Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 8s (2024)

Secure PSO based Energy Optimization Scheme using WSN for IoT Application

Divya Srivastava [1], Nitin Jain[2] and Manish Kumar[3]

[1,2] Electronics and Communication Department, BBD university, Lucknow, India

[3] Electronics and Communication Department, SUAS, Indore, India

divya.div1912@gmail.com

Article History:

Received: 12-10-2024

Revised: 15-11-2024

Accepted: 01-12-2024

Abstract: Wireless sensor networks (WSNs) and the Internet of Things (IoT) are having a growing impact on a number of applications particular to a domain. Because nodes in IoT-integrated WSNs have limited battery capacity, energy efficiency is a major design concern. There are a number of cluster-based routing strategies for homogeneous WSNs, but not many concentrate on energy-efficient HWSNs. Ensuring secure end-to-end complete communication in HWSNs is still a significant difficulty, though. An energy-saving secure routing system for Internet of Things applications in HWSNs is proposed in this study. The multipath link routing protocol (MLRP) is used in the method to create secure routing for sensitive IoT data via sensor nodes with heterogeneous energies. Following routing path security, the hybrid-based TEEN (H-TEEN) protocol, which also enables balancing of load, improves energy efficiency and network longevity. Furthermore, data storage capacity is increased via the ubiquitous data storage protocol (U-DSP). After being put into practice and compared to other protocols, the suggested routing protocol has shown improvements in throughput, energy efficiency, end-to-end latency, network longevity, and storage capacity of data.

Keywords: IoT, MLRP, U-DSP, WSNs.

1. Introduction:

For monitoring and real-time data collection across a range of applications, such as automated irrigation, target tracking, clinical record monitoring, landslide detection, forest fire prediction, and disaster management, the wireless Sensor Networks (WSNs) and Internet of Things (IoT) are becoming attractive options. A WSN is made up of many sensor nodes (SNs) that keep an eye on the weather and surroundings, particularly in hard or isolated places. As important predictors of impending calamities, these SNs assess vital atmospheric characteristics like pressure, temperature, humidity, sound, and moisture levels. After an SN has finished sensing, the information it has gathered is sent to a base station (BS) for additional processing.

The energy consumption of SNs is a critical concern, as their sensing and data transmission functions require significant power. Once a sensor node exhausts its energy, it becomes inoperative, and replacing or recharging it is often impractical. Therefore, optimizing power consumption is essential to enhance the longevity and performance of WSNs. To address this challenge, clustering approaches have been widely adopted, as they significantly extend network lifetime and improve efficiency are grouped by clustering, and each group is assigned a cluster head (CH), who is in charge of compiling

data from cluster members (CMs) and sending it to the BS. Clustering can be either temporary or permanent, depending on the method used. To ensure effective data communication, the clustering mechanism takes into account similarity metrics including cluster density, transmission radius, and distance from the base station.

After clusters are formed, the selection of an appropriate CH is crucial, as it directly impacts energy consumption and network performance. In some cases, when a single-node cluster is formed, the node must communicate directly with the sink instead of the BS, further reducing energy usage. However, WSNs face various challenges due to resource constraints, including limited energy, communication capabilities, stability, fault tolerance, mobility, bandwidth, reliability, heterogeneity and precision. Additionally, external environmental factors such as humidity, extreme temperatures, pressure variations, snow, rain, and dust can degrade sensor performance, necessitating robust and adaptive SNs. Other pressing challenges include network duration, throughput, security vulnerabilities, and routing protocol efficiency.

Energy consumption remains one of the most critical factors affecting WSN performance. Efficient energy utilization directly influences network lifespan, making energy optimization strategies essential. The key metrics for routing and cost function estimation (CF) in WSNs include total energy, energy consumption, and residual energy. Selecting an appropriate routing protocol is crucial to ensuring efficient data transmission while minimizing power consumption and network overhead. Despite ongoing research and technological advancements, further innovations are needed to optimize WSN performance and address existing limitations.

The IoT offers a wide range of benefits, particularly in urban environments. Urban IoT systems enhance public service management by optimizing transportation, parking facilities, street lighting, public area surveillance, waste collection, and cultural heritage preservation. Moreover, IoT-based solutions contribute to improved healthcare and education infrastructure, benefiting hospitals and schools. The vast amount of data generated by IoT-enabled smart cities can be stored in the cloud or centralized data warehouses, increasing transparency and promoting better governance. By leveraging IoT technology, local governments and municipalities can enhance public awareness, improve decision-making, and create smarter, more efficient cities. However, widespread adoption of IoT in urban settings requires time, investment, and strategic planning to fully realize its potential.

2. Related Works:

Energy saving is a major problem in large-scale networks with limited resources, including sensor networks (SNs) and the Internet of Things (IoT). The cluster head (CH) in cluster-based networks is essential to the transmission and aggregation of data. Due to limited resources and insufficient security measures, secure data routing in large-scale WSNs linked with IoT continues to be difficult. Many existing approaches fail to ensure reliable and secure routing, lacking protection against network threats.

The LEACH protocol operates in multiple stages. Its performance was enhanced using multi-hop transmission, but unstable energy consumption persisted due to random cluster formation. Additionally, the multi-hop paths were not optimized, leading to frequent route failures. The chain–chain-based routing protocol (CCBRP) combined LEACH and Power-Efficient Gathering in Sensor

Information Systems (PEGASIS), improving energy efficiency in SNs. However, the two-stage execution of CCBRP led to high energy consumption and latency, making it unsuitable for large-scale networks.

Kumar et al. proposed a data collection and load-balancing scheme to improve network performance through sequential data aggregation. An authentication protocol for industrial IoT-based WSNs enhanced data security through mutual authentication but consumed excessive energy, reducing network lifetime. Similarly, the Shamir secret-sharing method involved share generation and reconstruction, increasing routing overhead due to additional energy consumption during data transmission.

ETLHCM reduced control traffic during CH selection, extending network lifetime by 18% compared to the HHCA. However, it was ineffective for grid head (GH) selection. To counter Sybil, wormhole, and black hole attacks, Haseeb et al. introduced a novel protocol for secure routing. However, integrating GIN with the GEAR protocol proved too complex for effective security of data.

A hybrid ensemble classification approach based on voting achieved 96% accuracy in predicting parking lot availability, with an 89% success rate. The best possible network coding backpressure routing (NCBPR) method managed large-scale IoT networks by diverting data flow from the congested nodes to less loaded ones, load balancing and battery power optimization. Battery power was used to select CHs, and redundant data packets were eliminated to enhance throughput.

A load-balancing optimization algorithm improved energy-efficient routing and extended network lifetime. A cluster-based backpressure routing algorithm addressed congestion and energy issues in IoT environments. Further discussions on sustainable development through IoT explored its role in environmental monitoring using wireless sensors. A framework allowed real-time observation of sensor data via a web application, alerting users when environmental parameters exceeded set thresholds.

Energy efficiency remains a crucial issue in IoT and WSNs, particularly for applications in smart city, requiring continuous advancements to optimize performance and sustainability.

Research Objectives

1. To develop a safeguard and reliable routing mechanism for confidential IoT data transmission through sensor nodes with heterogeneous energy by making use of the Multipath Link Routing Protocol (MLRP), ensuring data integrity and protection against potential security threats.
2. To enhance energy efficiency and extend the overall network lifetime by implementing a hybrid-based TEEN (H-TEEN) protocol with advanced load-balancing capabilities, reducing energy consumption disparities among sensor nodes.
3. To optimize data management and improve storage efficiency by integrating the ubiquitous data storage protocol (U-DSP), enabling seamless data access, retrieval, and scalability in large-scale IoT-based WSN environments.

4. Methodology:

The suggested routing protocol combined with a storage feature enhancement mechanism, is structured into three key phases.

1. **Secure Data Routing:** The first phase focuses on establishing a secure and efficient data routing framework for IoT-based sensor networks. Using the Multipath Link Routing Protocol (MLRP), confidential data is securely transmitted through sensor nodes with heterogeneous energy, ensuring robust security and reliability in data transmission.
2. **Energy Optimization and Load Balancing:** In the second phase, the Hybrid Threshold-Sensitive Energy-Efficient Network (H-TEEN) protocol is incorporated. This procedure enhances energy efficiency by distributing the workload among sensor nodes, thereby balancing energy consumption and prolonging network lifespan. Secure data transmission is maintained throughout this process, ensuring minimal energy wastage.
3. **Enhanced Data Storage:** The final phase focuses on optimizing data storage capacity using the U-DSP. This ensures efficient data management, improved scalability, and seamless retrieval of stored information, supporting large-scale IoT applications.

The architectural framework of the proposed system is illustrated in Figure 1.

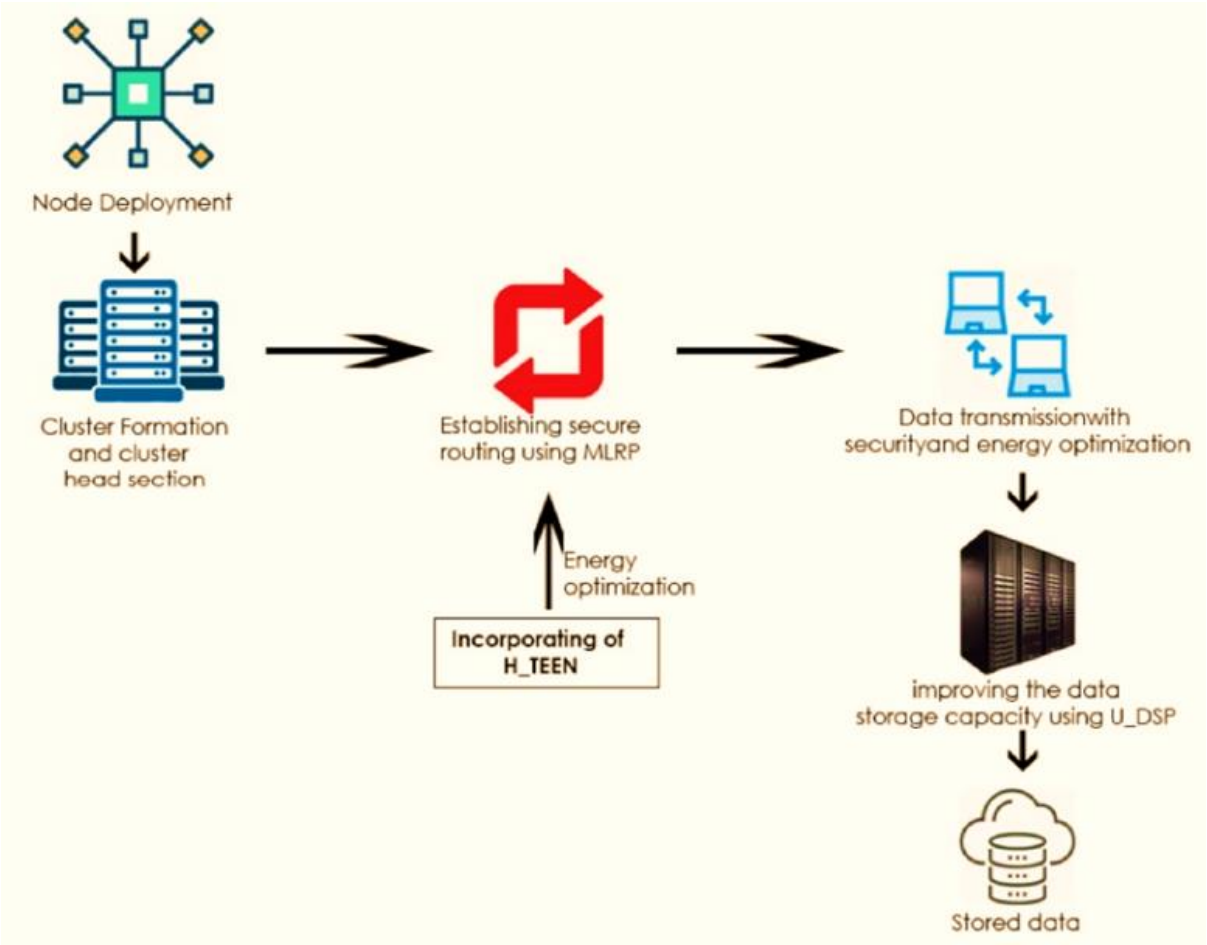

Figure 1. Proposed architecture.

3.1. MLRP

The five fundamental steps of the Multipath Link Routing Protocol (MLRP) are cluster formation, pairwise key distribution, neighbor identification, topology design, and transmission of data. For the IoT-based wireless sensor networks, each step is essential to creating a safe and effective routing system. Each sensor node is given a unique identity (IDx), a certificate (CERTx) for authentication, a public key (Kbs) for encryption, and a unique shared key (Kxbs) for secure communication during the neighbor identification and topology creation stage. To identify neighboring nodes, each node broadcasts a Neighbor Detection (NBR DET) packet, containing its ID and certificate (CERTx), which is received by nearby nodes to establish network topology. This structured topology ensures reliable communication and forms the foundation for secure routing. The subsequent phases—pairwise key distribution, cluster formation, and data transmission—build upon this topology, enhancing network security, optimizing energy usage, and ensuring seamless data flow. The overall process strengthens the efficiency and robustness of data transmission in large-scale IoT-integrated WSN environments.

$$x \rightarrow *: NBR\_DET|ID_x|CERT_x \quad (1)$$

Upon receiving the NBR_DET packet, the node first verifies the sender's identity by authenticating CERTx. If the authentication is successful, the sender's ID is added to the receiver's neighbor list. However, if authentication fails, the packet is discarded, preventing unauthorized nodes from participating in the neighbor detection process. Once the broadcasting process is completed, the collected neighbor information is transmitted to the Base Station (BS) as defined in the Equations (2) and (3).

$$x \rightarrow BS: NBR\_INFO|ID_x|CERT_x|E(k_{xbs}, NBR_x)| \quad (2)$$

$$MAC(k_{xbs}, NBR\_INFO|ID_x|CERT_x|E(k_{xbs}, NBR_x)| \quad (3)$$

A number of crucial tasks are carried out by an intermediary node that receives the NBR_INFO packet. First, it uses its certificate to confirm the sensor node's (SN) authenticity. The recipient node rebroadcasts the packet if the node's ID is approved. However, if a duplicate packet with the same ID is received again, it is discarded to prevent redundant transmissions. To efficiently manage this process, each node maintains a receiver packet table, which helps reduce network traffic and conserves energy. Once the NBR_INFO packet reaches the Base Station (BS), the BS verifies the Message Authentication Code (MAC) to ensure integrity and authenticity. Additionally, authentication of neighbor information is done via the shared key (Kxbs) between the SN and BS. The MAC, generated from the data and encrypted with Kxbs, ensures that , no one can fake or change neighbor information, enhancing the security and reliability of the network.

3.2. Distribution of Pairwise Key

Once the Base Station (BS) gathers neighbor information from network nodes, it thoroughly investigates the network topology and constructs a neighbor matrix, which represents the connectivity between nodes. To establish efficient data routing, the Depth-First Search (DFS) algorithm is applied, enabling the identification of multiple secure routes from the BS to every source node. This approach enhances network resilience by ensuring alternative routes are available in case of link failures.

Before executing the routing process, the BS generates a unique secret key for each neighbor pair, referred to as the pairwise key. This key is derived using a random number and a cryptographic hash function, ensuring a secure and tamper-resistant communication channel. The key generation process follows the mathematical formulation provided in Equations (4)–(6), strengthening the security framework of the network against potential cyber threats and unauthorized access..

$$k_{xy} = h(secret, ID_x, ID_y) \quad (4)$$

The Base Station (BS) unicasts this key to the relevant node as follows:

$$BS \rightarrow x: PAIR\_KEY|seqno|ID_{bs}|CERT_{bs}|\ ID_x|ID_y|E\left(k_{xbs}, k_{xy}|E\left(k_{ybs}, k_{xy}\right)\right) \quad (5)$$

$$MAC(k_{xbs}, PAIR_{KEY}|seqno|ID_{bs}|CERT_{bs}|ID_x|ID_y|E\left(k_{xbs}, k_{xy}|E\left(k_{ybs}, k_{xy}\right)\right) \quad (6)$$

The packet contains the following information: its type, sequence number, Base Station (BS) ID, neighbor and destination IDs, BS's certificate, pairwise key, and the Message Authentication Code (MAC) for the entire data. Each packet is received by an intermediary node that performs a series of operations:

Certificate Verification: The public key is used to validate the BS's certificate.

Sequence Number and Node Pair Check: The receiver packet table is consulted in order to verify the sequence number and node pair. The sequence number, packet type, and node pair are saved with the packet for broadcasting again if no matching values are discovered. If not, the packet is thrown away.

Destination ID Check: The pairing key is encrypted, the MAC is checked, and the encrypted neighbor packet is transmitted with a nonce and the destination ID (encrypted using the pairwise key) if the destination ID matches the node's ID. Equation (7) describes this procedure.

$$x \rightarrow y: CHALLENGE|ID_x|E\left((k_{yb}, k_{xy})|E\left(k_{xy}, ID_x|nonce\right)\right) \quad (7)$$

3.3. Cluster Formation

The Base Station (BS) initiates the cluster formation process, and the Cluster Head (CH) is selected based on the residual energy of the nodes. It is assumed that the energy level of each node remains constant after the cluster is formed. Typically, 5–8% of the cluster nodes are chosen as CHs, following these criteria:

Non-Neighboring Cluster Heads: No two CHs should be direct neighbors.

Neighbor Distribution: Each CH should have at least 7–10% of the nodes as its neighbors.

As seen in Figure 2, the BS unicasts a CH Initialization (CH INT) packet to every CH along the path from the CH to the BS after the CHs have been chosen. Equation (9) defines the format of the CH INT packet, taking into account the node as the subsequent hop in the route.

$$BS \rightarrow CH: CH\_INT|ID_{bs}|ID_i|E(K_{ibs}, PATH|seqno)|MAC(k_{chbs}, CH\_INT|\ ID_{ch}|PATH|seq\_no) \quad (9)$$

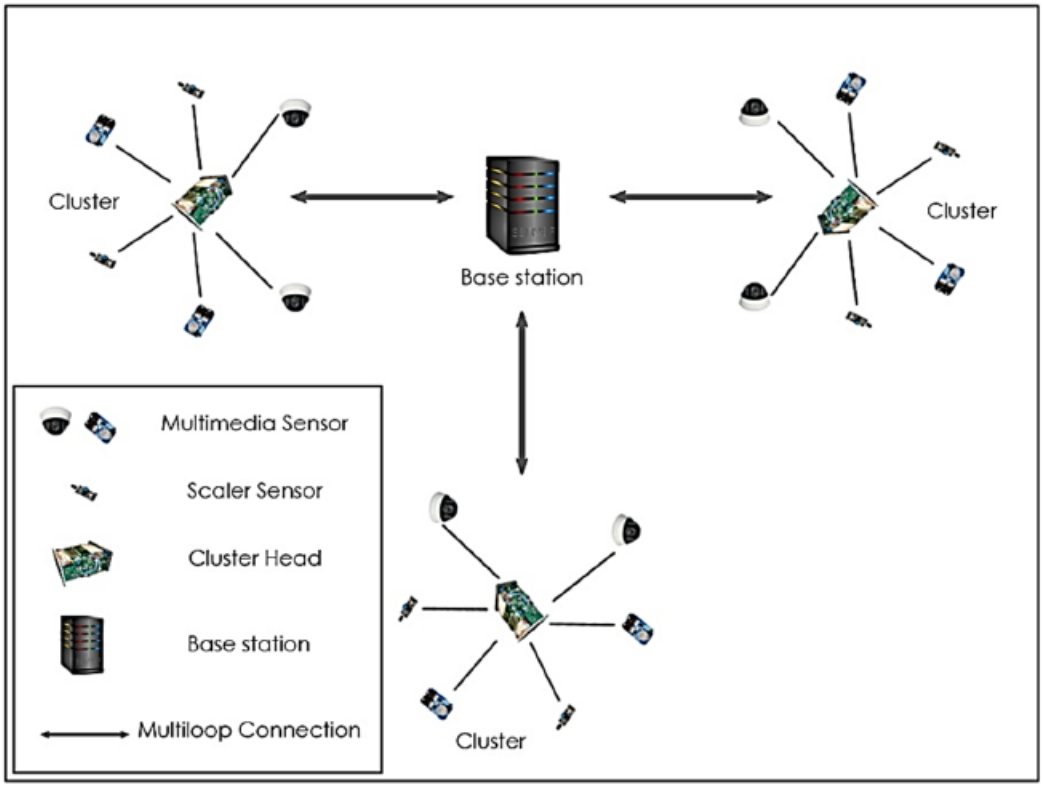

Figure 2. Clustered architecture.

Upon receiving the packet, each node performs several key operations. First, it checks the next hop ID to ensure it matches its own. The next hop is determined and the routing path (PATH) is decrypted if the IDs match; if not, the packet is deleted. Next, the node checks the recipient packet table for the sequence number. The type of packet and sequence number are saved, and the required adjustments are made, if the sequence number is missing. The packet is dropped if the sequence number is already there. The node determines the next hop ID from the PATH and assigns the previous hop ID. In order to guarantee correct data delivery to the Base Station (BS), the routing table is updated and kept in memory. The revised packet is then forwarded once the pairwise key has been used to encrypt the PATH and the sequence path for the subsequent hop. Upon receiving the CH INT packet, the Cluster Head (CH) decrypts the PATH, uses the Message Authentication Code (MAC) to confirm the data, and then uses the same path to send an acknowledgment (ACK) to the BS. The path is recalculated and the CH INT packet is retransmitted if the BS does not get the ACK within a predetermined amount of time.

A number of criteria, including power usage and residual energy, are taken into consideration while choosing the routing plan. The preferable route is the one with fewer hops and a higher residual energy. The CH announces its presence by sending a CH ADV packet, which includes the CH ID and certificate (CERT) for recipient nodes to verify, in order to create a cluster. Two criteria are used by nodes that receive several CH ADV packets to choose the CH.: (1) whether the pairwise key is in existence in the advertised ID, and (2) the signal strength of the forwarded advertisement. Once a CH is chosen, the nodes forward their intent to join the cluster using a CH JOIN packet, which includes their ID, MAC, nonce and a paired key. After receiving all CH JOIN packets, the CH sends the cluster member information to the BS and generates a TDMA schedule based on the number of nodes in the cluster.

This schedule is then unicasted to each member, and the packet format is defined in Equations (10)–(12)..

$$CH \rightarrow *: CH\_ADV|ID_{ch}|CERT_{ch}$$

$$x \rightarrow CH: CH\_JOIN|1D_x|MAC(K_{xch}, CH\_JOIN|1D_x|\ noncex$$

$$CH \rightarrow x: CH\_SHED|ID_x|E(k_{xch}, t_x)MAC(CH_{SCHED|ID_x|E(k_{xch},t_x)noncex} + 1)$$

3.4. Data Transmission

The phase of data transmission consists of three subphases:

1. Data Transmission from Member Node to CH: The data sensed by the member node is encrypted and authenticated before being transmitted to the Cluster Head (CH). If the node is not connected to any active route, it can enter a sleep mode to conserve energy.
2. Data Aggregation and Forwarding by CH: After receiving the data, the CH compiles and compresses it to create a new signal, which is subsequently sent along the specified path to the Base Station (BS). Node J is thought to be the next hop in the routing table.
3. Decryption and Authentication by BS: Upon receiving the data, the Base Station (BS) uses a uniquely shared key to decrypt and authenticate the information.

These subphases are represented in the form provided by Equations (13) and (14).

$$x \rightarrow CH: DATA|1D_x|E(K_{xch}, d_x)$$

$$MAC(K_{xch}, DATA|1D_x|E(K_{xch}, d_x)$$

Following receipt, the Cluster Head (CH) aggregates the data before sending it to the Base Station (BS), as indicated by Equation (15).

$$CH \rightarrow BS: AGGR\_DATA|ID_{ch}|ID_j|E(K_{jch}, seq_{no})|E(K_{chbs}, d_{ch})|MAC$$
$$(K_{chbs}, AGGR\_DATA|seq_{no}|E(K_{chbs}, d_{ch})$$

The AGGR_DATA packet specifies the packet type, with IDch and IDj representing the previous and next hops in the path, respectively. Upon receiving the AGGR_DATA packet, the node verifies the packet reply by checking the encrypted sequence number. If the number of sequences matches the one already recorded, the packet is discarded. Dch represents the encrypted data for the Base Station (BS), along with the Message Authentication Code (MAC), which ensures the integrity and the packet's authenticity.

The node receiving this packet performs the following operations:

1. The next hop ID is checked. If it matches the node's own ID, the sequence number is decrypted.
2. The sequence number is verified packet table of the receiver. When the sequence number is not found, the packet type and sequence number are recorded; otherwise, the packet is discarded.
3. The subsequent hop entry is updated with the next hop node's ID, while the preceding hop's ID is also updated.

4. Using the pairwise key, the sequence number is encrypted of the next hop, and the packet is forwarded again.

In this manner, the data is transmitted through the specified route to the BS, which uses a uniquely shared key (Kchbs) to evaluate the efficiency and authenticity of the received data.

3.5. Incorporation of H-TEEN

In H-TEEN, after selecting the Cluster Heads (CHs), the CHs forward the following parameters:

1. Attributes (A): These are the physical parameters that enable the user to collect relevant data from the network.

2. Thresholds: This consists of two types—Hard Threshold (HT) and Soft Threshold (ST). HT is a specific value that triggers a node to broadcast data, while ST represents a slight variation in data value that prompts the node to rebroadcast the information.

3. Schedule: The schedule is organized using Time Division Multiple Access (TDMA), which allocates specific time slots to each node for data transmission.

4. Time Count (TC): This represents the maximum duration between two consecutive reports sent by a node. It defines the time span within the schedule, considering the practical aspects of transmission. In a Wireless Sensor Network (WSN), neighboring nodes often form a cluster and sense similar data, which can lead to data collisions. To prevent this, the TDMA schedule ensures that each cluster member is assigned its own transmission slot, thus avoiding simultaneous transmissions and reducing collisions.

4o mini

3.6. U-DSP

In a storage system, businesses typically store data on remote servers to ensure data authenticity and integrity. However, when unauthorized users delete or modify data, it can compromise the server, potentially leading to Byzantine failures or other unpredictable errors. To address this, cloud storage systems implement a flexible and effective distributed approach that provides dynamic data support, enabling the distribution of files across cloud servers. This system uses a homomorphic token, computed with a universal hash function, to verify the integrity of erasure-coded data. Additionally, the system is designed to identify misbehaving servers. Finally, procedures for file retrieval and error recovery based on erasure-correcting codes are established to quickly recover from data loss or corruption.

3.7 CH selection

The suggested process and its stages are thoroughly explained in this section. In order to improve network performance, namely in terms of energy consumption, effective data transport, and security, the protocol is made for devices with low constraints. There are two primary stages to the work.

The protocol optimizes decision-making for reliable data routing in the first phase by using a metaheuristic algorithm based on Particle Swarm Optimization (PSO). This heuristic method

minimizes the nodes' memory requirements while intelligently choosing the next hop by taking into account a number of factors, including link integrity.

Ensuring safe and genuine data routing is the main goal of the second stage. It employs a counter-encryption mode that strikes a compromise between randomization and computational simplicity. By executing data encryption and decryption concurrently, the suggested protocol lessens the computational strain on the nodes. Additionally, to lessen the possibility of route failures and to guarantee more consistent energy usage throughout the network, energy-alert and traffic analysis techniques are combined. Figure 1 shows the protocol's phases and architecture.

Particles are created at random in the first stage, and the top points are chosen to serve as cluster heads. After assigning nodes close to each cluster head to the appropriate cluster, a fitness function is computed for each cluster head. A cluster head is replaced if its fitness function outperforms the global best. For a thousand generations, this procedure is repeated. After that, each node prepares a control message that is transmitted straight to the base station and includes its identity and remaining energy. After receiving this data, the base station carries out the clustering process.

In order to produce more cohesive clusters that are farther apart, the clustering is designed for higher intra-cluster density and lower inter-cluster density. This principle is used to determine the ideal number of clusters. The number of clusters is first chosen, and the distance between clusters and the dataset's total center for the specified number of clusters is used to determine the rate of cluster separation. Since compact and well-separated clusters are more preferable for clustering, the ratio between these distances is then computed. Equation 1 shows that the validation index is made up of two components, F1 and F2.

validity = max (F1 + F2) (1)

The better the clustering performance, the higher the value of the aforementioned criterion. The F1 index is represented by equation (2), and the cluster dispersion and node density inside each cluster are depicted in Figure 1:

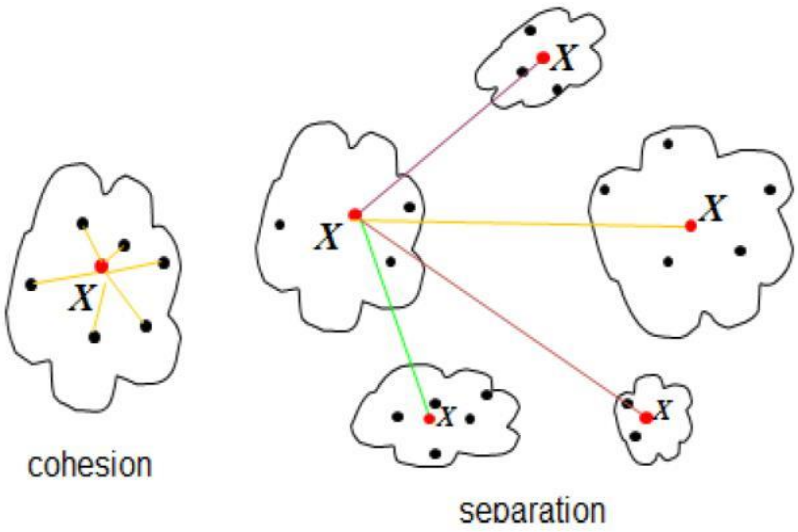

Fig 3. Performance criteria description of the proposed validation index

Eq. (2), (3) denotes the intra and inter cluster separation:

$$i_{intra}(c) = \sum_{i=1}^{c} d \, \Sigma_{j=1}^{N}(X_J - X\iota) \qquad (2)$$

The total distance between each cluster's nodes and the associated cluster head is determined by Equation (3). Here, N is the total number of nodes, Xj is the cluster head, c is the number of clusters, and Xi is the distance between a node and its corresponding cluster head. The following formula represents the intra-cluster separation.

$$\text{Inter(c)} = \sum_{j}^{c}(Xj - X) \qquad (3)$$

The distance between each cluster's center and the dataset's overall center is calculated to determine the inter-cluster separation. After that, a chart is created showing the value of this index for a given cluster range. The ideal number of clusters can be estimated more precisely when the curve's slope is steeper. The best number of clusters can be found by conducting a local search around this steep slope. The calculation of F2 is explained in equation (4).

F2= cluster heads degree+ (2. residual energy) / centrality + distance to base station (4)

Residual Energy: We have quadrupled the coefficient of residual energy because of its substantial influence on cluster heads' efficacy.

Degree of Cluster Head: This is determined by dividing the total number of nodes in the network by the number of inter-cluster nodes.

Additionally, the following formula is used to determine the centrality in the relationship mentioned above:

$$\text{centrality} = \frac{\sqrt{\frac{\Sigma dis^2}{n}}}{100} \qquad (5)$$

In which, $\sum d_{i,s}^2$ is the sum of squared distances of nodes to cluster heads. Every node is presumed to know its location and be able to determine how far away it is from the base station. Each experimental cluster head has a corresponding F2 coefficient, and the sum of the values for all cluster heads. The residual energy of the cluster heads is more significant and influential during the election process than other parameters, which is why the F2 coefficient is used for energy. We have therefore doubled its coefficient.

Without a value coefficient, the F1 formula's validity and importance would be diminished because the F1 score would be significantly lower than the F2 score. To address this, additional coefficients are applied to balance the effects of F1 and F2, creating a more effective and meaningful comparison.

4. Performance Analysis and Discussion

A series of simulated experiments using a randomly changing network topology were used to assess the effectiveness of the secure routing protocol, which integrates data storage with energy optimization. A multi-hop network comprising between 50 and 200 sensor nodes (SNs) and measuring 1000 m by 1000 m was used for the simulations. It was set up in a randomized grid. In the middle of the network was the sink node. Constant Bit Rate (CBR) traffic was produced at a rate of 600 packets per second,

with 316 bytes in each packet. By evaluating the environment with several node configurations, the network's heterogeneity was illustrated. Table 1 provides specifics on the simulation parameters.

Table 1. Simulation parameters.

Parameters	**Value**
Sensor nodes	200
Network Size	1000 m X 1000 m
Number of Nodes	10 to 500
Transmission Rate	50 to 250 Kbps
MAC Protocol	IEEE 802.11
Data Flows	2 to 10
Packet Size	512 bytes
Initial Energy	14.0 Joules
Receiving Power	0.4 Watts

The performance measures evaluated in this study included throughput, end-to-end delay, energy efficiency, network lifetime, and data storage capacity. End-to-end delay, a crucial metric, is particularly important for handling real-time traffic and ensuring that data packets are transmitted within the required time frame. It refers to the total time taken for data to travel from the source node to the sink node. This delay is the cumulative result of transmission delay, propagation delay, queuing delay, and processing delay at each hop along the route.

An end-to-end latency comparison of the suggested protocol against existing protocols such as LEACH, CCBRP, and PEGASIS is shown in Table 2. According to the results, the suggested protocol performs better than the others and has the least amount of delay. This is because the Cluster Heads' (CHs') hierarchical architecture always chooses routes with fewer hops and high-quality links, maximizing the total delay.

Table 2. Comparison of end–end delay.

Network Size	CCBRP	LEACH	NCBPR	PEGASIS	ETLHCM	HHCA	MLRP-HTEEN-UDSP
50	40	42	35	38	28	31	25
75	69	75	59	63	38	48	28
100	72	78	63	67	42	52	32
125	75	81	69	70	48	58	38
150	79	85	76	77	55	65	45

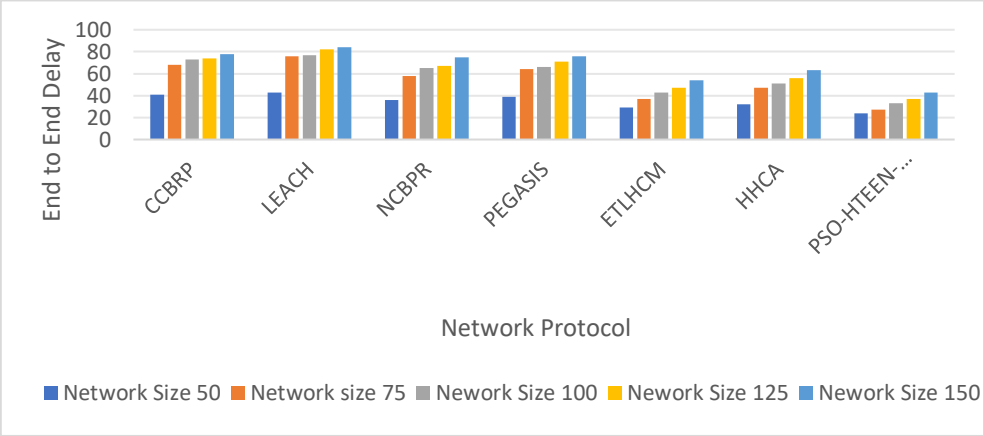

Figure 3: Comparison end to end delay

The total number of packets that the sink successfully receives in a certain amount of time is known as throughput. Table 3 displays the throughput comparison between the suggested protocol and other protocols, emphasizing the variations in performance among the different routing techniques.

Table 3.: Comparison of throughput

Network Size	CCBRP	LEACH	NCBPR	PEGASIS	ETLHCM	HHCA	MLRP-HTEEN-UDSP
50	28	20	35	30	45	40	52
75	36	34	44	40	55	52	61
100	47	43	52	50	65	63	78
125	62	58	69	66	79	74	82
150	68	63	72	70	80	76	85

The suggested protocol's throughput is contrasted with alternative methods in Figure 4. In order to balance the load and make optimum use of the wireless spectrum, several pathways and minimum latency are chosen. As a result, it surpasses other protocols in throughput.

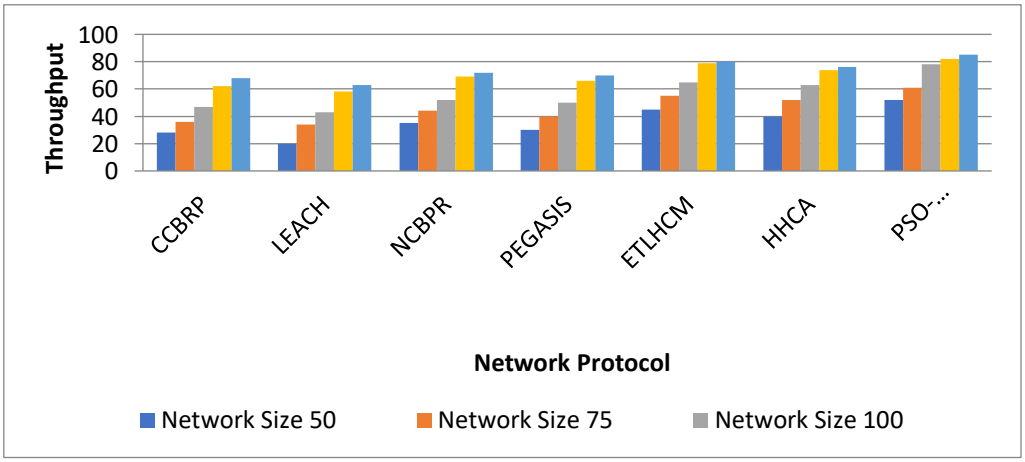

Figure 4: Comparison of throughput

A comparison of the energy efficiency of several methods is shown in Table 4. The average energy efficiency is shown, demonstrating that across different node configurations, the suggested protocol MLRP-HTEENUDSP dissipates less energy than other protocols like LEACH, CCBRP, and PEGASIS.

Table 4. Comparison of Energy Efficiency

Network Size	CCBRP	LEACH	NCBPR	PEGASIS	ETLHCM	HHCA	MLRP-HTEEN-UDSP
50	23	20	28	25	38	32	44
75	38	35	42	40	50	46	51
100	40	38	45	45	58	51	61
125	53	50	50	55	69	63	72
150	58	52	62	60	70	68	75

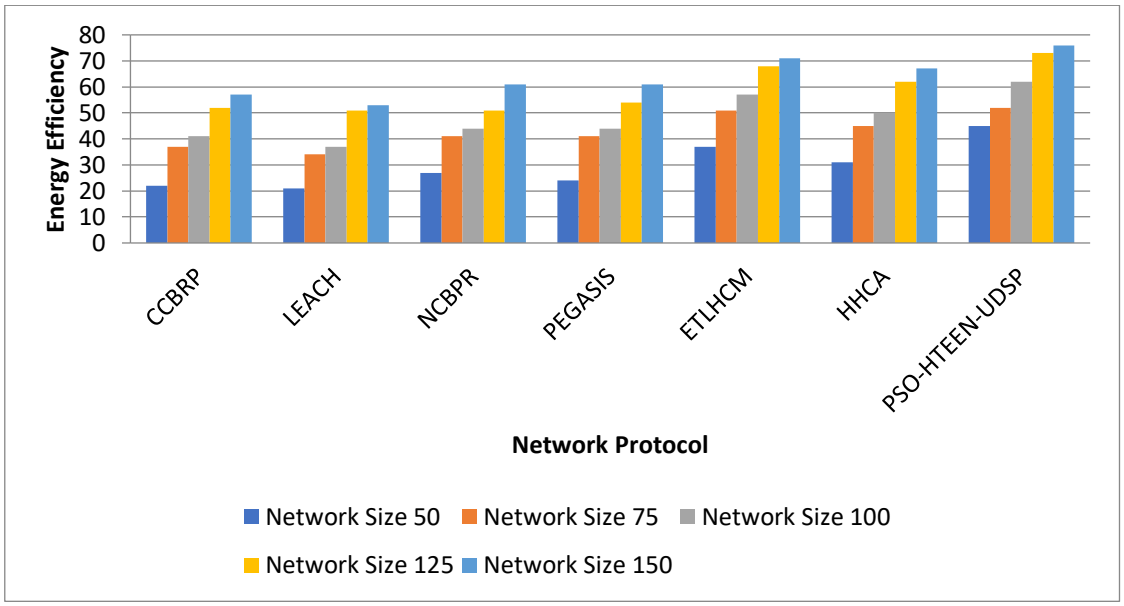

Figure 5. Comparison of energy efficiency.

Table 5. Comparison of network Lifetime.

Network Size	CCBRP	LEACH	NCBPR	PEGASIS	ETLHCM	HHCA	MLRP-HTEEN-UDSP
50	30	28	38	33	50	45	55
75	48	45	55	50	63	59	65

100	51	49	65	56	78	71	81
125	56	50	66	59	82	79	85
150	59	52	72	61	85	80	88

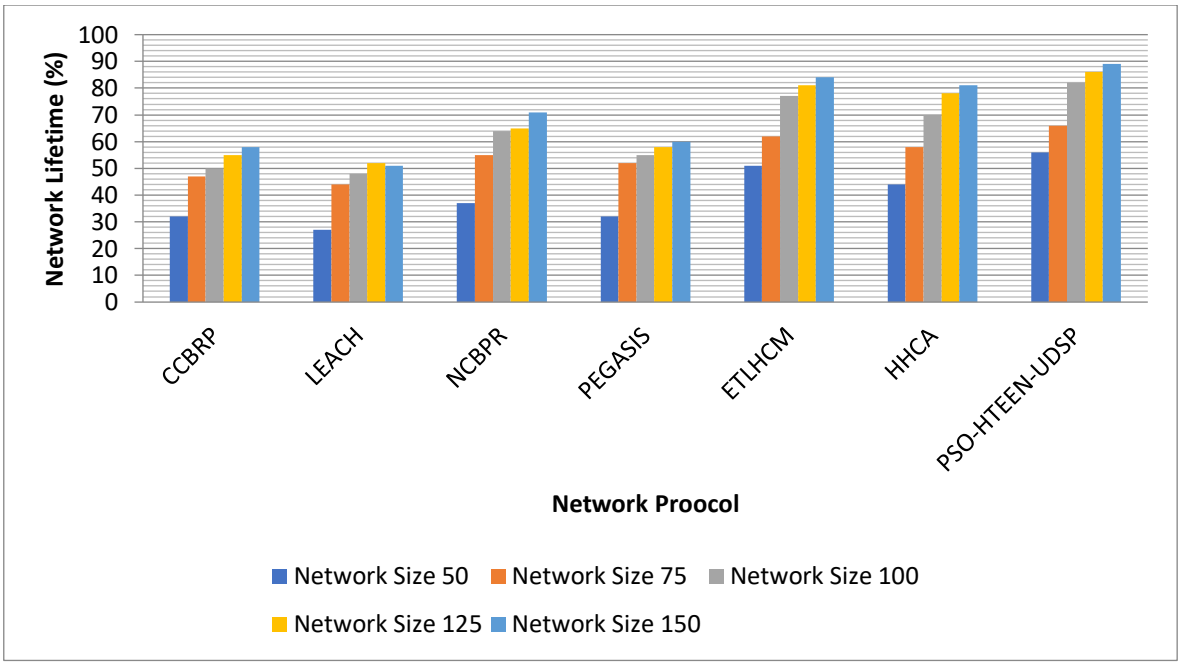

Figure 6. Comparison of network Lifetime.

Table 6 presents a comparison of data storage across different protocols. Figure 12 illustrates the comparison of data storage capacity between the proposed protocol and existing techniques, highlighting the improvements achieved by the proposed approach.

Table 6. Comparison of data storage.

Network Size	CCBRP	LEACH	NCBPR	PEGASIS	ETLHCM	HHCA	MLRP-HTEEN-UDSP
50	23	19	32	28	38	35	42
75	28	22	39	30	45	40	51
100	31	26	42	35	64	59	68
125	35	28	52	37	70	65	72
150	39	31	61	41	72	68	75

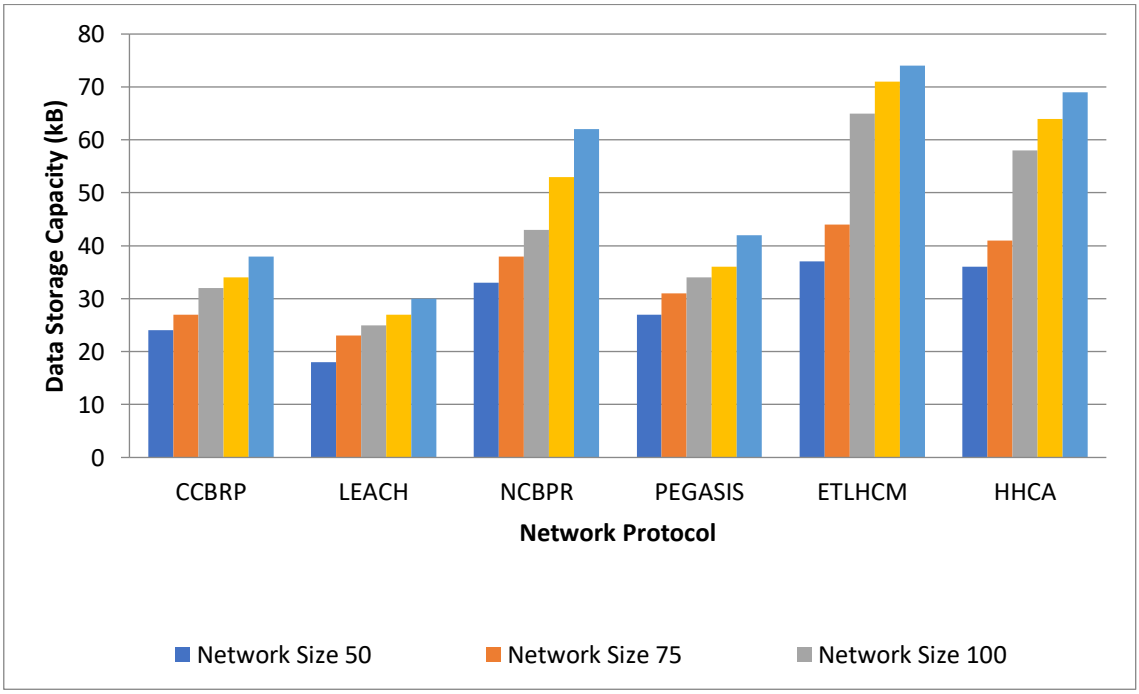

Figure 7. Comparison of data storage.

Table 7 presents a comprehensive comparison of the overall parameters between the proposed protocol and existing techniques. The graphical representation of this comparison is shown, highlighting the performance differences across various metrics.

Table 7: Overall comparison of MLRP-HTEEN-UDSP

Network Size	End to End Delay	Throughput	Energy Efficiency	Data Storage Capacity	Network Lifetime
50	25	52	44	42	55
75	28	61	52	51	65
100	32	78	61	68	81
125	38	82	72	72	85
150	45	85	75	75	88

5. Conclusion:

For IoT-based heterogeneous WSN applications, this study suggests an energy optimization technique with safe routing. At the Base Station (BS), the dependable and secure routing protocol gathers information about nearby nodes, produces keys, and builds energy-efficient multipaths for every node. Cluster Heads (CHs) help aggregate data and send it to the base station (BS), which keeps an eye on nodes' remaining energy to choose new pathways and CHs. The integrated implementation of MLRP-HTEEN-UDSP minimizes end-to-end delay for data packets and lowers energy usage at sensor nodes

(SNs) by utilizing the intricacy of processing multimedia and the process of aggregate at the CH side, while also avoiding path loops and cycles during route establishment. Additionally, a lightweight distributed key management method is introduced to support secure communication among the nodes. The performance of MLRP-HTEEN-UDSP outperforms existing protocols such as LEACH, CCBRP, and PEGASIS across all performance metrics, including end-to-end delay, throughput, energy efficiency, network lifetime, and data storage capacity. Future work will expand on the proposed protocol, focusing on performance analysis in green IoT environments with larger network sizes.

References:

[1] 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.

[2] 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 9,477,865 B2, 26 October 2016.

[3] Pirbhulal, S.; Zhang, H.; Alahi, M.E.; Ghayvat, H.; Mukhopadhyay, S.C.; Zhang, Y.-T.;Wu,W. A Novel Secure IoT-Based Smart Home Automation System Using aWireless Sensor Network. Sensors 2017, 17, 69. [CrossRef]

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

[5] 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]

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

[7] 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]

[8] 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]

[9] 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]

[10] Haseeb, K.; Islam, N.; Almogren, A.; Din, I.U. Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things. IEEE Access 2019, 7, 185496–185505. [CrossRef]

[11] Kumar, K.; Kumar, S.; Kaiwartya, O.; Cao, Y.; Lloret, J.; Aslam, N. Cross-Layer Energy Optimization for IoT Environments: Technical Advances and Opportunities. Energies 2017, 10, 2073. [CrossRef]

[12] Minoli, D.; Sohraby, K.; Occhiogrosso, B. IoT Considerations, Requirements, and Architectures for Smart Buildings—Energy Optimization and Next-Generation Building Management Systems. IEEE Internet Things J. 2017, 4, 269–283. [CrossRef]

[13] Guo, X.; Lin, H.; Li, Z.; Peng, M. Deep-Reinforcement-Learning-Based QoS-Aware Secure Routing for SDN-IoT. IEEE Internet ThingsJ. 2020, 7, 6242–6251. [CrossRef]

[14] Pirbhulal, S.; Wu, W.; Muhammad, K.; Mehmood, I.; Li, G.; de Albuquerque, V.H.C. Mobility enabled security for optimizing IoT based intelligent applications. IEEE Netw. 2020, 34, 72–77. [CrossRef]
[15] Haseeb, K.; Almogren, A.; Islam, N.; Ud Din, I.; Jan, Z. An Energy-Efficient and Secure Routing Protocol for Intrusion Avoidance in IoT-Based WSN. Energies 2019, 12, 4174. [CrossRef]
[16] Preeth, S.K.; Dhanalakshmi, R.; Kumar, R.; Shakeel, P.M. An adaptive fuzzy rule based energy efficient clustering and immuneinspired routing protocol for WSN-assisted IoT system. J. Ambient. Intell. Humaniz. Comput. 2018. [CrossRef]
[17] Hammi, B.; Zeadally, S.; Labiod, H.; Khatoun, R.; Begriche, Y.; Khoukhi, L. A secure multipath reactive protocol for routing in IoT and HANETs. Ad Hoc Netw. 2020, 103, 102118. [CrossRef]
[18] Sampathkumar, A.; Maheswar, R.; Harshavardhanan, P.; Murugan, S.; Jayarajan, P.; Sivasankaran, V. Majority Voting based Hybrid Ensemble Classification Approach for Predicting Parking Availability in Smart City based on IoT. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020.
[19] Sampathkumar, A.; Murugan, S.; Rastogi, R.; Mishra, M.K.; Malathy, S.; Manikandan, R. Energy Efficient ACPI and JEHDO Mechanism for IoT Device Energy Management in Healthcare. In Internet of Things in Smart Technologies for Sustainable Urban Development; Springer: Cham, Switzerland, 2020; pp. 131–140.
[20] 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. [CrossRef]
[21] Sharma, S.; Rani, M.; Goyal, S.B. Energy Efficient Data Dissemination with ATIM Window and Dynamic Sink in Wireless Sensor Networks. In Proceedings of the 2009 International Conference on Advances in Recent Technologies in Communication and Computing, Kottayam, India, 27–28 October 2009; pp. 559–564. [CrossRef]
[22] Maheswar, R.; Jayarajan, P.; Sampathkumar, A.; Kanagachidambaresan, G.R.; Hindia, M.H.D.; Tilwari, V.; Dimyati, K.; Ojukwu,
[23] H.; Sadegh Amiri, I. CBPR: A Cluster-Based Backpressure Routing for the Internet of Things. Wirel. Pers. Commun. 2021, 118, 3167–3185. [CrossRef]
[24] Raut, R.; Kautish, S.; Polkowski, Z.; Kumar, A.; Liu, C.M. Energy-Efficient Routing Protocol for Green IoT Network, Green Internet of Things and Machine Learning: Towards a Smart Sustainable World; John Wiley & Sons: Hoboken, NJ, USA, 2021; ISBN 9781119792031. [CrossRef]
[25] Kanagachidambaresan, G.R.; Maheswar, R.; Manikantan, C.; Ramakrishnan, K. Internet of Things in Smart Technologies for Sustainable Urban Development, 1st ed.; EAI/Springer Innovations in Communications and Computing Book Series; Springer: Cham, Switzerland, 2020.
[26] Sharma, S.; Goyal, S.B.; Qamar, S. Four-Layer Architecture Model for Energy Conservation in Wireless Sensor Networks. In Proceedings of the 2009 Fourth International Conference on Embedded and Multimedia Computing, Jeju, Korea, 10–12 December 2009; pp. 1–3. [CrossRef]

[27] Rajawat, A.S.; Bedi, P.; Goyal, S.B.; Alharbi, A.R.; Aljaedi, A.; Jamal, S.S.; Shukla, P.K. Fog Big Data Analysis for IoT Sensor Application Using Fusion Deep Learning. Math. Probl. Eng. 2021, 2021, 6876688. [CrossRef]

[28] Rani, S.; Maheswar, R.; Kanagachidambaresan, G.R.; Jayarajan, P. Integration of WSN and IoT for Smart Cities, 1st ed.; EAI/Springer Innovations in Communications and Computing Book Series; Springer: Cham, Switzerland, 2020.

[29] Khan, M.; Ilavendhan, A.; Babu, C.N.K.; Jain, V.; Goyal, S.B.; Verma, C.; Safirescu, C.O.; Mihaltan, T.C. Clustering Based Optimal Cluster Head Selection Using Bio-Inspired Neural Network in Energy Optimization of 6LowPAN. Energies 2022, 15, 4528. [CrossRef]

[30] Goyal, S.B.; Bedi, P.; Kumar, J.; Varadarajan, V. Deep learning application for sensing available spectrum for cognitive radio: An ECRNN approach. Peer-to-Peer Netw. Appl. 2021, 14, 3235–3249. [CrossRef]

[31] Rajawat, A.S.; Bedi, P.; Goyal, S.B.; Shukla, P.K.; Jamal, S.S.; Alharbi, A.R.; Aljaedi, A. Securing 5G-IoT Device Connectivity and Coverage Using Boltzmann Machine Keys Generation. Math. Probl. Eng. 2021, 2021, 2330049. [CrossRef]

[32] 31 Anurag et. al., “Load Forecasting by using ANFIS”, International Journal of Research and Development in Applied Science and Engineering, Volume 20, Issue 1, 2020

[33] Raghawend, Anurag, "Detect Skin Defects by Modern Image Segmentation Approach, Volume 20, Issue 1, 2020