm swarm optimization. Factors such as the optimum decision radius variations will improve GSO, resulting in the optimal solution and also providing a global optimum objective function in the finite-dimensional vector space. The authors presented the algorithm by modifying GSO in such a way that the defects were conquered, and the modified MGSO was thus applied to blind signal separation with this algorithm, proving its effectiveness.

The main idea behind the constrained optimization problem is to discover the optimal solution in the possible region. Most of the conventional optimization design algorithms that were identified earlier worked on the concept of gradients, and this was made clear to show the distinction between the objective function and constraint conditions. It has been identified that the solution obtained through this procedure is the most local optimal solution. The methods that deal with the penalty function are found to be easy and suitable, but the major drawback is in locating the appropriate penalty factors. Aside from this, considering the low accuracy and poor stability while determining the solutions for constrained optimization problems, Yadav et al. [14] proposed a hybrid glowworm optimization (HGSO) algorithm. The proposed algorithm combines the artificial fish swarm algorithm (AFSA) with glowworm swarm optimization (GSO) algorithm to form an improved GSO and also uses differential evolution (DE). During the evolution phase, based on the feasibility rule, constraint-based technology is applied in HGSO to identify the optimal location of the population. Thus, this in turn builds the population in a rapid manner which is convergent to feasible regions so that the most feasible solution can be found. The proposed method uses the local search strategy based on simulated annealing (SA) to find the optimum local optimal value. This technique helps in avoiding premature convergence.

In WSNs, it is necessary to gather information from different sensor nodes for further processing. Removing the duplicate data and minimizing the redundant data transmission is achieved by data aggregation, as stated by Idrees et al. [15]. To increase the efficiency, the cluster head collects the data from all nodes and performs data aggregation as described in [16]. Rawat et al. [17] discussed lifetime approximation and improving the efficiency of data aggregation. The tree and star structures were used for secure data

aggregation by Maryam et al. [18]. Multi-criteria decision making (MCDM) is widely used in different areas of research for decision making. It can be categorized into two types based on objective, as explained in [19], and attributes, as explained in [20]. The difference between multi-objective decision making (MODM) and multi-attribute decision making (MADM) involves considering all the criteria for selecting one alternative which is not dominating, while MADM ranks all the alternatives based on their attributes and then selects one. VIKOR is a multi-criteria decision-making method for optimizing the process of cluster head selection. It gives the ideal solution by considering the closeness measure. The method ranks the alternative solutions and selects the ideal one from it by analyzing the criteria which conflict and are incommensurable, as discussed by Ghadikolaei et al. [21] and Guiwu Wei et al. [22], so that it can implement decision making.

There are many challenges in framing the AES algorithm, which is quick and inexpensive according to [23]. It prevents key exchange through unsecured communication channels, which puts symmetric algorithms at risk. Security and confidentiality for data transmission in WSNs are provided by the Advanced Encryption Standard (AES) algorithm. It is based on a scheme called Kerberos server authentication proposed by Oasim (2010) for validating WSNs. The existing clustering methods in WSNs were analyzed in [24]. Improving the energy efficiency in WSNs using a genetic algorithm was described by Ajmi et al. [25]. The fuzzy grasshopper optimization algorithm is used for energy efficiency [26].

2.1. Problem Formation

In remote IoT devices, a key problem is energy constraints. In this section, the different issues associated with energy management and the preceding energy-efficient clustering protocols are explained, along with their advantages and disadvantages. Some optimization algorithms have been implemented to overcome combinatorial and arithmetic optimization issues. These algorithms are categorized into various groups by considering whether they are stochastic, deterministic, iterative, based on population, and so on. This algorithm employs a probabilistic rule for enhancing the solution. After that, it is known as probabilistic or stochastic. It describes the meta-heuristic-based optimization algorithm methodology, and it can be used in WSNs for identifying the optimal cluster heads which effectively enhance a WSN's lifetime. As discussed in the literature survey, it is not a new research problem to resolve the network lifetime issue in WSNs, but when considering the security aspect, very few methods were proposed. Liu et al. [27] discussed data aggregation with a WSN-based IoT model for secure and effective network transmission. Aljumaie et al. [28] explained a low-cost and secure SLEACH-PRO protocol. A multi-hop system neural network-based enhanced backpropagation method for improving node energy and transmission was discussed in [29]. Another LEACH-based routing protocol proposed for secured node communication was also presented in [30]. Additionally, the extended DE-LEACH protocol was proposed for improving consumption of energy in [31]. In summary, all these specific models consider the WSN nodes to be homogeneous sensor nodes.

In the Internet of Things, many modes of communication can be joined to form complex heterogeneous systems, which can then be used to implement storage operations that offer data gathering, continuous monitoring, transmission, processing, and saving. Edge nodes, also known as RFID tags or sensor nodes, are responsible for data collection in the Internet of Things. These data are then transmitted to service providers or consumers via the network layer. In order to accomplish this, resources are put into an active mode and reserved for future use. The overall cost of the service can be reduced to its absolute minimum by improving both the quality of the service provided by network layer services and the performance of the end nodes. In the Internet of Things, it is still challenging to precisely define the quality of service and the network lifetime. Because the service in this context encompasses other features, such as information accuracy and service availability, conventional approaches to service quality are manifestly ineffective when applied to the Internet of Things (IoT).

By considering all these issues, Rawat et al. [17] proposed a new methodology for heterogeneous WSNs to be energy-efficient and heterogeneously clustered for network lifetime enhancement. Additional research by Li et al. [32] proposed a new energy-efficient clustering technique (EECT) was applied to gathered data periodically in WSNs. These problems were also addressed through the single-hop energy-efficient clustering protocol for heterogeneous WSNs to improve network lifetimes, as discussed in [33]. All these models discussed the static nodes, and the authors did not consider the node mobility.

Nodes in the network typically have a low-capacity power supply in IoT implementations. As a result, there is a pressing requirement for the development of novel approaches to decrease energy loss, which reduces the lifespan of networks. The increased density of network nodes, in combination with these limits, has led to a number of challenges in wireless network design and administration, as well as the need for energy optimization at every level of the protocol stack. For instance, at the network layer, we have an extreme requirement to locate data transmission and path discovery methods that minimize their impact on the environment while simultaneously maximizing their efficiency. IoT routing has become a significant obstacle for researchers to overcome because of how important it is and how much of an influence it has on lowering the amount of energy that is consumed. Hence, an integrated combination of information accuracy, coverage, power consumption, network implementation cost, and traditional service quality is required to provide quality of service in the Internet of Things.

2.2. Contributions Made in This Article

Energy-efficient routing is one of the approaches for optimizing energy usage in the Internet of Things. This methodology recognizes that the needed amount of energy can be decreased by selecting a more advantageous path. This approach sends data to their destination by routing it through nodes that have adequate energy resources. Additionally, it excludes the participation of any nodes that have energy resources which are lower than a predetermined threshold value. Additionally, removing redundancy lowers the amount of energy required to transmit data, which in turn enhances the lifespan of the network.

An energy-efficient approach to Internet of Things (IoT) routing is proposed in this paper. In order to achieve energy efficiency through efficient routing and communication, this research has been proposed to provide an effective method for selecting CHs. To accomplish this goal, numerous QoS parameters, such as energy and mobility, are taken into consideration. In order to provide the most accurate assessment of fitness that is feasible, the GSO method is combined with the most optimal CH. The technique for clustering is carried out on the cluster head that has been selected. The data aggregation of individual sensor nodes and the aggregation of data from their cluster nodes through this model results in a reduction in the bandwidth that is used. Following the completion of the aggregation phase, the data are transmitted to the sink or base station. To determine the effectiveness of the suggested technique, the remaining energy, network life, and coverage rate are evaluated. The proposed approach can be utilized as a dependable method for data routing and transfer in the Internet of Things, since it consistently outperforms the basic designs in all scenarios and assessment criteria, according to an analysis of the results in two distinct case study simulations.

3. Proposed TIGSO-EDS System Architecture

A WSN is a cluster of sensors that engage in monitoring and sharing information with the central server. Transmitting the information over a wireless medium (sensor) needs to be performed with a minimized packet loss rate. Clustering models are used to overcome the overhead of energy, which is a challenging issue in these networks.

In the proposed method, a hybrid VIKOR GSO model is used for selecting the CH. The overview of the proposed model which used VIKOR GSO is presented in Figure 2.

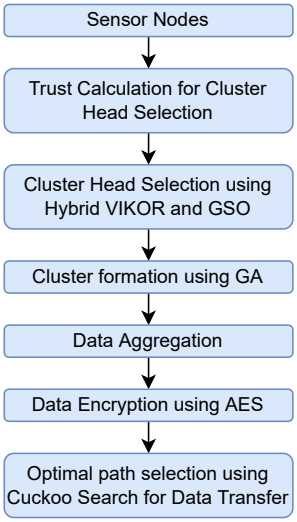


Figure 2. System architecture of TIGSO-EDS.

Step 1: The best and worst values, f_i^* and $f_i^\sim$, respectively, for all the criterion functions are determined, where i ranges from 1 to n. Equations (1) and (2) represent the best and worst values, respectively:

$$f_i^\sim = \min_j f_{ij} \text{ if i}^{\text{th}} \text{ function symbolizes a benefit} \tag{1}$$

$$f_i^* = \min_j f_{ij}, f_i^\sim = \min_j f_{ij} \text{ if i}^{\text{th}} \text{ function symbolizes a cost} \tag{2}$$

Step 2: The values of S_j and R_j are given by Equations (3) and (4), respectively, where $j = 1, 2, 3, \ldots J$:

$$S_j = W_i(f_i^* - f_{ij})/(f_i^* - f_i^\sim) \tag{3}$$

$$R_j = W_i(f_i^* - f_{ij})/(f_i^* - f_{ij}^\sim) \tag{4}$$

Step 3: Determine the values of Q_j using the relation represented in Equation (5):

$$Q_j = v(S_i - S^*)/(S^\sim - S^*) + (1 - v)(R_j - R^*)/R^\sim - R^* \tag{5}$$

where the following definitions apply:

- $S^* = \min_j S_J$;
- $S^\sim = \max_j S_J$;
- $R^* = \min_j R_J$;
- $R^\sim = \max_j R_J$;
- v represents the weight strategy for the majority criteria;
- $(1 - V)$ represents the weight of individual regrets.

Step 4: After ranking the alternatives, the values of S, R, and Q are sorted in decreasing order for three ranking lists.

Step 5: A compromised solution is proposed with the attentive ($F^{(1)}$), which is considered the best-ranked value with the (minimum) measure Q if the subsequent conditions are satisfied.

Condition 1 depicts the "acceptable advantage" and is represented as $Q(F(2) - F(1)) \geq DQ$, where F(n) represents an alternative solution in the rank list with the help of Q (in the n^{th} position) and $DQ = 1/(M - 1)$.

Condition 2 represents the "acceptable stability" ($F(1)$), which must be ranked as the best by either the S and R or S or R values. Within this decision-making process, the

compromised solution is stable, and it is the scenario of the maximal group utility. Here, the values of V vary based on the requirements, which are $v \geq 0.5$ when needed, $v = 0.5$ by concurrence, or $v \leq 0.5$, where the "v" signifies the weight of the decision-making strategy.

The set of compromised solutions is proposed if any one of the conditions is not satisfied. The compromised solutions are the following:

- If condition 2 is not satisfied, then the alternatives are $F(1)$ and $F(2)$;
- If condition 1 is not satisfied, then the alternatives are $F(1), F(2), F(3), \ldots F(M)$, where $F(M)$ is determined using the relation represented in Equation (6) with the maximum M:

$$Q(F^{(M)}) - Q(F^{(1)}) < DQ \tag{6}$$

During this method, it is guaranteed that these alternatives satisfy the closeness property. GSO has glowworms, which carry a luminescence quantity along with the agents, which are called luciferin. Based on the objective function of the value of luciferin broadcasted by the glowworms to their neighbors, the fitness of their current locations is evaluated. The best possible CH selection is ensured by combining the VIKOR technique with GSO for selecting the node to be the CH.

Condition 1 depicts the "acceptable advantage" and is represented by $Q(F(2)\check{}F(1)) \geq DQ$, where $F(n)$ represents an alternative solution in the rank list with the help of Q (in the n^{th} position) and $DQ = \frac{1}{M-1}$. During this method, it is guaranteed that these alternatives satisfy the closeness property.

The GSO objective function is based on energy and mobility. Let N, the number of nodes, stand for the position vector of a node i and time t where $d_{ij}(t) = |n_j(t) - n_i(t)|$, which is the distance from node i to j at time t.

The communication range is computed using Equation (7):

$$T_r = \sqrt{\left(\frac{(dn_d/dn_c)}{coveragearea}\right)} \tag{7}$$

where the following definitions apply:

- $dn_d = S + 1$ is the degree of the desired node;
- $S = nodedensity * d(C, N)$;
- $d(C, N) = \sqrt{\sum_{i=1}^{n}(N_i - C_i)^2}$;
- C and N represent the cluster head and node, respectively;
- dn_c is the degree of the current node;
- The coverage area represents the region covered by the cluster.

The consumption of total energy E_t is determined using Equation (8):

$$E_t S_i, d = \begin{cases} S_i E + S_i \varepsilon_{fs} d^2, d \leq d_0 \\ S_i E + S_i \varepsilon_{mp} d^2, d > d_0 \end{cases} \tag{8}$$

where the following definitions apply:

- $d_0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}$;
- E represents the energy consumed to transmit or receive 1-bit messages;
- ε_{fs} stands for the free space signal's augmentation coefficient;
- ε_{mp} stands for the fading signal amplification coefficient of multiple paths, which rely on the amplifier model's circuit;
- d shows the distance between the receiver and transmitter;
- s_i represents the fragment of sent information.

The transmission range of the neighborhood nodes is initially checked by the node, and the ID is transmitted with the required information to its neighborhood nodes. In GSO,

the physical entities are known as a glowworms. At time t, the condition of the glowworm n has three limitations:

- The search space position ($x_i(t)$);
- The level of luciferin ($l_i(t)$);
- The neighborhood range ($r_i(t)$).

The level of luciferin is measured by the node's weight. The level of luciferin selects the CH. GSO has three phases: (1) updating the luciferin level (Equation (9)), (2) glowworm (nodes) movement (Equation (10)), and (3) updating the neighborhood range. The current position of a glowworm i is used for finding the fitness value:

$$l_i t = (1-\rho) l_i(t-1) \gamma J(X_i(t)) \tag{9}$$

where the following definitions apply:

- ρ represents the luciferin evaporation factor;
- γ represents the luciferin constant;
- J represents the objective function.

$$X_i(t+1) = X_i(t) + S * \left(\frac{X_j(t) - X_i(t)}{\|X_j(t) - X_i(t)\|} \right) \tag{10}$$

Here, the following definitions apply:

- s denotes the step size;
- $\|X_j(t) - X_i(t)\|$ represents the Euclidean norm operator.

Each node (glowworm) conducts a trace to find its neighbors based on the x_j and x_i difference values, which determine whether there will be a higher value or a smaller value, respectively. The neighbor is determined by calculating the distance between the glowworm and neighbor (i.e., i and j, respectively). This is analyzed by two parameters. First, if the glowworm value is brighter and the neighbor value is shorter in GSO, then the neighbor value is considered. The luciferin level and search space position are updated using the aforementioned formulae accordingly. The probability in Equation (11) is used by the glowworm to choose one neighbor when it has several options:

$$p_{ij}(t) = \frac{l_j(t) - l_i(t)}{\sum_{k=N_i(t)} l_k(t) - l_i(t)} \tag{11}$$

The neighborhood range $(r_i(t))$ is updated to limit the range of communication in a group of nodes. The neighborhood range is calculated using Equation (12):

$$r_d^l(t+1) = \min\{r_s, \max\{0, r_d^l(t) + \beta(n_t - \mid N_i(t) \mid)\}\} \tag{12}$$

where the following definitions apply:

- r_s is a sensor range which is a constant that limits the size of the neighborhood range;
- $n + t$ the number of desired neighbors;
- $\mid N_i(t) \mid$ is several neighbors of the node n at t time, and β is a model constant.

In GSO, the specifications used are $\gamma = 0.6, \rho = 0.4, \beta = 0.08, n_t = 5, s = 0.03$, and $l_k = 5$.

The glowworm identifies its neighbor's movement and computes it by exploiting an adaptive neighborhood, which is bounded above by its sensor range. Each glowworm selects a neighbor using a probabilistic method, and it has a luciferin value superior to its other value, which moves toward it. The movements are based on the local information, and the selected neighbor interactions enable the glowworm swarms to divide into separate subgroups which converge on the several optima for a multi-modal function. Here, VIKOR is used to determine the fitness evaluation. The overview of the hybrid integration of the VIKOR GSO model for clustering in the proposed work is depicted in Figure 3.

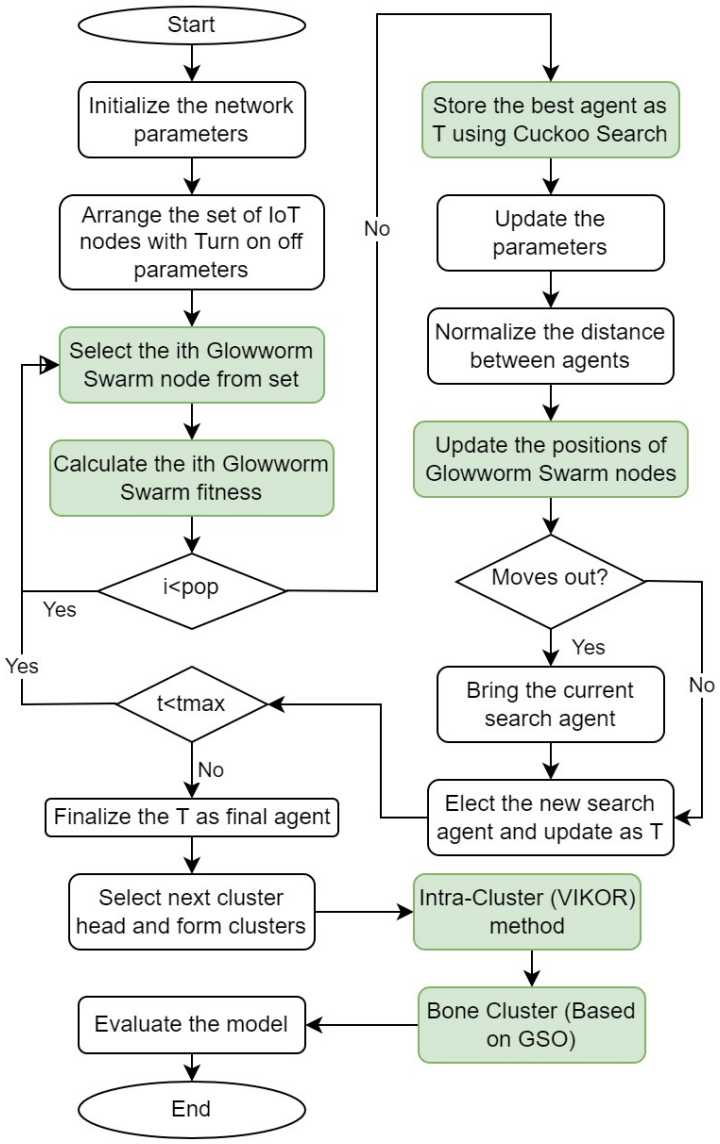


Figure 3. Hybrid integration of VIKOR GSO model for clustering in TIGSO-EDS.

After clustering, information is gathered by the CH and later aggregated and encrypted before being forwarded to the BS. At this point, a new hybrid encryption algorithm [34] is used to ensure security and develop useful security mechanisms. In the authenticating protocols, the sensor nodes initiate the key establishment process to communicate with a trusted third party, which is typically the base station, and obtain a session key. Usually, this communication is multi-hop with other nodes working as routers, particularly when large sensor networks are considered.

3.1. Security Enhancements

The proposed model uses a hybrid encryption approach which combines symmetric and asymmetric encryption techniques. The homomorphism encryption method will be utilized to encrypt the raw data with the public key. Through the implementation of a hybrid cryptographic method, the proposed model will enable both public and private key encryption. The suggested approach is meant to accommodate event-driven applications as well as continuous monitoring applications. In an event-driven application, the intermediary nodes verify the availability of the nodes when a sensor node identifies an event. In a system of continuous monitoring, the node's accessibility is validated via public key exchange. The sink node verifies the data's authenticity by decrypting the cypher data

using both the public and private keys. When a sink node is unable to decrypt data using the public key, the data are deleted, as they are unauthorized. By employing a hybrid encryption technique, data secrecy is assured in the suggested architecture. The integrity of the data gathered by the intermediate nodes and sink node may be ensured by the homomorphism nature of the proposed encryption algorithm. Lastly, the authorization of the node may be confirmed by the routing algorithm, which is proposed as TIGSO-EDS.

3.2. Summary and Discussion

Compared with a traditional network, a wireless sensor network has many constraints. Thus, there is difficulty in applying security methods directly in WSNs. In this work, secured data transmission is ensured by taking into account the trust parameter while choosing the CH. The optimization intends to determine the objective function, whose value may be either the maximum or minimum based on the problem being solved. However, assessment of the convergence rate and computational time is carried out to validate the optimization algorithms.

Cuckoo search is a general and resilient optimization technique that may be used in a wide variety of optimization problems. Additionally, it possesses desirable characteristics, such as simple implementation, a steady convergence characteristic, and reasonable computing efficiency. This optimization algorithm was inspired and proposed based on the egg laying and hatching life cycle of the cuckoo bird. A few birds such as Guria pigeons and anis (black birds), which belong to the cuckoo species, lay eggs in common nests [35]. However, to improve the probability of hatching their eggs, the process of laying eggs in another bird's nest is termed the parasitic brood method. During the laying period, one egg is laid in the host nest, and the remain ones are in other nests. The egg laid in the host nest will hatch more quickly than the eggs in the other nests. When this happens, the non-hatched eggs are evicted by the foreign cuckoo. This etiquette reduces the hatching probability of legitimate eggs. In addition to this, the chick of the foreign cuckoo tries to get more food by just mimicking the host's chicks. This nature of the cuckoo has been implemented as cluster construction process, as represented in Algorithm 1. Here, nests are considered as clusters, and eggs are considered as IoT devices in the network.

Algorithm 1 Cuckoo Search pseudo-algorithm.

Require: Initial population of N set of nodes.
Ensure: $N - x$ hosts are identified by an objective function
Start
Objective function(x)
Initiate host nests
while (**do**$s < MaxGen$)
    obtains a random cuckoo using levy fights
    Calculate its quality/fitness ff_i
    Choose a nest among the n randomly and consider it as j
    if $ff_i > ff_j$ **then**
        Replace j with a new value
    end if
    Fractions of worse nests are unrestricted and so built new one
    Save the best solution
end while

Various experimental studies concluded that the different insects and animals' flight behaviors exhibit the classic characteristics of Levy flights. The characteristics of Levy flights include a series of straightforward flight paths, which are efficient in examining the large search areas when compared with the traditional random walks due to a faster increase in variances. A Levy flight reduces the iteration of optimization algorithms by four times more than the normal random walk method [36]. The hybridized VIKOR-GSO approach was adopted to choose the optimal CH, and the aggregation of data was carried

out on the elected CH. The optimal clusters were searched with the help of a GA. Then, the cumulative data were communicated to BS through the best possible path, selected using the Cuckoo Search algorithm given in Algorithm 1.

4. Results and Performance Evaluation

The simulation was performed by considering 100 nodes in the network with the given simulation parameters shown in Table 1. There were numerous energy-efficient clustering techniques using a GA developed in the early stages. The election of the CH plays a vital role in minimizing the maximum intra-cluster distance between itself and its cluster member's energy consumption in the optimization of a network.

Table 1. Simulation parameters used for TIGSO-EDS.

Description	Symbol	Value
The proportion of normal nodes and advanced nodes	M	0.3
The proportion of advanced nodes and super nodes	m_0	0.5
Advanced nodes energy factor	β	2
Supernodes energy factor	α	3
Primary energy level	E_o	0.5 J
Size of the data packet	L	4000 bytes
The constraint of transmit amplifier	ε_{fs}	10 pJ/bit/m^2
Constraint transmit amplifier if $d_{BS} \leq d_0$	ε_{mp}	0.0013 pJ/bit/m^4
Dissipated energy per bit $d_{BS} \geq d_0$	E_{elec}	50/bit

4.1. Performance Metrics

The performance metrics used are summarized as follows:

- The number of alive nodes per cluster round.
- Network Lifetime Rate: This gives the alive node rate of the nodes present over the cluster round indirectly. It can also be called the possible remaining lifetime in the form of cluster rounds with changing levels of energy.
- Data Packet Received: This is the network throughput, which refers to the data packets or messages delivered successfully.
- Energy Consumption: The energy consumption in the network for cluster rounds is calculated by the difference between the initial energy and the residual energy.
- Fairness and Effectiveness: The fairness and effectiveness of the experiment can be ensured by analyzing the network lifetime, data packet received, and energy consumption.

The performance analysis of the different parameters was calculated, and we compared EEHC [17], EECT [32], and S-EECP [33] with the TIGSO-EDS method. The comparison of the alive nodes of the TIGSO-EDS method with EEHC, EECT, and S-EECP was performed, and the analysis shows that the proposed TIGSO-EDS method improved the alive node rate by 10.12%, 6.79%, and 4.53% when compared with EEHC, EECT, and S-EECP, respectively.

A comparison of the alive nodes of TIGSO-EDS is shown in Figure 4. A method with EEHC, EECT, and S-EECP was implemented, and the analysis shows that the proposed TIGSO-EDS method improved the alive node rate by 10.12%, 6.79%, and 4.53% when compared with EEHC, EECT, and S-EECP, respectively. There were three methods, namely energy-efficient heterogeneous clustered, energy-efficient clustering technique, and single-hop energy-efficient clustering protocol, for calculating the network lifetime, which were proposed by TIGSO-EDS. Figure 5 shows that TIGSO-EDS improved the network lifetime rate by 19.77%, 9.25%, and 6.37% when compared with EEHC, EECT, and S-EECP, respectively.

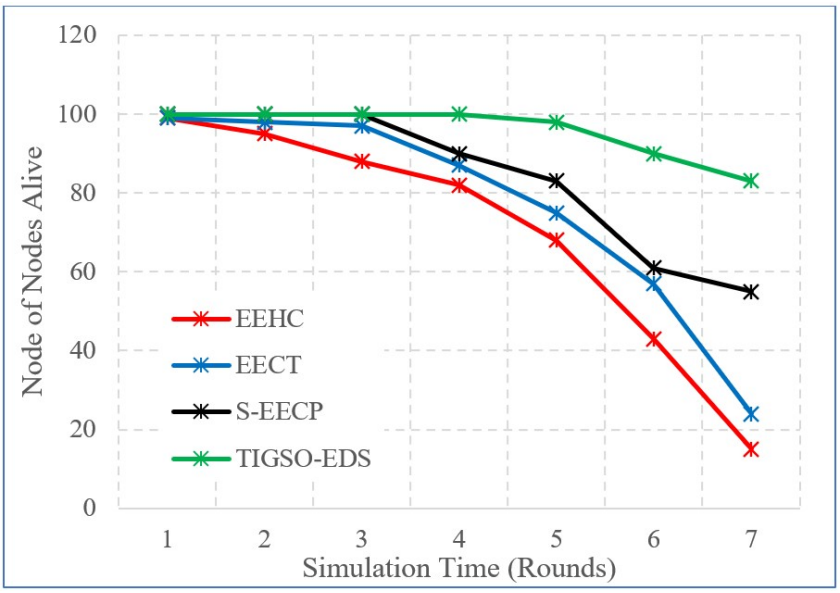


Figure 4. Comparison of alive nodes (base station located at 50 × 50).

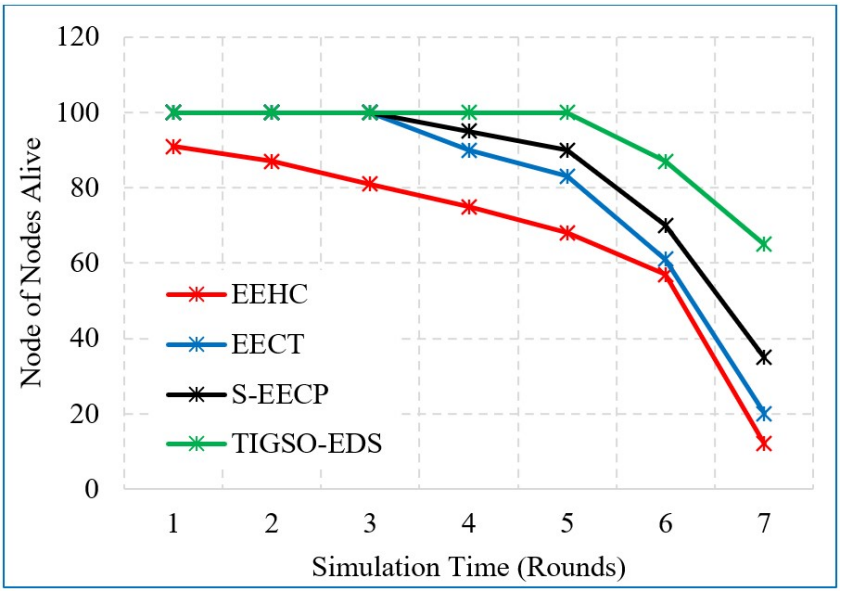


Figure 5. Comparison of alive nodes (base station located at 100 × 250).

4.2. Simulation Results

The simulation was performed with a maximum of 20,000 data packets that could be exchanged during the experiment, and the quantity of the data packets received during various simulation rounds was recorded. The device speed and direction of the communication device decided the mobility. The simulation was carried out based on the parameters given in Table 1. The constraint of the transmit amplifier was important so that even weak signals could be captured with low power transmission. The heterogeneous sensors were used by providing the amount of initial energy for the sensor nodes, and the cluster head selection in every round was directly proportional to the initial energy of the node. The packet size was the most significant characteristic for reliability and transmission delay. The super nodes had and consumed a high amount of energy compared with the normal and advanced nodes, which would balance the consumption of energy by all the nodes and increase the lifetime of the network.

Figure 6 shows the comparison of the suggested TIGSO-EDS technique with the EEHC, EECT, and S-EECP methods based on the calculations and displays. TIGSO-EDS

improved the data packet delivery ratio by 5.66%, 3.84%, and 2.50% with EEHC, EECT, and S-EECP, respectively. When the base station was located at 100 × 250, the success data was evaluated, and it was observed to have worse performance than the previous scenario. The same was observed with the other models, and the comparison results are presented in Figure 7.

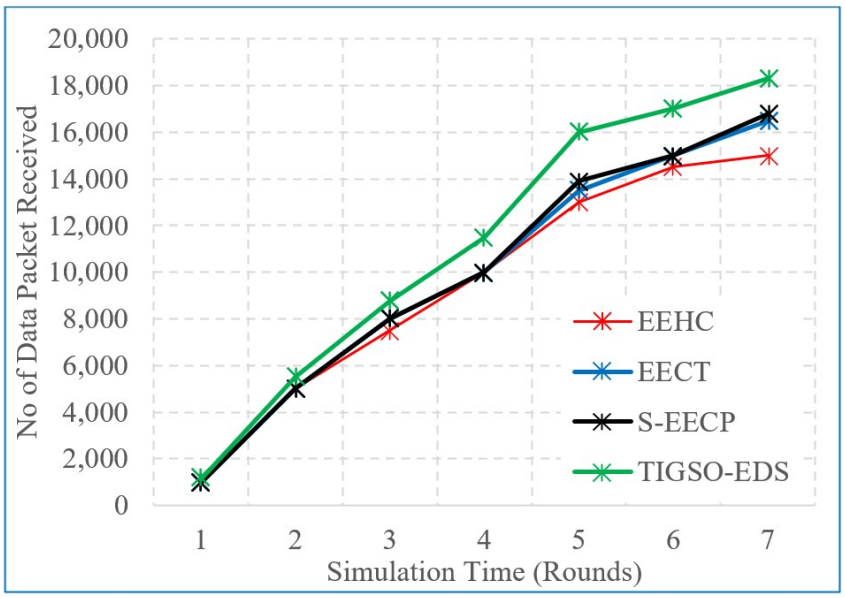


Figure 6. Comparison of data packets received at the base station (BS) located at 50 × 50).

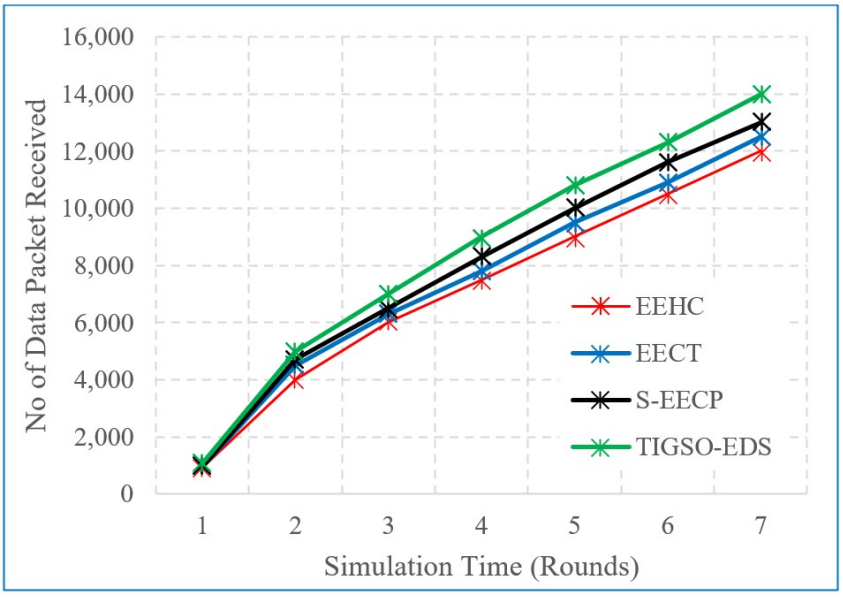


Figure 7. Comparison of data packets received at the base station (BS) located at 100 × 250).

The energy consumption per round for the proposed TIGSO-EDS method and other different methods were calculated, and they are shown below in Figure 8. A comparison of the energy consumption with TIGSO-EDS with the base station located at 50 × 50 is shown in Figure 8. From the analysis, it is shown in Figure 9 that the proposed TIGSO-EDS method improved the energy consumption per round by 19.96%, 16.85%, and 12.71% when compared with EEHC, EECT, and S-EECP, respectively.

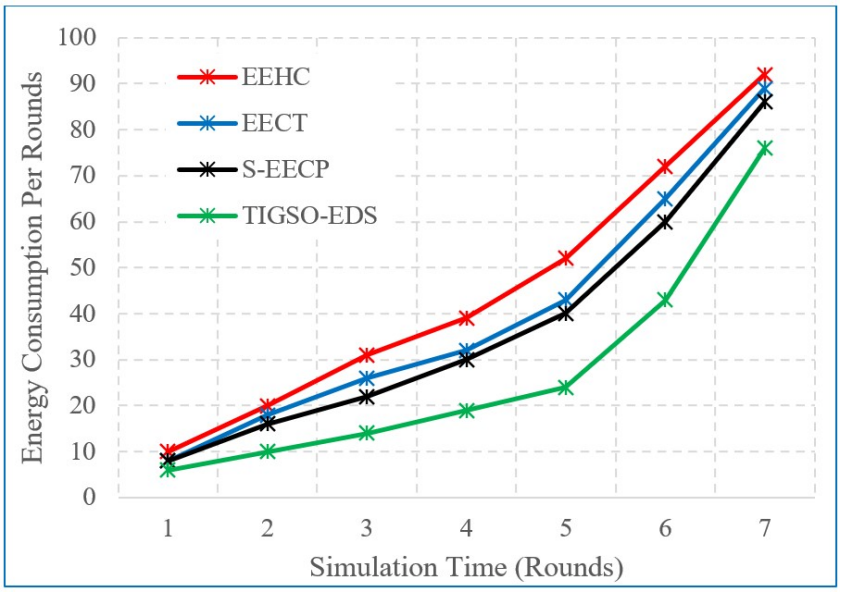


Figure 8. Energy consumption of different methods (base station located at 50 × 50).

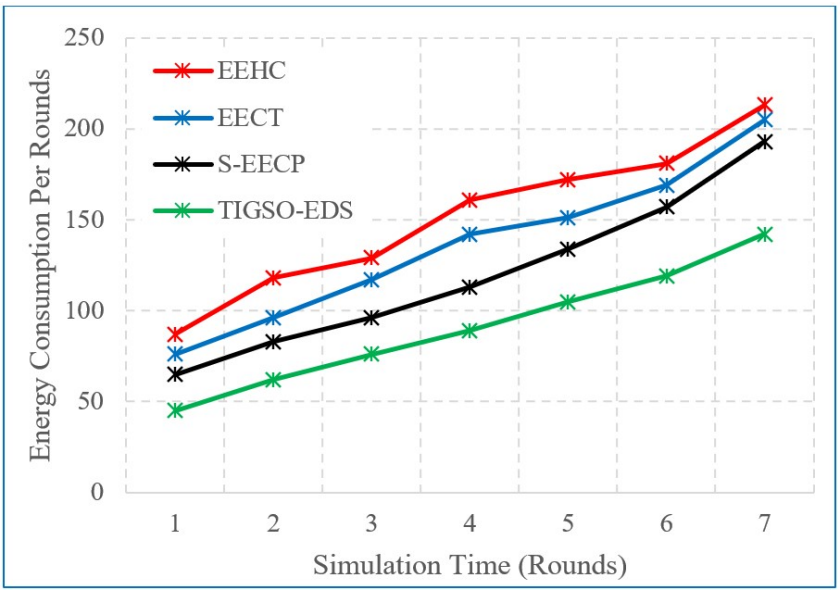


Figure 9. Energy consumption of different methods (base station located at 100 × 250).

The comparison of energy consumption per round for the proposed method TIGSO-ADC method with EEHC, EECT, and S-EECP was calculated with a base station located at 100 × 250, as shown in Figure 8. From the analysis, it is shown in Figure 9 that the proposed TIGSO-EDS method improved the energy consumption per round by 18.86%, 15.99%, and 12.16% when compared with EEHC, EECT, and S-EECP, respectively.

5. Conclusions

In this paper, an enhanced clustering method (TIGSO-EDS) was designed and implemented. Optimal CH selection was carried out using the hybrid VIKOR-GSO method, and data aggregation was performed on the selected CH. Next, the aggregated data were passed to the BS through the best possible path, selected using the Cuckoo Search algorithm. Here, the security was guaranteed by the encrypted process between the BS and the CH. The simulation results showed that the proposed TIGSO-EDS method had enhanced performance than the existing EEHC [17], EECT [32], and S-EECP [33] methods regarding the network energy consumption, throughput, aggregation latency, and delay

parameters. It uses the hybrid VIKOR method combined with GSO, which is applied to select the cluster head in the network. Then, for cluster formation, a GA was used, and data aggregation was performed. To transfer the data securely, they were encrypted using AES. The Cuckoo Search algorithm (CSA) was followed to find the optimum path, and then the data were communicated to the BS for further processing. The simulation results show that TIGSO-EDS performed better compared with the other methods.

Future Scope

In this paper, we talked about how long a grid lasts, how much energy it uses, and how well it covers an area. However, there are other ways to measure how well a routing method works, such as the rate at which packages are delivered, how reliable it is, and how good the service is. In future works, it is proposed that these indicators will be used to measure how well the proposed method works. In addition, in this work, sensors were put together in clusters based on their distance from each other. This method might not always obtain results in all real-time applications. It is suggested that future works on the clustering phase of sensors find better ways to get around this problem.

Author Contributions: Conceptualization, P.S., V.K.B., A.A. and M.B.; data creation, S.G.; formal analysis, S.G. and A.A.; investigation, A.A. and M.B.; methodology, S.G.; project administration, G.S. and S.G.; resources, G.S.; software, M.B.; supervision, P.S., M.B. and G.S.; validation, S.G. and P.S.; visualization, M.B.; writing—review and editing, G.S., M.B. and S.G. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number (IFP-2020-114).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

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

References

1. Zhao, H.; Guo, S.; Wang, X.; Wang, F. Energy-efficient topology control algorithm for maximizing network lifetime in wireless sensor networks with mobile sink. *Appl. Soft Comput.* **2015**, *34*, 539–550.
2. Amutha, J.; Sharma, S.; Sharma, S.K. Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions. *Comput. Sci. Rev.* **2021**, *40*, 100376.
3. Merabtine, N.; Djenouri, D.; Zegour, D.E. Towards energy efficient clustering in wireless sensor networks: A comprehensive review. *IEEE Access* **2021**, *9*, 92688–92705.
4. Ahmad, H.; Kohli, N. LBCM: Energy-efficient clustering method in wireless sensor networks. *Eng. Appl. Sci. Res.* **2021**, *48*, 529–536.
5. Rathore, P.S.; Chatterjee, J.M.; Kumar, A.; Sujatha, R. Energy-efficient cluster head selection through relay approach for WSN. *J. Supercomput.* **2021**, *77*, 7649–7675.
6. Maheshwari, P.; Sharma, A.K.; Verma, K. Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization. *Ad Hoc Netw.* **2021**, *110*, 102317.
7. Al-Zubi, R.T.; Kreishan, A.A.; Alawad, M.Q.; Darabkh, K.A. Solution for intra/inter-cluster event-reporting problem in cluster-based protocols for wireless sensor networks. *Int. J. Electr. Comput. Eng. (IJECE)* **2022**, *12*, 868–879.
8. Rodríguez, A.; Pérez-Cisneros, M.; Rosas-Caro, J.C.; Del-Valle-Soto, C.; Gálvez, J.; Cuevas, E. Robust clustering routing method for wireless sensor networks considering the Locust search scheme. *Energies* **2021**, *14*, 3019.
9. Zhao, Z.; Shi, D.; Hui, G.; Zhang, X. An energy-optimization clustering routing protocol based on dynamic hierarchical clustering in 3D WSNs. *IEEE Access* **2019**, *7*, 80159–80173.
10. Machado, K.; Rosário, D.; Cerqueira, E.; Loureiro, A.A.; Neto, A.; De Souza, J.N. A routing protocol based on energy and link quality for internet of things applications. *Sensors* **2013**, *13*, 1942–1964.
11. Yuehong, Y.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13.

12. Aslani, Z.; Sargolzaey, H. Improving the performance of rpl routing protocol for internet of things. *J. Comput. Robot.* **2017**, *10*, 69–75.
13. Sampathkumar, A.; Mulerikkal, J.; Sivaram, M. Glowworm swarm optimization for effectual load balancing and routing strategies in wireless sensor networks. *Wirel. Netw.* **2020**, *26*, 4227–4238.
14. Yadav, K.; Al-Dhlan, K.A. Performance evaluation using hybrid glowworm swarm-Pareto optimization in the smart communication system. *Comput. Electr. Eng.* **2022**, *103*, 108313.
15. Idrees, A.K.; Al-Qurabat, A.K.M. Energy-efficient data transmission and aggregation protocol in periodic sensor networks based fog computing. *J. Netw. Syst. Manag.* **2021**, *29*, 1–24.
16. Jain, K.; Mehra, P.S.; Dwivedi, A.K.; Agarwal, A. SCADA: Scalable cluster-based data aggregation technique for improving network lifetime of wireless sensor networks. *J. Supercomput.* **2022**, *78, 13624–13652*.
17. Rawat, P.; Chauhan, S.; Priyadarshi, R. A novel heterogeneous clustering protocol for lifetime maximization of wireless sensor network. *Wirel. Pers. Commun.* **2021**, *117*, 825–841.
18. Naghibi, M.; Barati, H. SHSDA: Secure hybrid structure data aggregation method in wireless sensor networks. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 10769–10788.
19. Mukherjee, P.; Pattnaik, P.K.; Al-Absi, A.A.; Kang, D.K. Recommended System for Cluster Head Selection in a Remote Sensor Cloud Environment Using the Fuzzy-Based Multi-Criteria Decision-Making Technique. *Sustainability* **2021**, *13*, 10579.
20. Gautam, A.K.; Kumar, R. A trust based neighbor identification using MCDM model in wireless sensor networks. *Recent Adv. Comput. Sci. Commun.* **2021**, *14*, 1336–1351.
21. Ghadikolaei, A.S.; Madhoushi, M.; Divsalar, M. Extension of the VIKOR method for group decision making with extended hesitant fuzzy linguistic information. *Neural Comput. Appl.* **2018**, *30*, 3589–3602.
22. Wei, G.; Wang, J.; Lu, J.; Wu, J.; Wei, C.; Alsaadi, F.D.; Hayat, T. VIKOR method for multiple criteria group decision making under 2-tuple linguistic neutrosophic environment. *Econ. Res.-Ekon. Istraž.* **2020**, *33*, 3209–3237.
23. Arpaia, P.; Bonavolontá, F.; Cioffi, A. Problems of the advanced encryption standard in protecting Internet of Things sensor networks. *Measurement* **2020**, *161*, 107853.
24. Shahraki, A.; Taherkordi, A.; Haugen, Ø.; Eliassen, F. Clustering objectives in wireless sensor networks: A survey and research direction analysis. *Comput. Netw.* **2020**, *180*, 107376.
25. Ajmi, N.; Helali, A.; Lorenz, P.; Mghaieth, R. MWCSGA—Multi weight chicken swarm based genetic algorithm for energy efficient clustered wireless sensor network. *Sensors* **2021**, *21*, 791.
26. Saffari, A.; Zahiri, S.; Khishe, M. Fuzzy grasshopper optimization algorithm: A hybrid technique for tuning the control parameters of GOA using fuzzy system for big data sonar classification. *Iran. J. Electr. Electron. Eng.* **2022**, *18*, 2131–2131.
27. Liu, X.; Yu, J.; Yu, K.; Wang, G.; Feng, X. Trust secure data aggregation in WSN-based IIoT with single mobile sink. *Ad Hoc Netw.* **2022**, *136*, 102956.
28. Aljumaie, G.S.; Alhakami, W. A Secure LEACH-PRO Protocol Based on Blockchain. *Sensors* **2022**, *22*, 8431.
29. Lilhore, U.K.; Khalaf, O.I.; Simaiya, S.; Tavera Romero, C.A.; Abdulsahib, G.M.; Kumar, D. A depth-controlled and energy-efficient routing protocol for underwater wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **2022**, *18*, 15501329221117118.
30. Hussein, S.M.; López Ramos, J.A.; Ashir, A.M. A Secure and Efficient Method to Protect Communications and Energy Consumption in IoT Wireless Sensor Networks. *Electronics* **2022**, *11*, 2721.
31. Hossan, A.; Akter, M.S.; Choudhury, P.K. Distance and Energy Aware Extended LEACH using Secondary Cluster Head for Wireless Sensor Networks. *Telemat. Inform. Rep.* **2022**, *8*, 100029.
32. Li, X.; Keegan, B.; Mtenzi, F.; Weise, T.; Tan, M. Energy-efficient load balancing ant based routing algorithm for wireless sensor networks. *IEEE Access* **2019**, *7*, 113182–113196.
33. El Alami, H.; Najid, A. ECH: An enhanced clustering hierarchy approach to maximize lifetime of wireless sensor networks. *IEEE Access* **2019**, *7*, 107142–107153.
34. Gopikrishnan, S.; Priakanth, P. HSDA: hybrid communication for secure data aggregation in wireless sensor network. *Wirel. Netw.* **2016**, *22*, 1061–1078.
35. Bruxaux, J.; Ashari, M.G.H.; Prŷs-Jones, R.; Joseph, L.; Milá, B.; Besnard, G.; Thébaud, C. Recovering the evolutionary history of crowned pigeons (Columbidae: Goura): Implications for the biogeography and conservation of New Guinean lowland birds. *Mol. Phylogenetics Evol.* **2018**, *120*, 248–258.
36. Mareli, M.; Twala, B. An adaptive Cuckoo search algorithm for optimisation. *Appl. Comput. Inform.* **2018**, *14*, 107–115.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.