International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Dynamic Fuzzy Based High-Efficiency Clustering and Intrusion Prevention Routing Protocol for IOT Based Wireless Sensor Networks.

[1]Mr. J. Devasundarraj, [2]Dr. M. Arasakumar, [3]Dr. C. N. S. Vinoth Kumar

Submitted:14/03/2024 **Revised**: 29/04/2024 **Accepted**: 06/05/2024

Abstract: The rapid expansion of the Internet of Things necessitated the development of numerous services, programs, electronic devices with built-in sensors, and associated protocols, all of which are currently active. With the help of the internet of things, real-life objects can now see, hear, think, and do remarkable things thanks to improved communication, data sharing, and decision-making capabilities. The growth of the Internet of Things (IoT) relies heavily on wireless sensor networks (WSNs), which are made up of inexpensive smart devices that collect data. But there are limits to the amount of processing power, memory, and energy that these smart gadgets can use. Achieving dependability while protecting transmitted data in a susceptible environment using energy-saving strategies is one of the main problems for WSN. Wireless sensor networks have a major issue with energy efficiency. Due to their dependence on batteries, sensor networks eventually fail. In order to alleviate these issues, this article presents the DFHC-IPR protocol for WSN-assisted IoT systems, which stands for dynamic fuzzy-based high-efficiency clustering and intrusion prevention routing protocol. An energy-efficient clustering technique called dynamic fuzzy multi-criteria decision making is used, which is a combination of fuzzy AHP with TOPSIS to find the best cluster heads. An intrusion prevention optimization technique is employed for routing purposes to improve data delivery security. The proposed method's first step is to use nodes' inherent properties to form various energy-efficient clusters. In addition, the *(k,n)* threshold-based Shamir secret sharing system ensures the confidentiality and dependability of the sensory information between the cluster head and the base station (BS). Performance metrics, including throughput, energy economy, and data security, have all been enhanced by implementing and comparing this routing protocol with two other existing protocols.

Keywords: necessitated, optimization, Achieving, Performance metrics

Introduction:

In recent years, the Internet of Things (IoT) has grown rapidly [1], providing limitless applications in numerous domains such as smart cities, smart buildings, smart grids, intelligent transportation systems, healthcare, education, industry, entertainment, and more.[2][3] Internet of Things (IoT) refers to the network of interconnected physical devices, services, and information that will enable communication among machines (M2M) and constitute the "next generation" of the Internet [4]. The fundamental idea behind the Internet of Things is to enable communication between any two homogenous items, regardless of their location. One of the first technologies for the Internet of Things (IoT), radio-frequency identification (RFID) [5][6][7] uses electromagnetic fields to automatically transmit identifying data to a reader over wireless connection devices. Radio frequency identification (RFID) systems primarily consist of tag readers and radio signal transponders (tags). Typically, radio frequency identification tags have data stored electronically, allowing individuals to categorize, follow, and keep tabs on the items. Radio frequency identification tags may be affixed to virtually anything in order to track its precise location and collect data.

A Wireless Sensor Network (WSN) is a system of interconnected, autonomous sensors that can detect and report changes in parameters including sound level, temperature, pressure, and motion. In order to send the data that they've gathered to a central server or computer, these sensors often use radio waves for wireless communication. Wireless sensor networks (WSNs) have several uses, such as in healthcare, smart homes, industrial automation, and environmental monitoring [8]. Their versatility and resilience in the face of extreme conditions make them an important component of many cutting-edge technological systems. The Internet of Things (IoT) and wireless sensor networks (WSNs) are becoming feasible solutions that are widely employed in real-time data gathering and monitoring applications [9]. These applications include automatic irrigation, target monitoring, viewing clinical records, tracking landslides,

[1]Research Scholar, Department of Information Technology Annamalai University, Chidambaram, Tamilnadu, India. Mail jdevasundarraj@gmail.com
[2]Department of Information Technology Annamalai University, Chidambaram, Tamilnadu, India.
[3]Department of Networking and Communications,School of Computing SRM institute of Science and Technology, Kattankulathur, Tamilnadu, India.

and making forecasts for forest fire and catastrophe management.

In addition, wireless sensor networks (WSNs) that are based on the Internet of Things are utilized in both monitored and unmonitored settings, such as monitoring water quality, air pollution, and smart cities, among other applications [10]. In addition to providing reliable data forwarding, another important concern is to enhance energy efficiency [11]. In the past, a number of researchers have developed a cluster-based approach for wireless sensor networks (WSN) in order to successfully achieve energy efficiency [12]. Clustering techniques include the nodes being partitioned into distinct regions, with a single cluster head that is referred to as the leader node between the various regions. The purpose of the cluster head is to collect the data from the nodes that are members of the cluster, aggregate it, and then send it on to the base station (BS). Either a single hop or a multi-hop technique can be utilized to fulfil the task of transmitting data from cluster heads to BS [13].

In addition, the ESR protocol takes advantage of a constrained clustering practice to update the cluster heads' status with minimal communication cost, as each cluster is inundated with the least amount of re-election packets. Secondly, ESR protocol uses a lightweight secret sharing technique between cluster heads and BS to provide trustworthiness and safe data routing over the whole network [14]. Each member of the set of cluster heads shares a portion of the secret key that the BS creates under this method. The suggested secret sharing approach encrypts incoming packets as they travel between cluster heads and BS. Likewise, the suggested data security solution initiates decryption upon packet receipt at the BS from the cluster heads prior to onward transmission to the end user [15].

Early on, the Internet is shifting its focus from connecting people to connecting things, in order to encourage a new way of thinking about the Internet of Things (IoT). According to Farman et al. (2018) [16], and Mahajan et al. (2016) [17], this new pattern introduces items or objects to the Internet and opens up new economic opportunities. Everything is operational and can become a new source of data for the internet, from interior wearable appliances to outside natural sensors. Raising the online components with a heightened awareness of the here and now. Internet of Things (IoT) is an exciting new field with a fresh, cutting-edge pattern. It is possible to get items online using a variety of approaches. Two methods to improve WSN energy efficiency in the IoT are routing and clustering.

Here are the key points of the paper:

In order to identify the cluster head, our proposed intrusion prevention routing protocol for IoT-based wireless sensor networks combines the TOPSIS approach with dynamic fuzzy based high efficiency clustering. Data security is improved with the usage of intrusion prevention routing protocol.

The following is the outline of the paper: Section 2 details the relevant literature. The approach that was presented is detailed in Section 3. Section 4 provides the experimental outcomes.

The conclusion and future scope are included in Sect. 5, the last section.

Related works:

The energy conservation aim is a demanding criterion in most large-scale networks, including the Internet of Things (IoT) and sensor nodes with limited resources [18][19]. Cluster heads often serve as a symbolic governing entity during data transmission and collection in cluster-based networks [20][21].

This means that, particularly in terms of network homogeneity and stability, picking the right cluster heads has a meaningful impact on network performance [22][23]. Due to resource constraints, safe data routing is an important component of large-scale IoT-based WSNs. The lack of safeguards against malevolent attacks causes most of the current systems' [24][25] network communication unreliable and unsafe.

In WSNs, layered and tiered data transmission is one of the most popular and reliable methods. Following extensive testing, this method is today considered to be one of the most effective routing systems for delivering data packets to their final destination, such as BS. Layers such as CMs, CLHs, and CLGs include all of the sensor nodes, and each layer is responsible for a certain function.

In large-scale networks with limited resources, like the Internet of Things (IoT) and sensor networks (SNs), energy saving is usually the most important consideration. Typically, CH is the controlling entity in cluster-based networks [26]. Its primary function is to collect and send data. Additionally, due to resource constraints, securely routing data is the most important component of large-scale WSNs connected with the IoT.

Due to a lack of a threat prevention schema, some current methods fail to deliver dependable and safe data routing in the network [27]. There are several steps to a LEACH protocol, which stands for low-energy adaptive clustering hierarchy [28]. Using a multi-hop foundation for data transmission improves the performance of the LEACH protocol [29].

A method for energy-limited heterogeneous fog-supported wireless sensor networks has been designated by Naranjo et al. (2017) [30]. This study presents an alternative method for selecting CHs in WSNs and organizing progressive nodes. Both the basic and advanced nodes' energy levels depend on prolong SEP (P-SEP), which was presented in this study. When it comes to choosing CHs from among the hubs, P-SEP is totally logical as it means that every node has an equal chance of being picked.

The data gathering technique and load balancing that the authors suggested in [31] are an attempt to reduce energy consumption and boost the network's performance in terms of data aggregation and forwarding. The suggested approach builds a stack of layers according on the number of hops between nodes and the sink node. On the other hand, communication costs rise due to the hop-by-hop nature of the next-hop selection operation. There are more route discoveries and more transmission delays as the network size increases.

According to the EEBCDA method [32], which stands for energy-efficient balanced cluster-based data aggregation, the network field is divided into rectangular grids of uneven sizes, each containing one cluster head. Within each grid, the position of the cluster head is moved among the member nodes. The knowledge about residual energy is used to choose a small number of nodes within each grid to serve as cluster heads. However, creating a grid is a more involved process that necessitates additional overhead.

A protocol for source location protection in WSNs based on dynamic routing has been proposed for the social internet of things (Han et al. 2018) [33]. In order to solve the problem of source zone security, this study suggests doing research on source region assurance conventions using dynamic coordination. We provide an adaptable course correction strategy for data transfer. An underlying hub is initially selected at random from the system's limit by the introduced plot. In order to reach the sink, the packet will first take an avaricious path and then a coordinated one.

Our plan can guarantee source territory security and combat various security disclosure assaults without hurting the system lifespan, according to both theoretical and exploratory outcomes.

A Dynamic fuzzy based high-efficiency clustering and Intrusion Prevention routing protocol:

The use of clustering and data aggregation is a crucial approach to improving energy efficiency using software-based protocols, which is a critical issue in WSN applications for energy efficiency. In order to reduce energy consumption and increase service quality, this article suggests a DFHEC-IPR protocol. We first assumed that WSNs have a variety of nodes with different types of data. In every single one There are various degrees of nodal energy at each node. The battery life of each sensor node is limited, and they cannot be recharged. The nodes may merge all the duplicate data, which reduces power consumption. Figure 1 explains the general technique that was introduced.

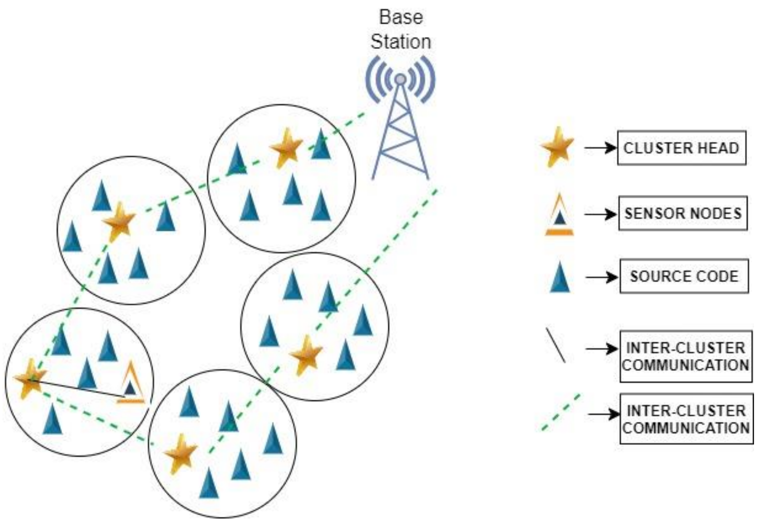

Fig.1 Flow of DFHC-IPR Methodology

• Minimize the cost of the intra-cluster communication.

• Minimize the cost of the inter-cluster communication.

The phrase "intra-cluster communication cost" refers to the total amount of all the individual expenses that are related with the links that connect all of the members of the cluster to their respective CHs. The overall cost of the tree that was formed, which is also referred to as the inter-cluster communication cost, is defined as the total of the costs of the links that connect with the CHs that comprise that tree.

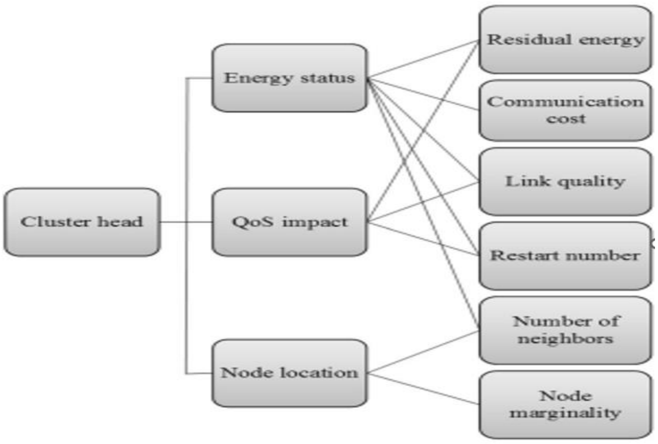

Fig 2. Decision Making Criteria for Cluster Head Selection

Implementation of the recently proposed system will be carried out with the assistance of the MATLAB platform. As far as quality-of-service parameters are concerned, the performance is evaluated and compared with an earlier clustering and routing scheme. These parameters include the ratio of packet delivery to packet loss, throughput, network lifetime, end-to-end delay, channel load, jitter, bit error rate (BER), buffer occupancy, and energy consumption. Concerning the performance, this evaluation and comparison is carried out in relation to the performance.

The following section provides a concise summary of the energy-efficient and secure routing (ESR) protocol that has been suggested for wireless sensor networks that are based on the Internet of Things. In the ESR protocol that has been described, the overall functionality of the protocol is split down into two major components. These components will be discussed in the subsequent sections of this article. In order to guarantee secure data routing inside the first component, the ESR protocol is in charge of organising the optimal hierarchical topology construction and the thresholding-based secret sharing scheme (SSS) [34]. This is done with the intention of guaranteeing that the data is routed safely within. The optimal cluster heads are determined in conjunction with the scattered clusters in a manner that is both balanced and efficient in terms of energy consumption. In addition to the restrictions imposed by the quality of service, this assessment is informed by a number of other considerations.

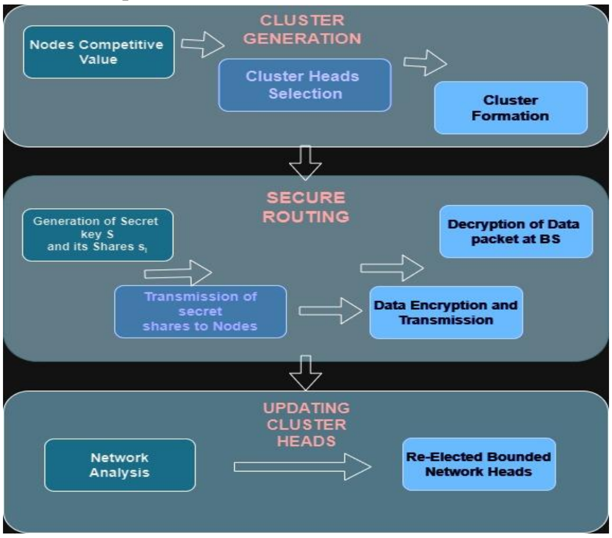

Fig 3. Block diagram of the energy-efficient and secure routing protocol (ESR) protocol

Optimise Clusters:

The initialization step begins by randomly dispersing the number of nodes in a square-sized network field. With a fixed identifier and few restrictions, each node continues to function normally. In terms of boundless resources, the BS 180 is limitless. At first, all of the nodes in the monitoring field were able to receive the 181 hop-by-hop broadcasts of *BS*'s location. In addition, each node's routing 182 table is updated with the neighbour's information. After that, ESR protocol 183 makes a dispersed announcement in the network field about the procedure for selecting the cluster leader. The competitive value 185 is calculated for all the nodes by taking into account the residual energy ei, the Received Signal Strength Indicator ($RSSIi$)184, the distance from the base station $di\ to\ BS$, and the queue length $QLii$ variables. In the process of exchanging control messages, every node learns about its 186 neighbours. Firstly, the maximum residual energy of a node is given 188 greater significances since node energy is the most important aspect in the network's survivability. Second, if the RSSI value is higher than a specific threshold, it indicates that the wireless link is performing well and can receive packets at a good pace (189). The RSSI threshold, as indicated in Equation 1, is calculated by the ESR protocol and is equal to the average reception rate of beacon packets from N neighbours at a specific time period (Δt). A number higher than the 192 calculated threshold is required for the node's RSSI. Low connection quality, as indicated by an RSSI value below the threshold, increases the chance of packet loss ratio (193). To get the value of R, we apply the following equation, where X is the reception rate of beacon 194 packets.

$$\text{RSSI}_{\text{threshold}} = \frac{X}{N}$$

As a third point, minimising energy consumption and maximising network lifetime are achieved by using the shortest path of node towards BS. Ultimately, the node-level congestion is measured by the queue length factor $Q\mathbf{O}ii$, which also increases data delivery performance 197. Equation (2) may be used to calculate the queue length QL_i of a node i, where RR_i is the packet receipt in bytes and TB is the total buffer size in bytes.

$$QL_i = \frac{RR_i}{TB}$$

Last but not least, as demonstrated in Equation (3), all factors are averaged using weights, and the nodes with the greatest competitive value $C_\text{v}$are chosen to serve as the first cluster heads. The suggested ESR technique chooses the best cluster heads according to their intrinsic properties, making the resulting clusters more flexible. A normalisation series of [0,1] is applied to the calculated value of C_v.

$$C_\text{v} = \text{w1} \times e_i + \text{w2} \times RSSI_i + \text{w3} \times \left(\frac{1}{d_i \text{ to } BS}\right) + \text{w4} \times QL_i$$

Cluster formation:

The initialization step begins by randomly dispersing the number of nodes in a square-sized network field. With few exceptions, every node has its own unique identifier and stays put. In terms of boundless resources, the BS 180 is limitless. At the outset, all the nodes in the field were able to receive the 181 hop-by-hop broadcasts of BS's location.

$$k = \sqrt{\frac{n}{2\pi}}\sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{mp}}}\frac{D}{x_{BSS^2}},$$

XBS is the average distance from all of the sensor nodes to the base station, where n is the number of nodes in the network and D is its dimension. The distances between the sensor nodes and the cluster centres are calculated using the following equation, which makes use of the concept of Euclidean distance.

$$X_{n2CC} = \sqrt{\sum_{j=1}^{N} (X_j - X_{CC})},$$

In this case, *Xn2CC* is the total distance from the node to the cluster centre, *Xj* is the position of the j*th* sensor node, and *XCC* is the total of all cluster centre coordinates.

Dynamic fuzzy based high-efficiency clustering

This work presents a dynamic clustering strategy that combines fuzzy PAH and CNN techniques to achieve optimum cluster head selection, resulting in great efficiency. Within In this method, three criteria and six sub-criteria are taken into account. it instantly stimulates the network's lifespan. The text is indistinct or unclear. PAH is used to determine the weights of each criterion. The CNN technique is used for the purpose of prioritising the options. There are three. The factors include energy status, influence on quality of service (QoS), and node placement. The number is six. The sub-criteria consist of residual energy and communication cost between. The information includes a node and its neighbouring nodes, the quality of the links between them, the number of times the node has been restarted, the number of neighbours it has, and the marginality of the node. Fig. 2 provides explanations for many criteria.

Risk Assessment

In this part, we conduct the weighting factor sensitivity analysis for the cluster head selection process in the dynamic network architecture. The equation optimises the cluster heads selection process by applying weighting factors w1, w2, w3, and w4. These variables take into account the values of residual energy, RSSI, proximity from BS, and the queue length factor. When calculating the relative importance of each component in an assessment, all of the relevant criteria are considered and weighted. For all weighted factors to be included, the total of their impact fractions must be 1, or 100%.

In order to assess the improved performance of cluster head selection, four distinct weighted factor values are employed.

Configuration-1 consists of w1 = 0.5, w2 = 0.3, w3 = 0.1, and w4 = 0.1.

Configuration-2 is characterised by w1 = 0.1, w2 = 0.5, w3 = 0.3, and w4 = 0.1.

Configuration-3 is defined by w1 = 0.3.

Configuration-4, the values are as follows: w1 = 0.2, w2 = 0.1, w3 = 0.1, and w4 = 0.6.

In the initial configuration, w2 = 0.1, w3 = 0.5, and w4 = 0.1.

All designs are evaluated based on energy usage, route breakages, and transmission.

Distance and packet delivery performance are used as benchmarks to get the optimal values for w1. w2, w3, and w4.

Furthermore, error bars are used as a visual depiction to illustrate the

Measurement errors or uncertainties in the experimental findings

Fig 4. Energy Consumption while cluster head selection

Figure 4 shows that when comparing configurations 2, 3, and 4 in terms of energy usage, configuration 1 yields superior results, with an average improvement of 31%. When sending and receiving cluster head election packets, the average power consumption ratio between sensor nodes is used to calculate energy usage.

You can see the results of route breakages for all the configurations in Figure 5, however configuration-2 performs better than configuration-1, configuration-3, and configuration-4 by an average of 38%.

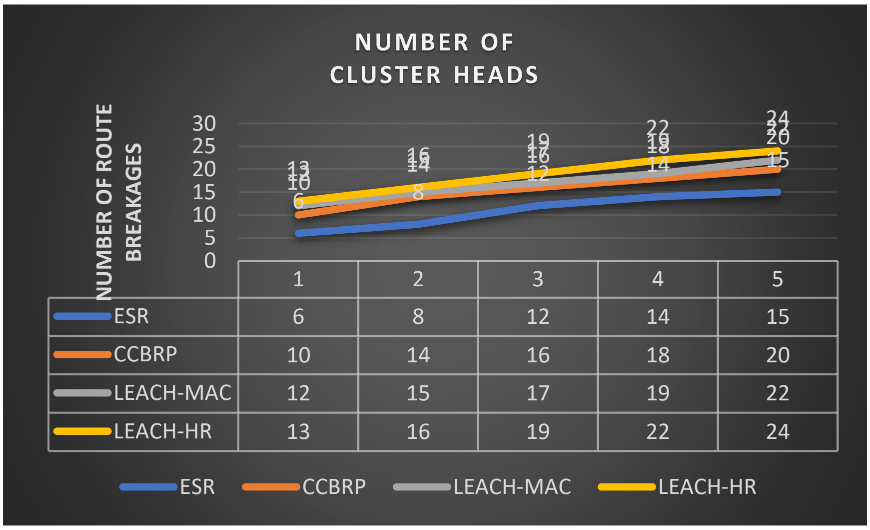

Fig 5. Performance of route breakages for all given configurations using different weighting factors

Finally, Figure 6 shows that compared to other configurations, configuration-4 yields superior results, on average, in terms of packet delivery ratio, by 37%.

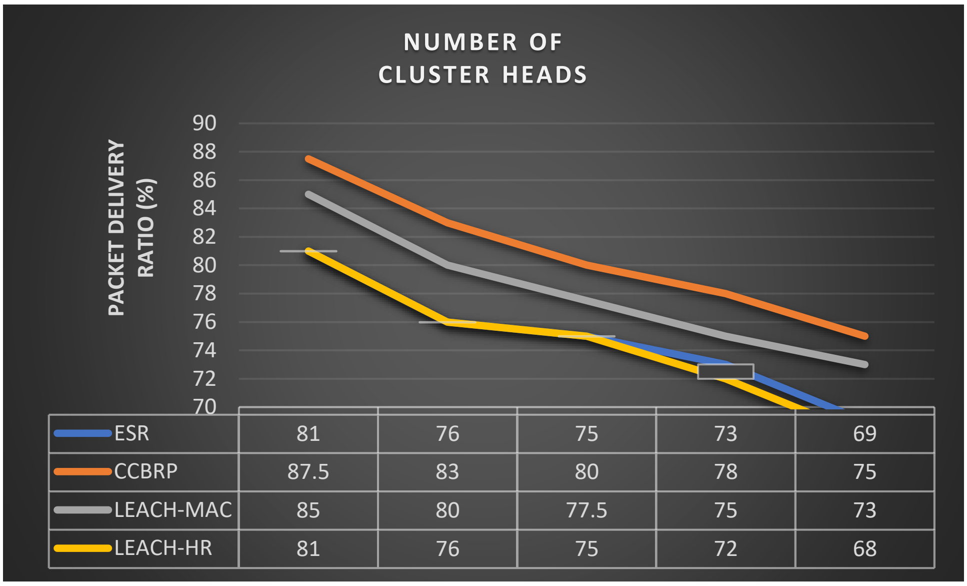

Fig 6. Packet delivery ratio for given all configurations with different weights

Experiment findings showed that under different IoT-based WSN topologies, each weighted component significantly affects the selection of cluster head, according to the performance sensitivity analysis shown in figures 4 – 6.

Remaining power

When thinking about wireless sensor networks, energy is the most crucial resource to consider. When it comes to processing, routing, and aggregating data, nodes that serve as cluster leaders use more power than other members of the cluster. This equation calculates the remaining energy.

$$E_r = E_0 - E_c$$

How much it costs for a node to communicate with its neighbours

The energy used by the sending message is exactly proportional to the square of the distance between the candidate nodes and the source node. The communication cost is defined as the numerical amount that represents the expense associated with transmitting information.

$$C = \frac{d_{\text{avg}}^2}{d_0^2},$$

The energy used by the sending message is exactly proportional to the square of the distance between the candidate nodes and the source node. The communication cost is defined as the numerical amount that represents the expense associated with transmitting information.

Emergence of issues with routing protocols

One way to put it is that the clustering and routing issue is a problem of minimising many objectives. In order to improve the dependability of data transmission, this article takes two goals into account. The goal is to keep the cost of communication inside and between clusters as low as possible. Data reliability is achieved via an optimisation process that is inspired by the immune system. This expression also optimises the cost of communication between clusters as well as within them.

$$\sum_{k=1}^{|V|} \sum_{m=1}^{|C_k|} w_{cm_{m,k} \to CH_k}$$

$$\sum_{k=1}^{|V|} w_{\text{CH }_k \to \text{ Next Hop }_{\text{CH }_k}},$$

Where, CH_k → CH number k; k → Total number of selected CHs; NextHop CH_k → Next hop for CH_k; $\text{cm}_{m,k}$ → Cluster

member number m of cluster $\square_k$; V→ The vector comprising the selected CHs; C_k→The vector covering the cluster members in the cluster that corresponds to CH_k

Experimental results and discussion

The presented technique is integrated into the MATLAB program. It determines how well the new method performs in comparison to the current clustering and routing protocols of MOBFO-EER, FRLDG, TCBDGA, and HEED. Using one hundred nodes, we can calculate the quality-of-service metrics for the following: end-to-end latency, energy consumption, channel load, jitter, bit error rate (BER), packet delivery ratio, throughput, and packet loss ratio. Table 2 displays the remaining simulation settings. As shown in Table 3, the parameters of the newly implemented routing and clustering protocol are examined.
In order to determine how effective the proposed routing

mechanism is, we use the following performance measures in conjunction with the simulation results.

$$\text{Packet Delivery Ratio} = \frac{No\ of\ packets\ transmitted\ successfully}{No\ of\ packets\ generated} X\ 100$$

Delay = Queuing delay + Processing delay + Propagation delay

PARAMETER	VALUE
Area	1000X1000 m
BS Location	1000-1150 m
Number of nodes	100
Initial Energy	0.1J
Bandwidth	20 kbps
Packet size	500 bytes
Node distribution	Random values
Total number of nodes in the region	500
Antenna direction	Omni-directional

Table 1: Simulation Parameters

No of nodes vs Qos parameters

QoS parameters	**No of nodes**	**Energy consumption (M_j)**	**Network life-time (rounds)**	**Packet deliv-ery ratio (%)**	**End to end delay (sec)**	**Throughput (Mbps)**	**Packet loss ratio (%)**	**Bit error rate (%)**	**Channel load (%)**	**Buffer occu-pancy (%)**	**Jitter (M_S)**
DFHC-IPR (Proposed)	100	45	5600	100	2.2	0.98	0	28	28	26	0.38
	200	70	5300	99	3.8	0.88	1	25	24	24.5	0.36
	300	97	5100	98	4.9	0.75	2	22.5	22	21	0.35
	400	110	4950	97	5.5	0.62	3	18	21	19	0.33
	500	145	4800	96	6.1	0.59	4	20	20	18	0.31
MOBFO-EER	100	55	5200	99	2.9	0.77	1	24	26	23	0.55
	200	80	4900	98	4.8	0.65	2	26	24	15	0.49
	300	107	4800	97	6.0	0.60	3	18	23	20	0.49
	400	140	4500	96	7.5	0.54	4	17	20	19	0.47
	500	165	4300	95	8.9	0.51	5	17.5	17	20	0.44
TCBDGA	100	65	4900	98	4.0	0.88	2	19	15.5	19.5	0.65
	200	105	4800	97	5.3	0.71	3	18	25	25	0.62
	300	140	4600	96	6.2	0.68	4	11	19	26	0.61
	400	158	4200	95	8.2	0.62	5	10.5	18.5	27	0.6
	500	183	4000	94	9.1	0.52	6	14	14	22	0.55
HEED	100	135	4500	97	5.8	0.44	3	8	14	24.5	0.6

	200	159	4300	96	6.2	0.75	4	9	24	25	0.59
	300	180	3900	95	7.4	0.69	5	14	19	19	0.57
	400	210	3500	94	8.0	0.60	6	20.5	18	17.5	0.56
	500	250	3300	93	9.5	0.50	7	24	16	15	0.5
FRLDG	100	143	4200	96	6.3	0.44	4	17	14	14.5	0.7
	200	170	4000	95	7.0	0.65	5	15.2	20	11	0.69
	300	195	3800	94	8.8	0.58	6	14	21	9	0.65
	400	240	3500	93	9.2	0.44	7	11	18	8	0.6
	500	275	3200	92	10.1	0.32	8	12	17	9	0.53

Table 2. Results obtained for Number of nodes versus QoS Parameters

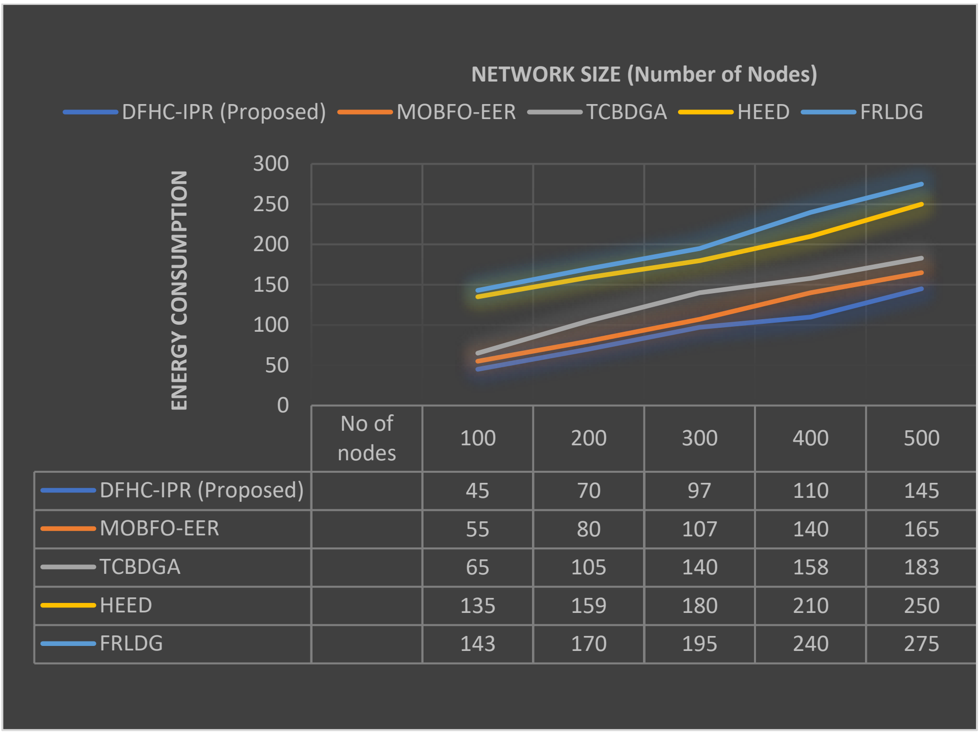

Fig 7. Performance of Energy Consumption

The results of the energy usage are shown in Figure 7. There is a range of 0 to 300 for energy usage. Compared to previous techniques, the one that was proposed utilises 45 M_S of energy in 100 nodes. Present methods MOBFO-EER (55 M_S), FRLDG (65 M_S), TCBDGA (135 M_S), and HEED (143 M_S) all use a considerable amount of energy in a network of 100 nodes.

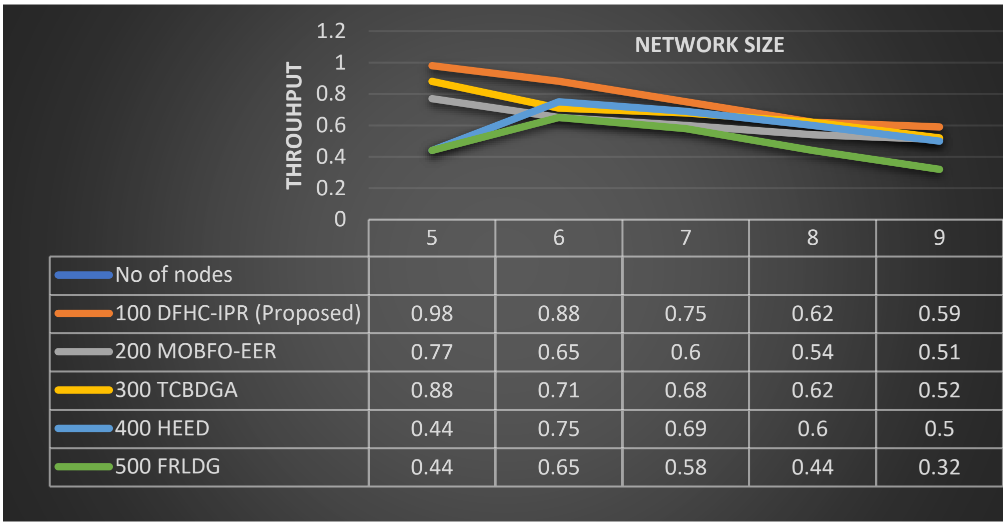

Fig 8. Throughput Performance

The comparison of network lifespan is shown in Figure 8. As can be seen from the graph, the proposed Fuzzy logic method outperforms the alternatives in terms of network lifespan. Whereas MOBFO-EER uses 5000 rounds, FRLDG uses 4800 rounds, TCB-DGA uses 4300 rounds, and HEED uses 4100 rounds, the presented method makes advantage of a wide network lifespan of 5500 rounds over 100 nodes.

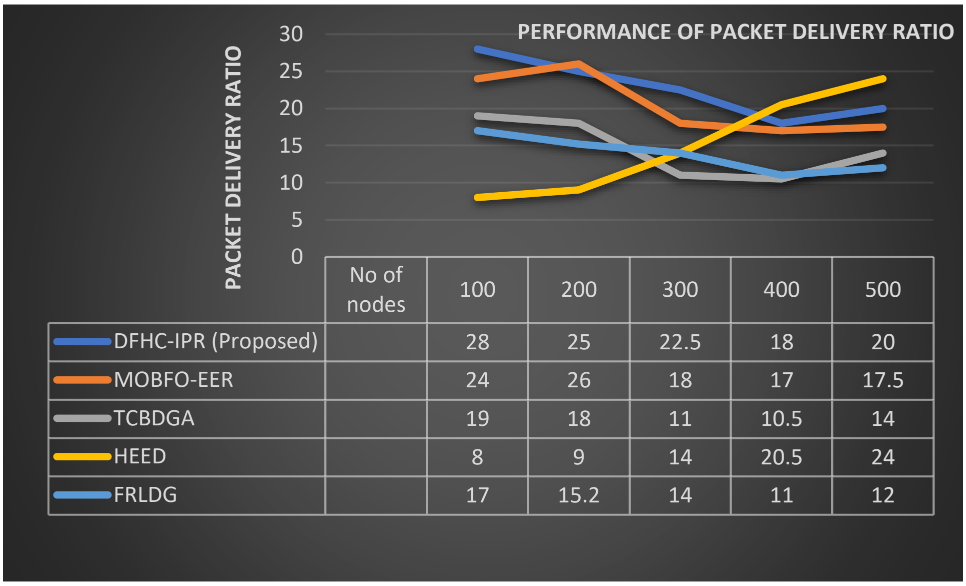

Fig 9. Performance of Packet delivery ratio

Figure 9 displays the results of the packet delivery ratio for both the current method and the newly introduced method (DFHC-IPR). As the number of nodes increases, the simulation shows that the packet delivery ratio decreases. In a network with 100 nodes, the presented method achieves an impressive packet delivery ratio of 99%. There are four current methods that provide packet delivery ratios of 98% in 100 nodes: MOBFO-EER, 97% in FRLDG, 95% in TCBDGA, and 93% in HEED.

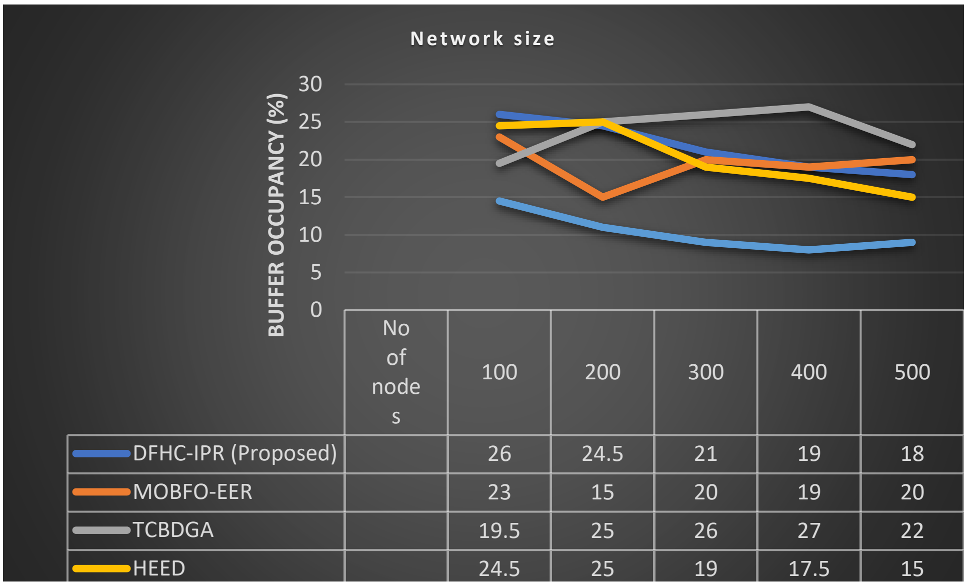

Fig 10. Performance of Buffer Occupancy

Figure 10 depicts the buffer occupancy performance of the new (DFHC-IPR) and current techniques. The simulation demonstrates that the suggested method successfully achieved a high buffer occupancy of 26% over 100 nodes. Hence, our newly implemented protocol is superior in terms of efficiency compared to existing energy-efficient protocols. The buffer occupancy percentages of the current techniques MOBFO-EER, FRLDG, TCBDGA, and HEED are 23%, 20%, 18%, and 15% respectively.

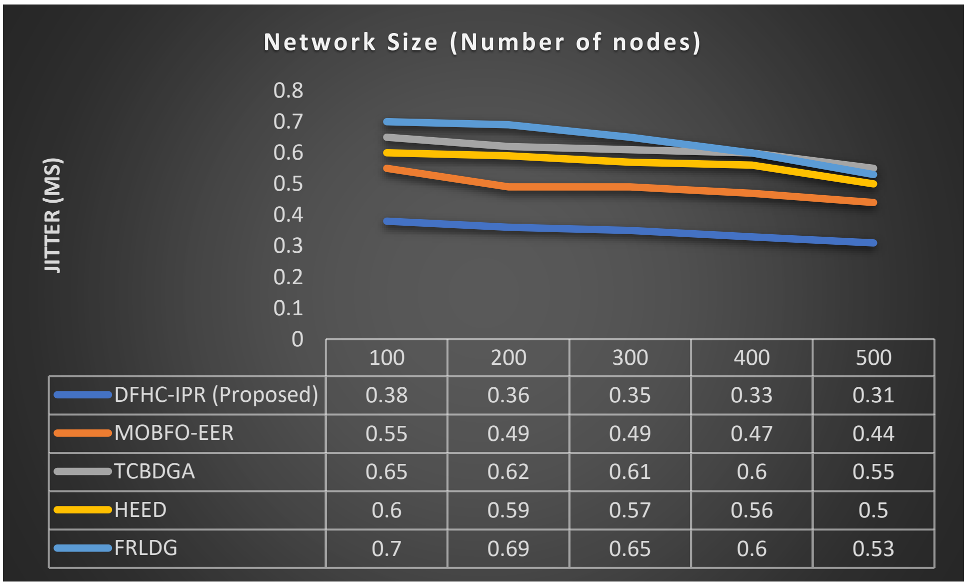

Fig 11. Performance of Jitter (M_S)

Figure 11 illustrates the comparison of jitter between our newly developed DFHC-IPR protocols and the old protocols. The findings indicate that our introduced method achieved a low jitter value of 0.38 M_S over 100 nodes. Hence, the newly developed protocol surpasses previous current energy protocols in terms of efficiency. The jitter values for the current protocols MOBFO-EER, FRLDG, TCB-DGA, and HEED are 0.55 M_S, 0.65 M_S, 0.6 M_S, and 0.7 M_S, respectively.

Conclusion

This work presents a dynamic fuzzy-based high-efficiency clustering and intrusion prevention routing algorithm for the Internet of Things (IoT). An advanced sensor network has been implemented. A novel clustering technique, called dynamic fuzzy-based high efficiency clustering, has been proposed. This approach selects a cluster head among the most eligible nodes based on critical parameters related to energy status. ESR enhanced the selection process of cluster heads and used a distributed strategy to create clusters that ensure equal distribution of energy usage. Furthermore, the cluster head selection strategy has the capability to decrease the amount of traffic and save energy. Most of the earlier solutions used a greedy algorithm to design the routing route, but failed to consider intrusions in an infrastructure-less and unsupervised environment. This leads to a significant increase in the number of route discoveries and re-transmissions, especially in situations when there are a large number of malicious nodes and a high network load. The intrusion prevention routing algorithm is used for the purpose of routing. In addition, the ESR protocol included a lightweight secret sharing system between cluster heads and BS to provide safe network-wide data routing and protect against rogue nodes. The MATLAB software package is used for simulating scenarios, and the data is obtained via real-time data transfer. The performance results are graphed based on QoS parameters, including packet delivery ratio (99%), packet loss ratio, throughput (0.95Mbps), network lifetime (5500 rounds), end-to-end delay, channel load, jitter, bit error rate (BER), buffer occupancy, and energy consumption (45 $\boldsymbol{M_j}$), in comparison to existing routing protocols. In the future, the goal is to discover the most efficient path with a significant amount of remaining energy for multi-hop inter-cluster communication. This involves strategically deploying many base stations in close proximity to a single base station in order to reduce the workload on cluster heads. This approach will enhance energy efficiency and prolong the total lifespan of the network in a wireless sensor network (WSN).

References:

[1] Kharrufa H, Al-Kashoash HA and Kemp AH. RPLbased routing protocols in IoT applications: a review. IEEE Sens J 2019; 19(15): 5952–5967.

[2] Lin JW, Chelliah PR, Hsu MC, et al. Efficient faulttolerant routing in IoT wireless sensor networks based on bipartite-flow graph modeling. IEEE Access 2019; 7: 14022–14034.

[3] Ercan AO¨, Sunay MO and Akyildiz IF. RF energy harvesting and transfer for spectrum sharing cellular IoT communications in 5G systems. IEEE T Mobile Comput 2017; 17(7): 1680–1694.

[4] Ahmed E, Yaqoob I, Gani A, et al. Internet-of-thingsbased smart environments: state of the art, taxonomy, and open research challenges. IEEE Wirel Commun 2016; 23(5): 10–16.

[5] Downie, J.D.; Nederlof, L.; Sutherland, J.S.; Wagner, R.E.; Webb, D.A.; Whiting, M.S. Radio Frequency Identification (RFID) Connected Tag Communications Protocol and Related Systems and Methods. U.S. Patent No. 9,652,707, 16 May 2017.

[6] Koch, M.J.; Swope, C.B.; Bekritsky, B.J. System for, and Method of, Accurately and Rapidly Determining, in Real-Time, True Bearings of Radio Frequency Identification (RFID) Tags Associated with Items in a Controlled area. U.S. Patent 9,773,136, 26 September 2017.

[7] Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Internet of things: Vision, applications and research challenges. Ad Hoc Netw. 2012, 10, 1497–1516. [CrossRef]

[8] Hong Z, Pan X, Chen P, Su X, Wang N, Lu W (2018) A topology control with energy balance in underwater wireless sensor networks for IoT-based application. Sensors 18:2306

[9] Sharma, N.; Sharma, A.K. Cost analysis of hybrid adaptive routing protocol for heterogeneous wireless sensor network. Sadhan ¯ a¯ 2016, 41, 283–288. [CrossRef]

[10] Wang, K.; Wang, Y.; Sun, Y.; Guo, S.; Wu, J. Green industrial Internet of things architecture: An energy-efficient perspective. IEEE Commun. Mag. 2016, 54, 48–54. [CrossRef]

[11] Abo-Zahhad, M.; Ahmed, S.M.; Sabor, N.; Sasaki, S. Mobile sink-based adaptive immune energy-efficient clustering protocol for improving the lifetime and stability period of wireless sensor networks. IEEE Sens. J. 2015, 15, 4576–4586. [CrossRef]

[12] Batra, P.K.; Kant, K. LEACH-MAC: A new cluster head selection algorithm for wireless sensor networks. Wirel. Netw. 2016, 22, 49–60. [CrossRef]

[13] Chen, G.; Li, C.; Ye, M.; Wu, J. An unequal cluster-based routing protocol in wireless sensor networks. Wirel. Netw. 2009, 15, 193–207. [CrossRef]

[14] Hassanabadi, B.; Shea, C.; Zhang, L.; Valaee, S. Clustering in vehicular ad hoc networks using affinity propagation. Ad Hoc Netw. 2014, 13, 535–548. [CrossRef]

[15] Xiong, Z.; Guo, T.; Xue, Z.; Cai, W.; Cai, L.; Luo, N. Online energy-efficient deployment based on equivalent continuous DFS for large-scale web cluster. Clust. Comput. 2018, 22, 583–596. [CrossRef]

[16] Farman H, Jan B, Javed H, Ahmad N, Iqbal J, Arshad M, Ali S (2018) Multi-criteria based zone head selection in internet of things based wireless sensor networks. Future Gener Comp Syst 87:364–371

[17] Mahajan S, Dhiman PK (2016) Clustering in WSN: a review. Int J Adv Res Comput Sci 7(3):198–201

[18] Batra, P.K.; Kant, K. LEACH-MAC: A new cluster head selection algorithm for wireless sensor networks. Wirel. Netw. 2016, 22, 49–60. [CrossRef]

[19] Hassanabadi, B.; Shea, C.; Zhang, L.; Valaee, S. Clustering in vehicular ad hoc networks using affinity propagation. Ad Hoc Netw. 2014, 13, 535–548. [CrossRef]

[20] Bian, X.; Liu, X.; Cho, H. Study on a cluster-chain routing protocol in wireless sensor networks. In Proceedings of the 2008 Third International Conference on Communications and Networking in China, Hangzhou, China, 25–27 August 2008; pp. 964–968.

[21] Enam, R.N.; Qureshi, R.; Misbahuddin, S. A uniform clustering mechanism for wireless sensor networks. Int. J. Distrib. Sens. Netw. 2014, 2014, 1–14. [CrossRef]

[22] Das, S.K.; Tripathi, S.; Burnwal, A. Intelligent energy competency multipath routing in wanet. In Information Systems Design and Intelligent Applications; Springer: Heidelberg, Germany, 2015; pp. 535–543.

[23] Latif, K.; Ahmad, A.; Javaid, N.; Khan, Z.; Alrajeh, N. Divide-and-rule scheme for energy efficient routing in wireless sensor networks. Procedia Comput. Sci. 2013, 19, 340–347. [CrossRef]

[24] Lou, C.; Zhuang, W. Energy-efficient routing over coordinated sleep scheduling in wireless ad hoc networks. Peer-to-Peer Netw. Appl. 2016, 9, 384–396. [CrossRef]

[25] Rani, S.; Talwar, R.; Malhotra, J.; Ahmed, S.H.; Sarkar, M.; Song, H. A novel scheme for an energy efficient Internet of Things based on wireless sensor networks. Sensors 2015, 15, 28603–28626. [CrossRef]

[26] Airehrour, D.; Gutierrez, J.; Ray, S.K. Secure routing for internet of things: A survey. J. Netw. Comput. Appl. 2016, 66, 198–213. [CrossRef]

[27] Deebak, B.D.; Al-Turjman, F. A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. Ad Hoc Netw. 2020, 97, 102022. [CrossRef]

[28] Yang, T.; Xiangyang, X.; Peng, L.; Tonghui, L.; Leina, P. A secure routing of wireless sensor networks based on trust evaluation model. Procedia Comput. Sci. 2018, 131, 1156–1163. [CrossRef]

[29] Safara, F.; Souri, A.; Baker, T.; Al Ridhawi, I.; Aloqaily, M. PriNergy: A priority-based energy-efficient routing method for IoT systems. J. Supercomput. 2020, 76, 8609–8626. [CrossRef]

[30] Selvakumar, K., & Revathy, G. (2018). Channel assinment using tabu search in wireless mesh networks. *Wireless Personal Communications*, *100*, 1633-1644.

[31] Guan, X.; Guan, L.; Wang, X.G.; Ohtsuki, T. A new load balancing and data collection algorithm for energy saving in wireless sensor networks. Telecommun. Syst. 2010, 45, 313–322. [CrossRef]

[32] Yuea, J.; Zhang, W.; Xiao, W.; Tang, D.; Tang, J. Energy efficient and balanced cluster-based data aggregation algorithm for wireless sensor networks. Procedia Eng. 2012, 29, 2009–2015. [CrossRef]

[33] Han G, Zhou L, Wang H, Zhang W, Chan S (2018) A source location protection protocol based on dynamic routing in WSNs for the social internet of things. Future Gener Comp Syst 82:689–697

[34] Shamir, A. How to share a secret. Commun. ACM 1979, 22, 612–613. [CrossRef]