

Article

Secure Routing-Based Energy Optimization for IoT Application with Heterogeneous Wireless Sensor Networks

Nagaraju Regonda ¹, Venkatesan C ², Kalaivani J ³, Manju G ⁴, S. B. Goyal ^{5,*}, Chaman Verma ⁶,
Calin Ovidiu Safirescu ^{7,*} and Traian Candin Mihaltan ⁸

¹ Department of Information Technology, St. Martin's Engineering College, Dhulapally, Secunderabad 500014, India; nagarajuit@smec.ac.in

² Department of Electronics and Communication Engineering, HKBK College of Engineering, Bengaluru 560045, India; venkatesanc.ec@hkbk.edu.in

³ Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Cheenai 603203, India; kalaivaj@srmist.edu.in

⁴ Department of CSE, SRM Institute of Science and Technology, Kattankulathur, Cheenai 603203, India; manju.shruthi@gmail.com

⁵ Faculty of Information Technology, City University, Petaling Jaya 46100, Malaysia

⁶ Department of Media and Educational Informatics, Faculty of Informatics, Eotvos Lorand University, 1053 Budapest, Hungary; chaman@inf.elte.hu

⁷ Environment Protection Department, Faculty of Agriculture, University of Agriculture Sciences and Veterinary Medicine Cluj-Napoca, Calea Manastur No. 3–5, 40033 Cluj-Napoca, Romania

⁸ Faculty of Building Services, Technical University of Cluj-Napoca, 40033 Cluj-Napoca, Romania; mihaltantraian83@gmail.com

* Correspondence: sb.goyal@city.edu.my (S.B.G.); calin.safirescu@usamvcluj.ro (C.O.S.)



Citation: Regonda, N.; C, V.; J, K.; G, M.; Goyal, S.B.; Verma, C.; Safirescu, C.O.; Mihaltan, T.C. Secure Routing-Based Energy Optimization for IoT Application with Heterogeneous Wireless Sensor Networks. *Energies* **2022**, *15*, 4777. <https://doi.org/10.3390/en15134777>

Academic Editor: Jose A. Afonso

Received: 29 May 2022

Accepted: 27 June 2022

Published: 29 June 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



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/>).

Abstract: Wireless sensor networks (WSNs) and the Internet of Things (IoT) are increasingly making an impact in a wide range of domain-specific applications. In IoT-integrated WSNs, nodes generally function with limited battery units and, hence, energy efficiency is considered as the main design challenge. For homogeneous WSNs, several routing techniques based on clusters are available, but only a few of them are focused on energy-efficient heterogeneous WSNs (HWSNs). However, security provisioning in end-to-end communication is the main design challenge in HWSNs. This research work presents an energy optimizing secure routing scheme for IoT application in heterogeneous WSNs. In our proposed scheme, secure routing is established for confidential data of the IoT through sensor nodes with heterogeneous energy using the multipath link routing protocol (MLRP). After establishing the secure routing, the energy and network lifetime is improved using the hybrid-based TEEN (H-TEEN) protocol, which also has load balancing capacity. Furthermore, the data storage capacity is improved using the ubiquitous data storage protocol (U-DSP). This routing protocol has been implemented and compared with two other existing routing protocols, and it shows an improvement in performance parameters such as throughput, energy efficiency, end-to-end delay, network lifetime and data storage capacity.

Keywords: WSNs; IoT; heterogeneous WSN; multipath link routing protocol (MLRP); hybrid-based TEEN; ubiquitous data storage protocol (U-DSP)

1. Introduction

The IoT and WSNs are becoming viable solutions that are widely utilized in real-time data collection and monitoring applications, which include automated irrigation, target monitoring, observing clinical records, tracking landslides and predictions for forest fire and disaster management. A WSN consists of numerous effective sensor nodes (SNs) that monitor climatic disasters found in harsh or remote areas. Furthermore, the SNs examine the atmospheric factors such as pressure, temperature, humidity, sound and moisture content representing intense symptoms. After an SN completes its sensing operation, the

information is gathered and transmitted to the base station (BS). The sensor and data communication units of SNs consume more energy and once the entire energy is exhausted, it expires or is unable to process [1]. Hence, a node that is considered dead is unsuitable for either replacing with or recharging using an alternate power source. Hence, balancing the power utilization of a SN is more essential. To overcome these challenges, several developers have used clustering approaches [2], which can scale up the network lifetime and provide remarkable efficiency. Furthermore, it is supportive in maintaining power as numerous reliable clusters are formed. These clusters, based on the techniques used, can either be considered temporary or permanent. Moreover, clustering distributes the nodes that are placed jointly, which is accomplished based on similarity metrics such as the distance from the base station (BS), radius of transmission and density of the cluster. After the clusters are formed, a node from the cluster is chosen as the cluster head (CH) whose responsibility is to organize the data gathered from cluster members (CM) and transmit those data to the BS. When a single node cluster is considered, it mandatorily communicates with the sink rather than the BS, which finally results in a reduction in power utilization. In WSNs, the serious threats, along with the technical challenges, which arise due to the nature of resource constraints and its limited availability [3], have to be focused on to ensure revision and distribution. With WSNs in an open area, the sensors are more vulnerable to the unfriendly environment that arises due to humidity, increased temperature, pressure, snow, rain, dust and so on. These affect the functions of the wireless sensor network, and hence a demand arises to introduce robust and flexible SNs. Moreover, general and future challenges are constrained to the limited resources, the limited ability of communication, fault tolerance, stability, mobility, bandwidth, precision, reliability, availability, heterogeneity, accountability, uncontrollable setup and denial of service (DoS). Above all, some specific challenges have turned the attention of the researchers towards the utilization of power, network duration, throughput, security and routing protocols. In WSNs, during communication, energy consumption is a highly prominent issue that seeks attention. Energy efficiency has a greater impact on the entire performance of the network and acts as a significant function in the lifespan of a WSN [4]. The metrics that are essential while routing and estimating the cost function (CF) in a WSN are total energy, energy consumed and residual energy. Energy is one of the most significant aspects of the efficient working of wireless sensor networks. The longevity of the network is totally dependent upon the optimum use of the available energy; therefore, optimization is much needed for the efficient utilization of energy. Routing protocol, considered as an important factor, has to be selected carefully to route the data packets safely to the destination with less overhead because of the resource constraints of SNs, namely, their limited power and shorter range for communication. Numerous efforts have been made to bring out the best solutions for WSNs, yet extraordinary works are required [5]. The benefits of the IoT are as follows. An urban IoT has many facilities that may bring a number of benefits such as the management and optimization of traditional public services, including transport and parking facilities, lighting, the surveillance and maintenance of public areas, preservation of cultural heritage, garbage collection, public health care, i.e., hospitals, and schools. Therefore, the availability of different types of data that will store in the cloud or be collected by a data warehouse in the urban IoT should increase the transparency and promote the actions of the local government or municipality towards the citizens, which can increase the awareness of people about the status of their city and their life style. Therefore, the application of the IoT paradigm to the smart city is attractive and expansive for local government and administrations; however, it takes times to adopt IoT technology in a wide manner.

This research is organized as follows: A detailed review of the literature related to this research is described in Section 2. The design, algorithms and functionality of the proposed protocol are elaborated on in Section 3. The simulation results of the proposed protocol are presented in Section 4, which is followed by the conclusion in Section 5.

2. Related Works

Mostly, in large scale networks such as the IoT and SNs with restricted constraints, the demanding factor is energy conservation. Generally, in networks based on clusters [6], the controlling entity is CH, whose significant role is to gather data and transmit them. Furthermore, in large scale WSNs integrated with the IoT, the crucial part is to route data securely as they involve constrained resources. Several existing approaches do not provide reliable and secure data routing in the network as they lack protection schema against threats [7]. A low-energy adaptive clustering hierarchy (LEACH) protocol consists of multi-stages [8]. The LEACH protocol's performance was improved by applying a multi-hop basis for transmitting information [9]. The design elucidated the unstable consumption of energy as the clusters were randomly created. Moreover, the multi-hop paths created were not optimized, which resulted in route breaks. In a chain-chain-based routing protocol (CCBRP) [10], the principles of LEACH as well as Power-Efficient Gathering in Sensor Information Systems (PEGASIS) were integrated, which resulted in scalable energy conservation in SNs while forwarding data. This hybrid CCBRP protocol, which was executed in two stages, reflected the drawback of a higher energy consumption in the nodes and the production of high latency. Subsequently, as the scalability is restricted, CCBRP was not suitable for larger networks. Kumar et al., proposed a data collection as well as a load balancing scheme that was designed to save energy. The network performance was improved in this scheme as the aggregating data were sequenced by data forwarding [11]. A vigorous authentication protocol for energy efficiency was developed for an industrial IoT-based WSN, which provided scalable data security. In this method, mutual authentication was followed between nodes, but the energy was consumed gratuitously, thereby compromising the network lifetime [12]. Likewise, the Shamir secret sharing method comprised two phases, namely, share generation as well as reconstruction. The generated secret was distributed among nodes and the secret key was reconstructed by the usage of any nodes of the subset. The data transmission using this method consumed additional energy leading to routing overheads [13]. If the flow entry exists, the forwarding is performed according to the flow table, and if not, the packet-in message is sent to the subset. After receiving the packet-in message, the subset will make a decision. An improved three-layer hybrid clustering method (ETL-HCM) analysed and limited the control traffic specifically while selecting CH. This method achieved an 18% improvement in the lifetime of the network as well as half of the nodes being alive compared with the hybrid hierarchical clustering approach (HHCA). However, this method was not suitable for selecting the grid head (GH) [14]. To beat hateful attacks such as Sybil, wormholes and a black hole, a novel protocol was introduced by Haseeb et al. to ensure reliable routing and data transmission [15]. The functioning of a combined GIN with GEAR protocol resulted in being too complicated to achieve data security [16]. A voting-based hybrid ensemble classification method was introduced for predicting the availability of parking lots, wherein 96% of the accuracy and 89% of the availability rate was achieved [17]. An optimal network coding backpressure routing (NCBPR) method was developed for a large-scale IoT to divert the flow of data packets from highly congested nodes to low ones, thereby balancing the load and optimizing the battery power [18]. The nodes in the network were formed as clusters and the CHs were selected based on the battery power. Moreover, an efficient data aggregation model was involved to improve the network throughput, wherein the redundant data packets were eliminated. An efficient load balancing optimization algorithm for the employment of energy effectual routing as well as a load balancing protocol were used to enhance the network lifetime [19,20]. The authors in [21] explored the cluster-based backpressure routing algorithm for IoTs, which discusses the energy and congestion issues in IoT environment. A brief discussion is also presented related to the sustainable development through the Internet of Things in [22,23].

A novel framework was proposed to handle environmental monitoring using wireless sensors connected with the internet, wherein two distinctive SNs were involved. Moreover, clients observed the information using the web application on the internet from anywhere. When the information of the SN surpassed the specified range, a notification was sent to the

clients insisting on the environmental setup being altered accordingly [24–26]. Energy is a critical issue in WSNs and the IoT, specifically when deployed in smart city applications and this was discussed briefly in [27–30].

Research Objectives

1. To establish secure routing for confidential data of the IoT through sensor nodes with heterogeneous energy utilizing MLRP.
2. To optimize the energy and improve the network lifetime using a hybrid-based TEEN (H-TEEN) protocol that has load balancing capacity.
3. To improve the storage capacity using the ubiquitous data storage protocol (U-DSP).

3. Proposed Methodology

The proposed routing protocol with a storage capacity protocol has been discussed in three phases. The first phase implements data routing with the security of the sensor nodes for confidential data through the IoT, which has heterogeneous energy using a multipath link routing protocol (MLRP). The next phase is to incorporate the H-TEEN protocol, which has load balancing capacity for sensor nodes that helps in attaining the energy optimization of nodes. Then the transmission of data is carried out using the security and optimization of energy. Finally, the data are stored with improved capacity using the ubiquitous data storage protocol (U-DSP). The architecture is given in Figure 1.

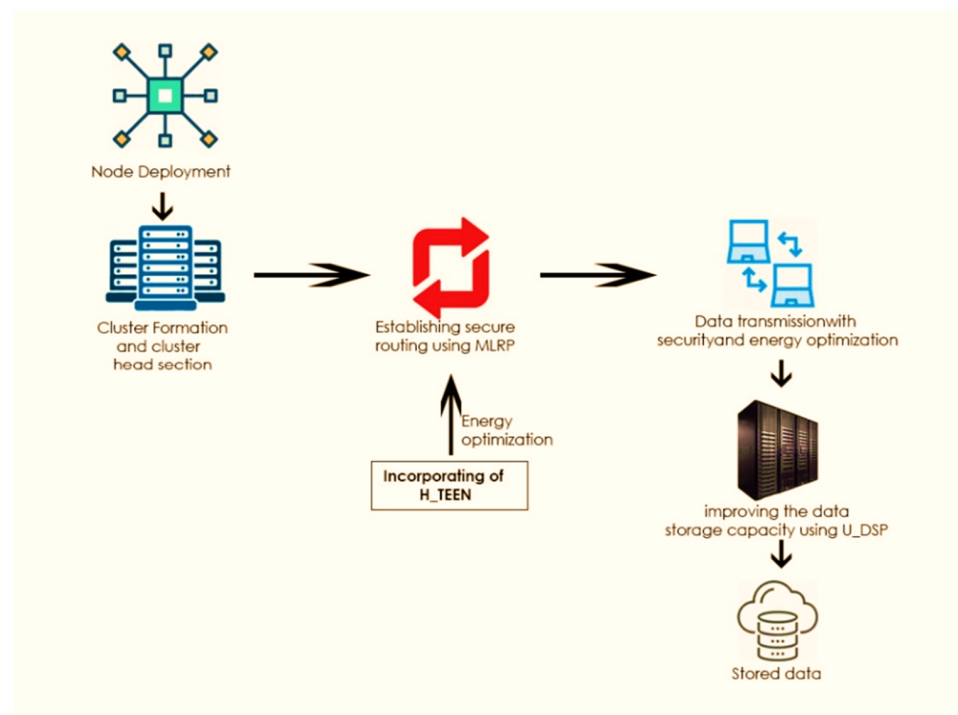


Figure 1. Proposed architecture.

3.1. Multipath Link Routing Protocol (MLRP)

MLRP comprises five various stages, namely, detecting neighbors, constructing topology, distributing pairwise keys, forming a cluster and transmitting data. Every process is described in detail below.

Detection of neighbors and construction of topology: It is considered that every node holds an ID $\{ID_x\}$, certificate $\{CERT_x\}$, public key $\{K_{bs}\}$ and unique shared key $\{K_{xbs}\}$. To identify the neighbors, node broadcasts and receives NBR DET packet containing its ID as well as its CERT as in Equation (1).

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

The node receiving the NBR_DET packet initially authenticates the ID of the node by verifying $CERT_x$. When authenticated, the ID is added to the neighbor list by the receiver, or else the packet is dropped such that the unauthenticated node does not participate in this process of detecting neighbors. Once broadcasting is complete, neighbor information is forwarded to BS as in Equations (2) and (3).

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

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

An intermediate node that is receiving the NBR_INFO packet performs few functions such as:

1. The authentication of the SN is verified by its certificate.
2. When the ID of the node is authorized, the packet is again broadcasted by the receiver node.
3. When the receiver receives a similar packet having a similar ID again, the packet is simply dropped.

Hence, a table is maintained by every node termed as a receiver packet table. Thus, the network traffic is reduced and node energy is saved to some extent. Once the NBR_INFO packet is reached at BS, BS verifies MAC for authenticity and integrity; then neighbor information is authenticated using K_{xbs} between SN and BS. MAC, obtained from the data and by encrypting K_{xbs} , is used such that the intruder cannot either alter or spoof neighbor information.

3.2. Distribution of Pairwise Key

Once the information about the neighbor is obtained from the network nodes, BS analyzes the exact network topology and generates the neighbor matrix. Then the DFS algorithm is applied by which multiple paths are identified from BS to each source node. Beforehand, for each neighbor pair, BS generates the secret key, a random number, termed as pairwise key with the help of the hash function given by Equations (4)–(6).

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

BS unicasts this key to the corresponding node as

$$BS \rightarrow x : PAIR_KEY|seq_{no}|ID_{bs}|CERT_{bs}|ID_x|ID_y|E(k_{xbs}, k_{xy})|E(k_{ybs}, k_{xy}))| \quad (5)$$

$$MAC(k_{xbs}, PAIR_KEY|seq_{no}|ID_{bs}|CERT_{bs}|ID_x|ID_y|E(k_{xbs}, k_{xy})|E(k_{ybs}, k_{xy}))) \quad (6)$$

The packet holds its type, sequence number, the ID of BS, neighbor and destination, certificate of BS, pairwise key and MAC of entire data. Every intermediate node that receives the packet performs the following operations:

- (1) The certificate of BS is verified with the public key.
- (2) The sequence number as well as the node pair is checked in the receiver packet table. When no such value is found, sequence number, type of the packet and node pair along with packet rebroadcasting is stored or else dropped.
- (3) When the ID of the destination is identical to its ID, the pairwise key is encrypted, MAC is verified and the encrypted packet of neighbor with nonce as well as its ID encrypted using a pairwise key is sent, which is given by Equation (7).

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

The packet at node y is decrypted using unique shared key K_{yb} and the pairwise key is generated followed by decrypting the next packet using the generated pairwise key then forwards the packet to x , which is given by Equation (8).

$$y \rightarrow x : CHALLENGE_REP | ID_x | E(k_{xy}, ID_y | nonce_1) \quad (8)$$

Both the neighboring nodes verify one another by swapping the challenge packet as well as reducing overhead of resending pairwise key to y from BS. In end, each pair of nodes holds a pairwise key. When the CHALLENGE_REP packet is not received at node x in the expected form, node x reports about the fake node to BS.

3.3. Cluster Formation

BS initiates cluster formation and cluster head (CH) is selected based on residual energy. It is assumed that the energy level of the node does not change after the cluster is formed. In total, 5–8% of the cluster nodes are selected as CH with the criteria given below: (1) Two cluster heads should not be neighbors; (2) every CH has not less than 7–10% nodes as a neighbor. Then BS unicasts CH INT to CH along the route from CH to BS as illustrated in Figure 2. By considering that the node is next hop in route, the format of the packet CH INT is given by Equation (9).

$$BS \rightarrow CH : CH_INT | ID_{bs} | ID_i | E(K_{ibs}, PATH | seq_{no}) | MAC(k_{chbs}, CH_INT | ID_{ch} | PATH | seq_{no}) \quad (9)$$

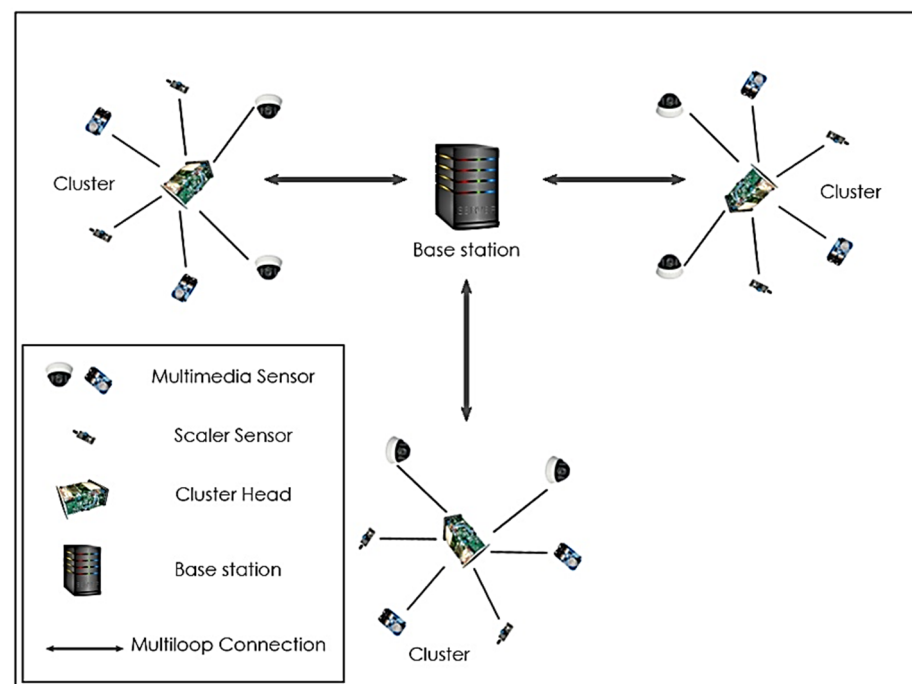


Figure 2. Clustered architecture.

Every node that receives the packet performs the following: (1) ID of the next hop is checked, if identical to its own, routing path (PATH) is decrypted and next hop from PATH is identified or else packet is dropped. (2) The sequence number is checked in the receiver packet table, then store packet type and sequence number if the sequence number did not exist in the table, and the changes needed are made, or else it is stopped. (3) Preceding hop is assigned its ID, while the subsequent one with the ID is found in PATH. (4) Routing table is stored in memory along with the previous one, as well as next hop, such that it helps in transmitting the data to BS. (5) PATH, as well as the sequence path for the subsequent hop, are encrypted with a pairwise key and the updated packet is forwarded. While CH is

receiving the CH INT packet, decryption of PATH takes place and the data are verified by the MAC; then acknowledgement (ACK) is sent to BS via the same path.

When ACK is not received by BS within certain time from CH, the path is recomputed and the CH INT packet is sent again. A few criteria are involved in determining the routing path including the path having residual energy and power consumed. A path is selected with more residual energy and small hops count. To form a cluster, a CH ADV packet is sent by CHs to publicize their will.

ID and CERT are present in CH and the ADV packet, such that the receiving node ensures authentication. Nodes receiving several CH and ADV select CH based on two factors: (1) checking if the pairwise key is present in the ID advertised and (2) signal strength of advertisement forwarded. Once CH is selected, the will of the nodes is forwarded by CH JOIN packet with ID as well as MAC with pairwise key and a nonce. Once entire CH JOIN is received, information of the cluster members is sent to the BS by CH, and the TDMA schedule is created based on the total nodes in the cluster and unicast to every member. The packet has the following format by Equations (10)–(12).

$$CH \rightarrow * : CH_ADV | ID_{ch} | CERT_{ch} \quad (10)$$

$$x \rightarrow CH : CH_JOIN | ID_x | MAC(K_{xch}, CH_JOIN | ID_x | nonce_x) \quad (11)$$

$$CH \rightarrow x : CH_SHED | ID_x | E(k_{xch}, t_x) MAC(CH_SHED | ID_x | E(K_{xch}, t_x) nonce_x + 1) \quad (12)$$

3.4. Data Transmission

The data transmission phase comprises three subphases;

- (1) The data sensed with encrypted and authenticated format transmitted by the member node to CH and when not linked to any route, can sleep so that energy is saved.
- (2) The received data are aggregated and compressed by CH to generate a new signal, which is then transmitted to BS through the route specified. (It is considered that node j is subsequent hop in routing table.)
- (3) Base station uses an exclusively shared key for decryption and authentication of the data received.

These subphases are observed with the form as given in Equations (13) and (14).

$$x \rightarrow CH : DATA | ID_x | E(K_{xch}, d_x) \quad (13)$$

$$MAC(K_{xch}, DATA | ID_x | E(K_{xch}, d_x)) \quad (14)$$

Once the data are received, they are aggregated by CH and then forwarded to BS by Equation (15).

$$CH \rightarrow BS : AGGR_DATA | ID_{ch} | ID_j | E(K_{jch}, seq_{no}) | E(K_{chbs}, d_{ch}) | MAC(K_{chbs}, AGGR_DATA | seq_{no} | E(K_{chbs}, d_{ch})) \quad (15)$$

AGGR_DATA specifies the type of the packet, ID_{ch} and ID_j denote the previous and next hop in the path, respectively; the packet reply is verified with the encrypted sequence number when AGGR_DATA packet is received by any node with identical sequence number, then packet is dropped. D_{ch} represents encrypted data for BS and MAC, which supports maintenance of the packet integrity and authentication. The following operations are performed by the node receiving this packet: (1) ID of the next hop is checked; when similar to its ID, the sequence number is decrypted. (2) The packet sequence number is verified in the receiver packet table, if not found, packet type and the sequence number is entered or else left out. (3) The entry of the subsequent hop is modified with the ID of the subsequent hop nodes and that of the preceding hops with its ID. (4) The sequence number is encrypted using the pairwise key of subsequent hop as well as then forwarded again. In this manner, data reach the BS through the route specified and BS uses an exclusively shared key (K_{chbs}), which evaluates the data efficiency.

3.5. Incorporation of H-TEEN

In H-TEEN, after selecting the CHs, CHs forwards the following parameters:

1. Attributes (A): This physical set of parameters helps the user to collect the data.
2. Thresholds: This is composed of hard and soft thresholds denoted by HT and ST, respectively. HT is the particular value that triggers the node to broadcast the data. ST is a little alteration in the significance that triggers the node to rebroadcast the information.
3. Schedule: It is scheduled by TDMA that allows the slot to each node.
4. TimeCount (TC): This is the utmost duration of the pair consecutive reports forwarded by a node. This is the numerous length of the schedule that accounts for the practical component. In a WSN, closer nodes form a cluster that senses analogous data and forwards them concurrently, which leads to collisions. TDMA schedule is introduced so that every cluster member is assigned a slot for transmission.

3.6. U-DSP

In a storage system, businesses store data in the data server located remotely, and hence data authenticity is assured. When, occasionally, unauthorized users delete or modify data, the server is compromised and/or randomly leads to Byzantine failures. As this is the initial process for recovering the storage errors quickly, cloud storage systems introduce a flexible as well as effective distributed approach with explicit dynamic data support for distribution of files in a cloud server. The homomorphic token is computed with the help of a universal hash function and is integrated with verification of erasure-coded data. Moreover, servers that misbehave are also identified. At last, file retrieving and error recovering procedures based on erasure-correcting code are defined.

4. Performance Analysis and Discussion

The efficiency of the secure routing protocol with energy optimization and data storage was evaluated with several simulation experiments with randomly varying topology. NS-2 version 2.34 was the simulation tool used and considered a multi-hop network with $1000\text{ m} \times 1000\text{ m}$ size located in a randomized grid with SNs from 50 to 200. The sink node was at the centre of the network. Traffic was CBR of 600 packets/sec and packet size was 316 bytes. The heterogeneity of the network was proven in the simulation by testing the environment with different sets of nodes. The simulation parameters are shown in Table 1.

Table 1. Simulation parameters.

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

The performance measures considered were throughput, end-to-end delay, energy efficiency, the lifetime of the network and data storage capacity.

End-to-end delay, an important metric, is considered to deal with real-time traffic and transmit data packets within the stipulated time. End-to-end delay is the difference in the time taken between the source node transmitting data and the sink receiving it. It is the sum of the delay in transmission, propagation, queuing and processing at every hop.

Table 2 shows a comparison of the end-end delay. Figure 3 depicts the end-end delay for the proposed MLRP-HTEEN-UDSP protocol and Figure 4 compares it with the other

protocols such as LEACH, CCBRP and PEGASIS. It suggests that the proposed protocol performs better than other protocols. The delay is at a minimum since the hierarchical architecture of the CHs for all the times chooses the route that has fewer hops with good quality links.

Table 2. Comparison of end-end delay.

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

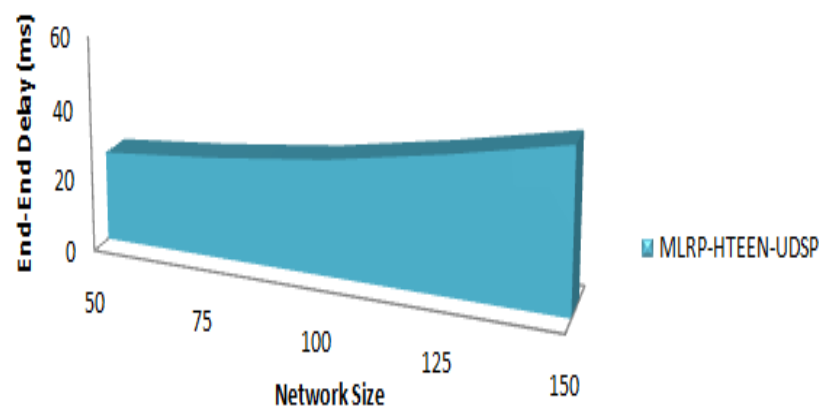


Figure 3. End-to-end delay of MLRP-HTEEN-UDSP.

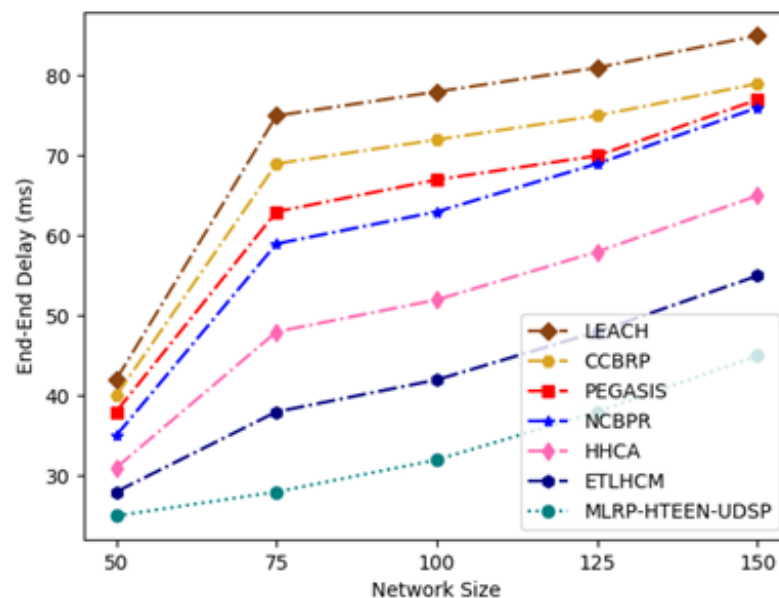


Figure 4. Comparison of end-to-end delay.

Throughput is the total packets received by the sink within a specified duration. The comparison of throughput is shown in Table 3.

Table 3. Comparison of throughput.

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

Figure 5 depicts the throughput of MLRP-HTEEN-UDSP, while Figure 6 compares the throughput of the proposed protocol with other protocols. The selection of multiple paths and minimum delay balances the load and uses the wireless spectrum efficiently. Thus, it achieves a higher throughput than other protocols.

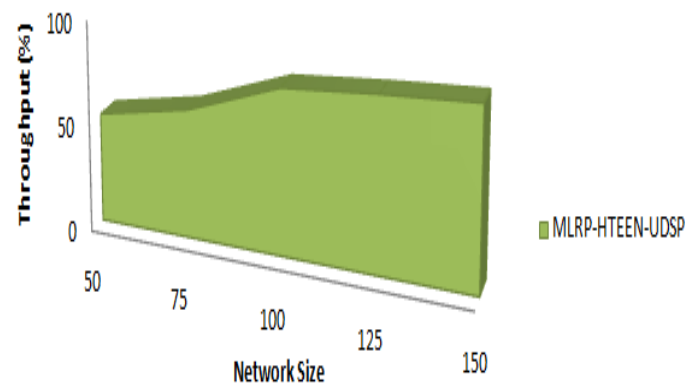
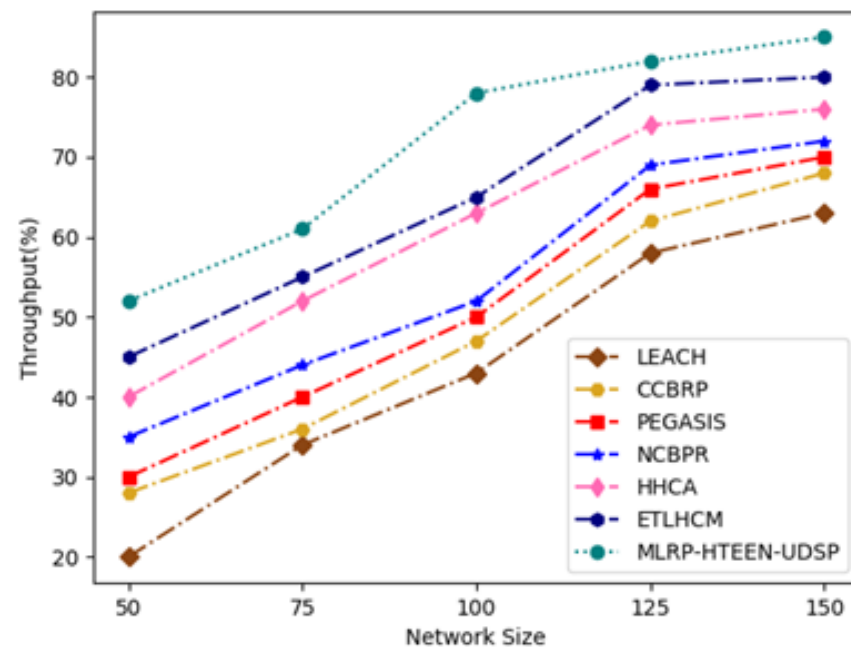
**Figure 5.** Throughput of MLRP-HTEEN-UDSP.**Figure 6.** Comparison of throughput.

Table 4 shows a comparison of the energy efficiency. The average energy efficiency is represented in Figure 7 where we can realize that our proposed protocol MLRP-HTEEN-UDSP has less energy dissipation compared with other protocols (LEACH, CCBPR and PEGASIS) as shown in Figure 8 with various node numbers.

Table 4. Comparison of energy efficiency.

Network Size	LEACH	CCBRP	PEGASIS	NCBPR	HHCA	ETLHCM	MLRP-HTEEN-UDSP
50	20	23	25	28	32	38	44
75	35	38	40	42	46	50	51
100	38	40	43	45	51	58	61
125	50	53	55	59	63	69	72
150	52	58	60	62	68	70	75

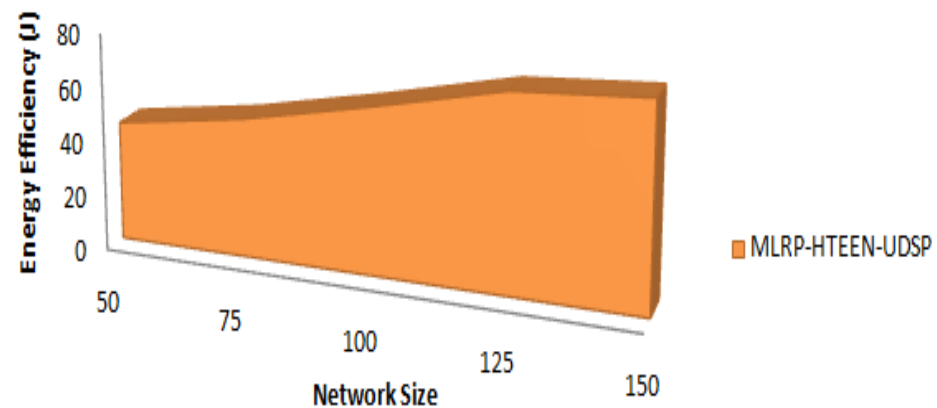
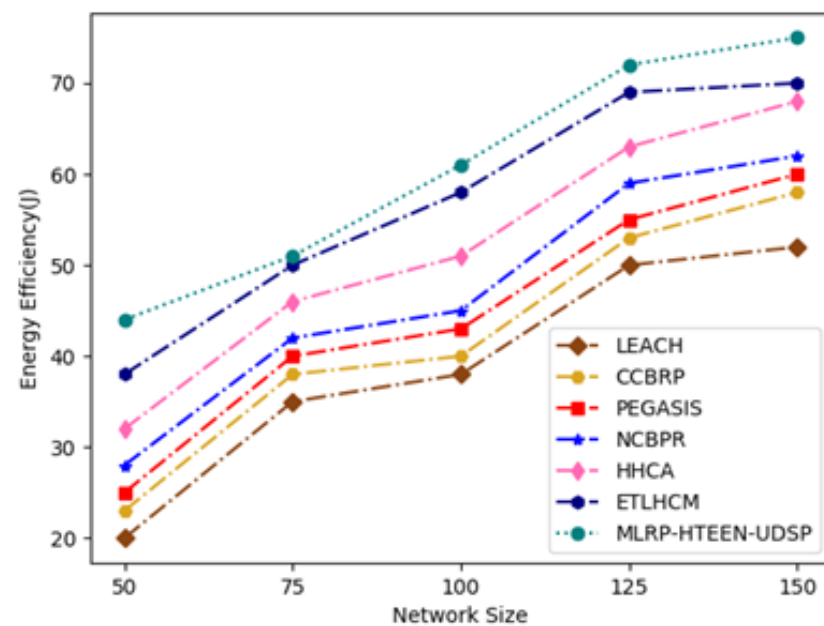
**Figure 7.** Energy efficiency of MLRP-HTEEN-UDSP.**Figure 8.** Comparison of energy efficiency.

Table 5 shows the comparison of the network lifetime. Figure 9 presents the network lifetime for the proposed MLRP-HTEEN-UDSP and Figure 10 shows a comparison of the network lifetime between the proposed and existing techniques.

Table 5. Comparison of network Lifetime.

Network Size	LEACH	CCBRP	PEGASIS	NCBPR	HHCA	ETLHCM	MLRP-HTEEN-UDSP
50	28	30	33	38	45	50	55
75	45	48	50	55	59	63	65
100	49	51	56	65	71	78	81
125	50	56	59	66	79	82	85
150	52	59	61	72	80	85	88

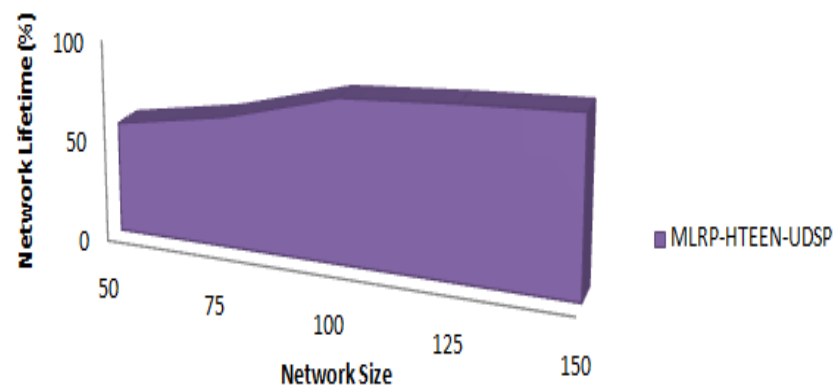
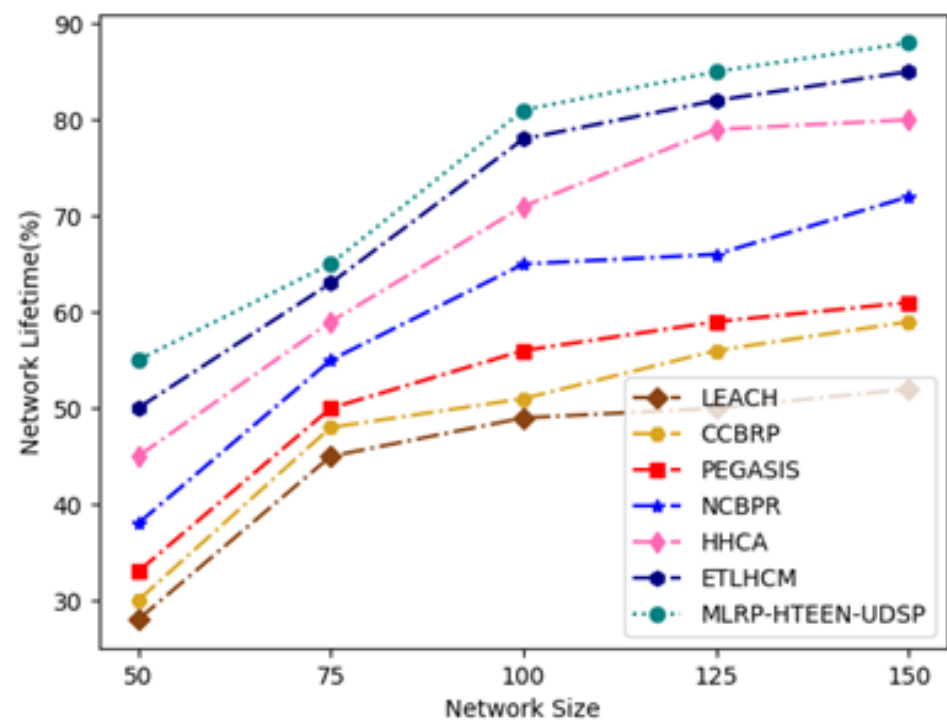
**Figure 9.** Network lifetime of MLRP-HTEEN-UDSP.**Figure 10.** Comparison of network Lifetime.

Table 6 shows the comparison of data storage. Figure 11 shows the data storage for the proposed MLRP-HTEEN-UDSP and Figure 12 shows the comparison of the data storage between the proposed and existing techniques.

Table 6. Comparison of data storage.

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

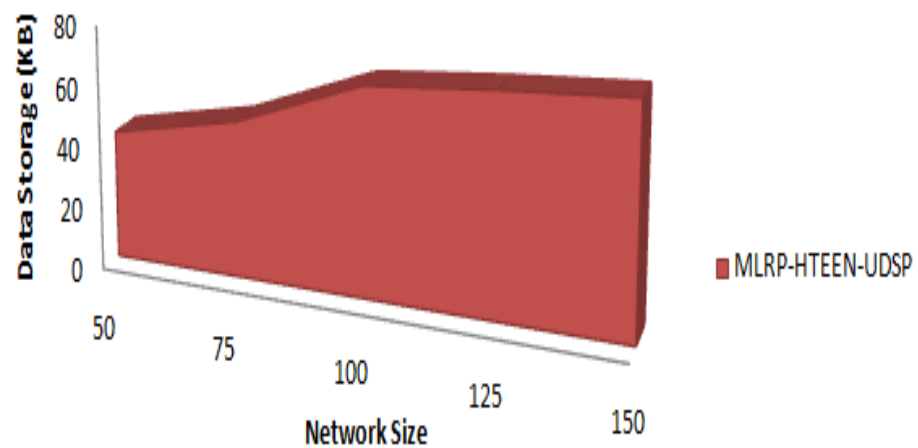
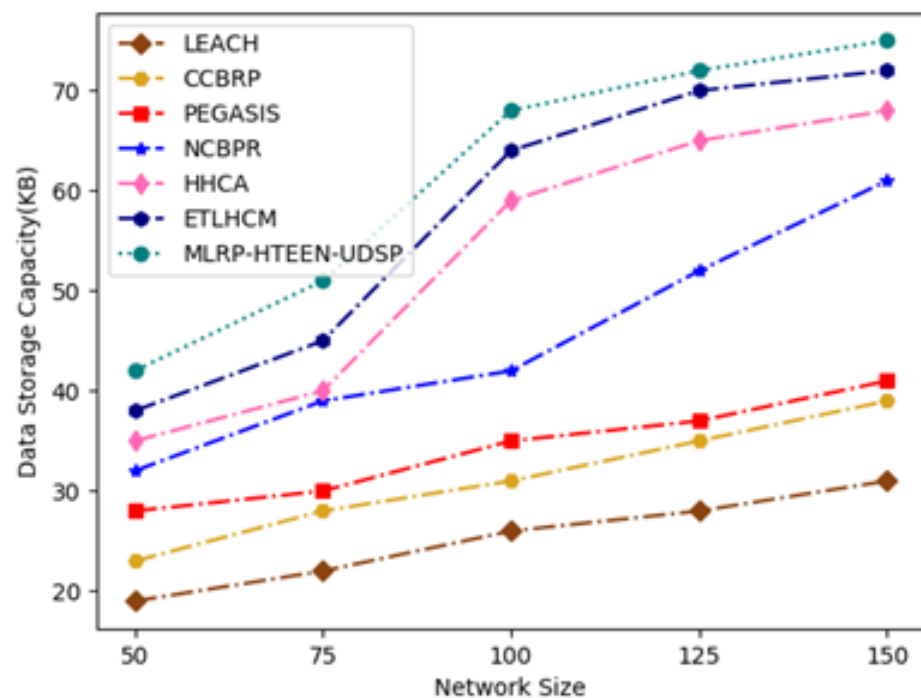
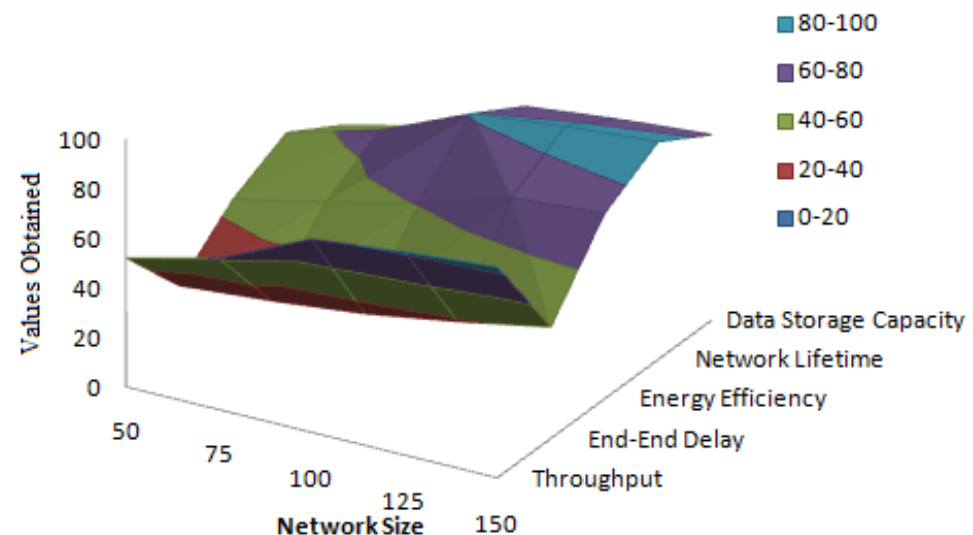
**Figure 11.** Data storage of MLRP-HTEEN-UDSP.**Figure 12.** Comparison of data storage.

Table 7 represents the overall parameter comparison of the proposed and existing techniques, and Figure 13 is the graphical representation of the overall comparison.

Table 7. Overall comparisons of MLRP-HTEEN-UDSP.

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

**Figure 13.** Overall comparison of MLRP-HTEEN-UDSP.

5. Conclusions

In this research, an energy optimization method with secure routing for IoT heterogeneous WSN applications is proposed. This secure as well as reliable routing protocol gathers data about neighbor nodes at BS, and generates the key and energy-efficient multipath for every node. CHs help in data aggregation and forward them to BS, which continuously monitors nodes for residual energy to choose some new paths and CHs. By using the complexity of multimedia processing and the aggregation process to the CHs side, as well as preventing path loops and path cycles for establishing routes, the integrated implementation of MLRP-HTEEN-UDSP produced a minimum end-to-end delay in suitable data packets and reduced the energy consumption at SNs. We also demonstrated a light-weight distributed key management method for supporting secure communication among nodes. The performance of MLRP-HTEEN-UDSP outperforms the existing ones such as LEACH, CCBRP and PEGASIS in all the performance metrics including end-to-end delay, throughput, energy efficiency, network lifetime and data storage capacity. Future work of the proposed protocol will be extended to the performance analysis in the green IoT environments with an increased network size.

Author Contributions: Conceptualization, Writing—original draft N.R.; Supervision, V.C. and S.B.G.; Writing—original draft and review & editing, K.J. and M.G.; Validation, C.V.; propose the new method or methodology, N.R. and S.B.G.; Formal Analysis, Investigation C.O.S.; Resources, S.B.G. and C.O.S.; Software, T.C.M.; Writing—review & editing, T.C.M. All authors have read and agreed to the published version of the manuscript.

Funding: National Research Development Projects to finance excellence (PFE)-14/2022-2024 granted by the Romanian Ministry of Research and Innovation, this paper was partially supported by UE-FISCDI Romania and MCI through projects AISTOR, FinSESCO, CREATE, I-DELTA, DEFRAUDIFY, Hydro3D, FED4FIRE—SO-SHARED, AIPLAN—STORABLE, EREMI, NGI-UAV-AGRO and by European Union’s Horizon 2020 research and innovation program under grant agreements No. 872172 (TESTBED2) and No. 777996 (SealedGRID).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data will be shared for review based on the editorial reviewer’s request.

Acknowledgments: The work of Chaman Verma was supported by the European Social Fund under the project “Talent Management in Autonomous Vehicle Control Technologies” (EFOP-3.6.3-VEKOP-16-2017-00001).

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

References

- 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.
- 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.
- 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 a Wireless Sensor Network. *Sensors* **2017**, *17*, 69. [\[CrossRef\]](#)
- Sharma, N.; Sharma, A.K. Cost analysis of hybrid adaptive routing protocol for heterogeneous wireless sensor network. *Sādhanā* **2016**, *41*, 283–288. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Airehrour, D.; Gutierrez, J.; Ray, S.K. Secure routing for internet of things: A survey. *J. Netw. Comput. Appl.* **2016**, *66*, 198–213. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Guo, X.; Lin, H.; Li, Z.; Peng, M. Deep-Reinforcement-Learning-Based QoS-Aware Secure Routing for SDN-IoT. *IEEE Internet Things J.* **2020**, *7*, 6242–6251. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Preeth, S.K.; Dhanalakshmi, R.; Kumar, R.; Shakeel, P.M. An adaptive fuzzy rule based energy efficient clustering and immune-inspired routing protocol for WSN-assisted IoT system. *J. Ambient. Intell. Humaniz. Comput.* **2018**. [\[CrossRef\]](#)
- Hammi, B.; Zeadally, S.; Labiod, H.; Khatoun, R.; Begriche, Y.; Khokhi, L. A secure multipath reactive protocol for routing in IoT and HANETs. *Ad Hoc Netw.* **2020**, *103*, 102118. [\[CrossRef\]](#)
- 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 JEHO 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, H.; Sadegh Amiri, I. CBPR: A Cluster-Based Backpressure Routing for the Internet of Things. *Wirel. Pers. Commun.* **2021**, *118*, 3167–3185. [\[CrossRef\]](#)
23. 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. [\[CrossRef\]](#)
24. 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.
25. 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. [\[CrossRef\]](#)
26. 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. [\[CrossRef\]](#)
27. 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.
28. 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. [\[CrossRef\]](#)
29. 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. [\[CrossRef\]](#)
30. 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. [\[CrossRef\]](#)