electronics

MDPI

Article

Detection of Hello Flood Attacks Using Fuzzy-Based Energy-Efficient Clustering Algorithm for Wireless Sensor Networks

S. Radhika [1,*], K. Anitha [2], C. Kavitha [3,*], Wen-Cheng Lai [4,5] and S. R. Srividhya [3]

[1] Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602105, Tamil Nadu, India
[2] Department of Computing Technologies, School of Computing, SRM Institute of Science and Technology, Chennai 603203, Tamil Nadu, India
[3] Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai 600119, Tamil Nadu, India
[4] Bachelor Program in Industrial Projects, National Yunlin University of Science and Technology, Douliu 640301, Taiwan
[5] Department Electronic Engineering, National Yunlin University of Science and Technology, Douliu 640301, Taiwan
* Correspondence: radhikas.sse@saveetha.com (S.R.); kavitha4cse@gmail.com (C.K.)

Abstract: Clustering is one among the most important strategies to improve the lifetime of wireless sensor networks (WSNs). The frequent occurrence of clustering and the subsequent interchange of data overload the sensor nodes and result in wasting power. WSNs are susceptible to attacks because of their resource-constrained nature and large applications in critical military areas. The objective of the threats to the security of wireless sensor networks is to compromise the network by seizing information for misuse. Security features have become a major concern in these types of networks as it is important to protect sensitive data from unauthorized users. This paper aims to present an enriched clustering strategy to minimize the overhead caused by clustering, by formulating an effective cluster update schedule. It also focuses on the attacks that occur during an exchange of initialization messages with neighbors. Clustering of the network is carried out on the basis of the energy of sensor nodes. The nodes that are the heads of the cluster nodes are determined according to the characteristics of energy factors; hence, the role is frequently switched among the nodes of the cluster. To formulate the next cluster update schedule, a fuzzy inference system is employed, and this uses the energy factor of the node, the distance the node is placed from the sink, and the number of member nodes of the cluster. A mechanism is included during an exchange of initialization messages that detects any malicious node pretending to be a neighbor node. The proposed algorithm is evaluated using simulation, and it is found to produce an improved lifetime of 1700 time units. It is shown to conserve the energy of sensor nodes and protect them from unauthorized nodes posing as legitimate neighbors.

Keywords: wireless sensor networks; fuzzy logic; clustering; energy efficiency; hello flood; attacks

Citation: Radhika, S.; Anitha, K.; Kavitha, C.; Lai, W.-C.; Srividhya, S.R. Detection of Hello Flood Attacks Using Fuzzy-Based Energy-Efficient Clustering Algorithm for Wireless Sensor Networks. *Electronics* **2023**, *12*, 123. https://doi.org/10.3390/electronics12010123

Academic Editors: Sabrine Kheriji, Olfa Kanoun and Faouzi Derbel

Received: 17 November 2022
Revised: 19 December 2022
Accepted: 19 December 2022
Published: 27 December 2022

1. Introduction

Thanks to remarkable advancements in the field of integrated circuits, wireless sensor networks (WSNs) have evolved to be an interesting area that has attracted larger attention in research. The networks that are widely deployed to observe environmental conditions consist of several sensor nodes, which may be the homogeneous type or the heterogeneous type. These nodes carry out sensing, processing, and communications with other sensors over a short range. A wireless sensor node's lifetime is restricted owing to constraints in the battery resources and accessibility. In addition, the sensor nodes are usually installed in harsh regions, which makes it very difficult to recharge batteries. The energy spent for

communication forms the major part of the consumption of power for individual sensor nodes. Thus, the energy efficiency factor gains importance as one of the critical issues to be addressed in sensor networks [1].

The primary function in sensing is to congregate data from the environment and transmit them. The transmission of data consumes considerably more energy than data collection does. Many prevailing methods tend to find the path that consumes minimal energy between any two nodes. Retransmissions by nodes significantly increase energy costs. Therefore, a tradeoff between energy and the lifetime of the network is important to enhance energy efficiency [2]. Energy conservation is one among the well-known challenges in wireless sensor networks. Clustering protocols enhance network characteristics, such as scalability, energy efficiency, etc. [3]

Clusters that are smaller in size create connectivity holes, greatly affecting the reliability of the observed network. Many clustering algorithms create less-optimal clusters independent of the energy and area coverage issues. If the number of clusters acting under a cluster head has not been regularized, then managing the energy usage of nodes becomes a concern. The optimized use of energy after clustering must also factor in the energy of individual sensor nodes [4].

The impromptu nature of sensor networks with the wireless multihop transmission, restricted energy, and processing capability pave the way for many security-related problems. The traditional method of gathering information in wireless networks is by broadcasting requesting messages. The basic element in the formation of the topology of sensor networks is neighbor discovery. The existing protocols based on neighbor discovery depend on the method of broadcasting request messages.

On the contrary, sensor nodes tend to broadcast hello messages informing their characteristics to their neighbor nodes. The vulnerability of sensor networks makes them affected opens them up to various kinds of flooding attacks, and the broadcasting characteristics of these protocols were exploited to formulate the hello flooding attack to influence a group of nodes. The attacker nodes use high transmission power such that the other nodes consider them as their neighbor. Identifying the attacker node and restricting the sensor nodes from the transmission of data to the attacker achieves considerable energy savings and security. Several studies have been performed to lessen the effects of flooding attacks [5].

With regard to the flooding attacks, the stability of the reliability of networks is improved in fifth-generation (5G) networks by utilizing big data analytics and machine-learning algorithms. Various machine-learning approaches can be incorporated to improve the energy efficiency of 5G networks. One such application is using massive MIMO for energy efficiency, where the estimation of channels and detecting them are identified as problems as a result of an increased number of antennae. Therefore, machine learning can help solve many challenges faced by 5G networks as several new technologies are integrated in an energy-efficient manner [6,7].

2. Contribution

The proposed system focuses on sensor nodes' energy and suggests a method by which the malicious nodes can be identified. The major contributions of the paper include the following:

(1) An approach focusing on the energy of wireless sensor nodes is put forward, in which there can be two types of sensor nodes, namely cluster head nodes and member nodes. This helps to identify the role of each sensor node, thus focusing on the energy parameter.
(2) On the basis of the initialization messages exchanged between the sensor nodes during cluster formation, the identification of malicious sensor nodes is performed. When the number of messages received by the member node exceeds the number of neighbors, a malicious node is detected.
(3) The aggregation of sensor readings is performed by the cluster head. The member node associates itself with the nearest head node.

(4) The clusters are updated periodically to make sure that the sensor nodes retain energy for their functionality. The schedule at which the cluster is to be updated is determined with the fuzzy inference system. This determines the update cycle on the basis of the remaining energy, distance, and the number of member nodes.
(5) The energy enhancement that was obtained by applying the proposed approach is evaluated by using the existing energy-efficient clustering with correlation and random update (EECRU) method.

3. Organization

The remainder of this paper is organized as follows: The review of the prevailing methods of reducing energy usage and ensuring security of wireless sensor networks in the literature is presented in the related work section. The energy model applied in the proposed approach is described in the energy model section. The proposed approach section describes the proposed fuzzy-based energy-efficient clustering algorithm. The experimental evaluation and the results obtained are shown in the results section. Finally, the conclusion and future research directions are presented.

4. Related Work

Usually, upon receiving the hello messages, the receiver nodes include the identity of the senders to their list of neighbors. This working model helps the attacker nodes to convince the group of nodes of their neighborhood. The solution for the flooding attack depends on the strength of the signal. On the basis of the signal strength, nodes are characterized as friends or strangers [8,9]. The request messages with abnormal power characteristics are omitted. The power-based solutions can be compromised by attacker nodes. Finding the distance of transmission is one of the ways of determining fraudulent neighborhood requests [10].

Martins and Guyennet 2010 proposed a cryptography-based method that limits the distance between nodes. However, the method was found to be inefficient because it was prone to internal attacks [11]. PalSingh, Anand Ukey, and Jain 2013 used an echo protocol based on distance estimation with a travel time of signal measurements [12]. In this method, the sender can either add a timestamp to the transmitted packet or attach its geographical location. The authenticity of the sender is validated on the basis of this information.

Bradbury and Jhumka 2017 identified that protocols can be classified according to time and location. The strategies that completely depend only on the time of signal propagation could not provide enough security [13]. However, the protocols that include time and location as factors provide better security from external attackers during the phase of neighbor discovery. V. Sharma and Pughat 2017 stated that a set of nodes are chosen randomly, and these nodes forward the hello message request report to the sink node that authenticates the validity of the hello request. This method suffers from the scalability issue and is very similar to the abnormal detection strategies based on graph theory [14].

Kim et al. 2015 claimed that sensor nodes initially discovered the neighbors by applying the challenge–response method, and they used a group of key values obtained from random-key generation. Therefore, the valid neighbor of the sensor node can identify the broadcast message. This method has the disadvantage of encountering internal attackers supplied with powerful receivers. The challenges in terms of security in wireless sensor networks include improving performance in security strategies, handling attacks in wireless links, the mobility of nodes, the scalability of the network, addressing dynamic addition, the removal of nodes without compromising security, etc. [15].

The confidentiality of sensor nodes can be compromised by internal or external attackers. These sensor nodes are deprived of protective measures, and they make the entire network vulnerable to attacks. Selective forwarding is an attack in which the affected nodes drop packets in due course of time, thus affecting the performance of the network [16]. This greatly impacts the integrity of data in applications involving healthcare and industrial

monitoring, where the significance of data is comparatively high. Many other attacks affect nodes in terms of the rate of data delivery, such as black hole attacks, wormhole attacks, etc.

Sensor nodes are characterized by restricted power supply, memory, and processing capability. The sensor nodes are grouped largely, whereas the topology of the network changes often thanks to the mobility, addition, or removal of nodes. The change in topology causes the sensor nodes to be easily affected by attackers, and this makes the security characteristics of wireless sensor networks vital [17]. Differentiating between valid and invalid sensor nodes is important primarily during the establishment of network connections. The disclosure of information to unauthenticated users affects the confidentiality of sensor data readings. There are many methods to preserve confidentiality, including cryptography. Data integrity defines the reliability and accuracy of data during network operations. This also involves the transmission of data without change or falsification by attackers [18,19].

A compromised node is an authentic node when compromised by unauthorized users. The nodes are manipulated to perform various despicable attacks, such as reporting false messages, injecting new messages, modifying messages during transmission, etc. The affected nodes can be applied with a recovery process to revoke the attacks. When the network can be accessed from anywhere at the user's request, then the network is said to be available. This network availability is said to be compromised if authentic users face a lack of access to the network. This type of attack is said to be a denial of service (DoS) attack. Wireless sensor networks suffer from various security problems that threaten their performance and consume resources. The characteristic of WSNs that makes them open to access paves the way for the attacker to launch attacks. The security holes in the network can be easily compromised by attackers.

The features of WSNs expose them to different types of threats. Some of these threats are common to all ad hoc networks. The attacks on WSNs focus mainly on the restricted power supply of the sensor nodes. Some attacks are passive, and they do not modify data readings sensed by the nodes. Instead, they listen to the network to seize information about the network. It is difficult to detect such types of attacks, and it is quite easy to compromise the data if they are transmitted with no enforced encryption. On the contrary, active attacks modify the sensor data [20,21].

In message injection, the intruder forwards false information to corrupt the transmitted sensor readings or simply floods the network. In replication, the attacker makes copies of the transmitted data and sends it to unintended sensor nodes on the network. Reprogramming and replacing the sensor nodes are two of the malicious activities of such attackers. This sensor will reproduce the data readings to the intruder, which can be misused. The use of hello messages is common in WSNs for neighbor discovery. Malicious nodes posing as genuine nodes tend to send hello messages to other nodes on the network, making them appear to be authentic neighbor nodes. These malicious nodes receive information from the nodes on the network [22].

The protocols that rely on the exchange of location information for the control of data flow and maintenance of topology are influenced primarily by the hello flooding attack. An attacker can retransmit packets with a sufficient power level to create this type of attack. It is usually assumed that communication is within a fixed range and that the sensor nodes are assumed to have the same transmission signal strength [23].

One of the important attacks in the network layer is the hello flood attack. This attack can be created by any node with high power, such that nodes that are farther away can receive messages from it. All transmitted messages will route through the attacker node; thus, there is a possibility of compromising the messages. The nodes will consider the malicious node as a genuine node and will initiate communication with this node. Any such communication will result in a waste of energy. Subsequently, the attacker node gains control over the network and also affects the routing decisions in the network.

The hello packets tend to have certain unique characteristics. These packets are usually smaller than data packets and are broadcast without any acknowledgment. Cryptographic methods can be applied to encounter hello flood attacks. Nodes share the secret key,

and only the authentic nodes can decrypt the key, thus gaining access to the transmitted messages. The new encryption key is generated for every new data transmission [24].

Strategies that use hello packets assume that the messages received by them come from legitimate neighbors. However, a high-powered malicious node can act as a neighbor within the range of communication. If the adversary node broadcasts a false route to all its neighbors, then all transmissions will be communicated through the attacker node, making it easy to sense the transmitted data [25,26].

A few clustering methods concentrate on preventing the faster death of head nodes. These methods, however, suffer from the following disadvantages:

i. The overhead of message transmissions are not properly addressed.
ii. Message transfers during cluster construction were redundant and complicated.
iii. Suitable parameters were not applied to the fuzzy inference system.
iv. The detection of attacks on hello flood messages was not consistently performed.
v. The impact of attacks on network operations was not sufficiently studied.
vi. Energy-focused methods that address hello flood attacks were not formulated.

To analyze the above-identified constrictions, this paper proposes an approach based on energy for wireless sensor networks. It addresses the attacks caused by flooding from hello packet attacks. It applies fuzzy logic to calculate the schedule of selecting the cluster heads for subsequent data transmission. Sufficient simulations have been organized to verify the efficiency of the recommended approach [27–29]. The results indicate that the proposed strategy identifies malicious neighbor nodes, if any, and also balances the energy usage among nodes on the network.

5. Energy Model

The power expended to transmit a packet is assumed to be Ep_t; it is related to the message segment length l_{ms}; and the distance is assumed to be d_{rt}. Hence,

$$Ep_t(l_{ms},\ d_{rt}) = l_{ms}(E_{el} + E_b) \tag{1}$$

$$Ep_t(l_{ms}, d_{rt}) = l_{ms}\left(E_{er} + \varepsilon_{sf} {d_l}^2\right) \text{ if } d_{\text{rt}} \ \leq \ d_{\text{lt}} \tag{2}$$

$$Ep_t(l_{ms}, d_{rt}) = l_{ms}\left(E_{er} + \varepsilon_{sf} {d_{rt}}^2\right) \text{ if } d_{\text{lt}} \ < \ d_{\text{rt}} \ < \ d_{\text{ut}} \tag{3}$$

$$Ep_t(l_{ms}, d_{rt}) = l_{ms}\left(E_{er} + \varepsilon_{mc} {d_{rt}}^4\right) \text{ if } d_{\text{rt}} \ \geq \ d_{\text{ut}} \tag{4}$$

E_b is the expended energy to transmit a bit; ε_{sf} indicates a free space model; and ε_{mc} indicates the multipath channel model. d_{lt} and d_{ut} signify the minimum value and maximum threshold value of distance d_{rt}, respectively, and E_{er} indicates the point of reference of usage of energy. The reference point level of energy usage is represented by E_{el}. The energy E_{rv} used upon a packet reception centers primarily on the length of the message segment, l_{ms}. Therefore,

$$E_{rv}(l_{ms}) = l_{ms} \times E_{er} \tag{5}$$

6. Proposed Approach

With the objective of highlighting the power constraints, this paper puts forward a clustering technique to achieve a remarkably improved network lifetime by making a selection of suitable parameters. To lessen energy exhaustion and to support substantially enhanced clustering, the recommended clustering algorithm decides on head nodes in every cluster that are at the smallest distance from the member nodes.

Each sensor node identifies itself as a cluster member or a cluster head by participating in the clustering process. The constructed clusters are regularly reorganized in a structure suggested by the fuzzy inference system. A node that maintains higher energy would be designated as the head node. The unexpended power of the nodes and their physical

position are generally taken into account for effective clustering. Network lifetime is the time when the energy of the first sensor drains off and subsequently other nodes start draining their energy.

The network is assumed to have N nodes, and every network node has a set of neighbor nodes in the limits of the radius r. The head node holds the onus of forwarding the assembled data, and consequently, this node requires preserving its power for unending monitoring. The remaining energy of the node and its neighborhood information are deliberated for the cluster construction, and it helps in enhancing the clustering implementation.

Initialization messages are exchanged between every pair of neighbors before the clustering process. The neighborhood information of every node determines the node's identity and its present energy. Sharing information enables a node to identify itself as a head or cluster member. If the number of initialization messages is greater than nodes in the neighborhood set, then the node suspects the presence of a suspicious node in the neighborhood. The node that identifies the malicious node sends a message to the base station and switches it off, into the sleep state. The node remains in a sleep state until the next cluster update process.

If the number of initialization messages equals the number of nodes in the neighborhood, then the node begins as a member of the head node. The identification is conducted by making a comparison of the energy of a node with the energy levels of all of its neighbors. The head node adds the requesting node's identity to its list of cluster members.

The algorithm for the proposed approach is as follows:

1. Each node n_i calculates its neighbor set NS_i.
2. Calculate the number of neighbor nodes $nb_i = |NS_i|$.
3. Each node sends (NodeID, BalEnergy) to NS_i.
4. Count the number of initialization messages m_i received from neighbors.
5. If the number of initialization messages (m_i) $\leq$ the number of neighbor nodes (nb_i), then perform steps 6 to 15.
6. For every node n_i and n_j belonging to the NS_i,
   a. if BalEnergy(n_i) > max (BalEnergy(n_j)), then Node_Type = HN.
   b. if BalEnergy(n_i) < max (BalEnergy(n_j)), then Node_Type = MN.
7. For every member node MN,
   a. find a node with Node_Type = Head Node(HN) and distance = min (distance with all neighbors).
   b. attach to the HN node as MN.
8. For every cluster head node HN, apply FIS (BalEnergy(HN), no. of MNs, distance to the sink node) to calculate the next cluster update schedule.
9. Perform data transmission until next cluster update schedule expires.
10. If next update schedule expires, go to step 3.
11. If the number of initialization messages (mi) > the number of neighbor nodes (nb_i), then send_message ("malicious neighbor found") to the base station and switch to sleep state.
12. Stay in sleep state until the next cluster update process.
13. End.

The fuzzy logic method is beneficial because its requirements can be readily utilized in the operations of sensor nodes, and thus, the overall performance of the network can be increased. It is found to be useful for clustering, cluster head identification, data grouping, and forwarding. The properties of fuzzy logic, such as robustness and execution simplicity, make it a viable solution for a variety of problems.

The fuzzy inference system applied in the proposed algorithm is shown in Figure 1. When the clusters are frequently reorganized, it incurs an extra overhead on the nodes of the network. To address this challenge, every head node determines the next cycle for updating the cluster by factoring in the remaining value of energy, number of members, and distance of the member nodes to the sink node. These are the major factors that

affect the energy consumption of a node, and they play major roles in the lifetime of a network. The essence of the fuzzy logic application simplifies decision-making to better understand the characteristics of the cluster head. The selection of distance as one of the parameters is inferred from the fact that the sink node expends substantial resources to transmit the collected data readings. Additionally, a head node with minimal energy decides on a smaller update cycle as it will not be competent to perform its functionality for a longer period.

$$\text{UpdateCycle}_i = \text{FIS}\ (\text{RemEnergy}_i, \text{Distance}_i, \text{Number of member nodes}) \quad (6)$$

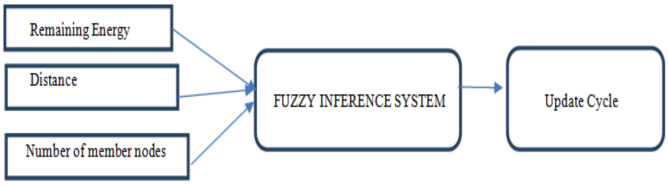

Figure 1. Fuzzy inference system.

Once the identified update cycle elapses, the successive clustering process occurs, where a new cluster is formed [30–32]. In addition, a new cluster head is selected, and appropriate member nodes get associated with the head node. A value of very low to very high is picked up as the scope for the residual energy inputs. Distance variables can take up values of near, medium, or far. Likewise, the number of nodes can include the values low, medium, or high. The choice of values for the cluster update cycle can vary between short, medium, and long [33–35]. Table 1 shows a subset of the values that can be assigned for the input and output variables. If the residual energy is low, the distance is near and the update cycle is very short, irrespective of the number of nodes. If there is sufficient residual energy, the update cycle can be considerably short.

Table 1. A subset of fuzzy rules for determining the update cycle.

RE	Distance	Number of Member Nodes	Update Cycle
Very Low	Near	Low/High	Very Short
Very Low	Medium	Low/High	Very Short
Very Low	Far	Low/High	Very Short
Low	Near	Low/High	Short
Low	Medium	Low/High	Short
Low	Far	Low/High	Short
Medium	Near	Low	Medium
Medium	Medium	Low	Long
Medium	Far	Low	Long

7. Results and Discussion

The clustering method that is proposed is valued by analyzing it with recently proposed algorithms, such as DDCD, EECRU, and LEACH. The proposed clustering method was implemented with the Intel Lab Dataset. This dataset consists of sensor data collected by 54 sensors installed in the Berkeley Research Lab. The data collection area was 40.5 m × 31 m and the duration was from February to April 2004. Factors such as temperature and humidity were examined by the installed sensor devices every 31 s. The dataset clearly defines the sensor locations. The algorithm's performance was measured by simulation using MATLAB. The factors used for analysis are listed in Table 2.

Table 2. Network parameters in the proposed algorithm.

Network Parameters for Simulation	Parameter Values
Network size	40.5 × 31 m
Node chosen as sink	9 at (21.5, 22)
No. of nodes in the sensed region	54 nodes
Initial energy for the nodes	2 Joules
Node's range of communication	5 m
E_{el}	0.01 J/bit
ε_{sf}	0.01 J/bit/m^2
ε_{md}	0.0013 J/bit/m^4

The relationship between temperature data over the sensed time period and the different sensor readings observed over the sensed time period is shown in the Figure 2. The correlation coefficient of the data is observed to be 0.692, and the R-square value is calculated as 0.479. While analyzing the network lifetimes of the proposed algorithm with the compared approaches, the depletion of energy has been continuously observed in the process. It is determined that a network lifetime of 1700 time units has been achieved, which significantly retained greater energy.

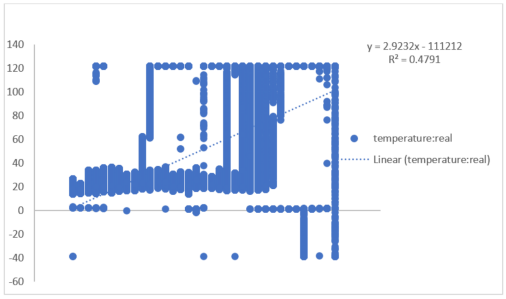

Figure 2. A representation of temperature data values over the sensed period.

The results in Figure 3 show that the lifetime of the network obtained by the proposed algorithm is prominently longer than the lifetime achieved by the chosen algorithms. This is possible by a reduction in the number of messages and decreased data, thanks to the benefits of machine-learning models. These observations show that the proposed algorithm performs better than the other similar algorithms concerning network lifetime and the individual energy levels of sensor nodes.

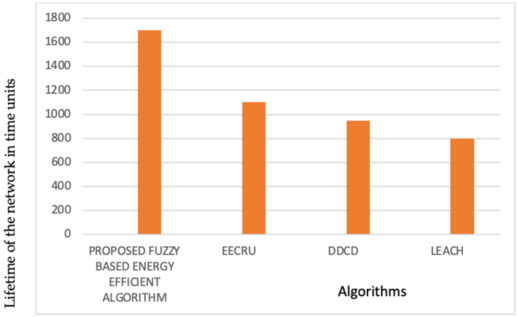

Figure 3. Comparison of the proposed algorithm with EECRU, DDCD, and LEACH algorithms.

The performance of the proposed algorithm in comparison with the existing algorithms is shown in Figure 4. The representation clearly shows that the proposed algorithm outperforms the existing algorithms.

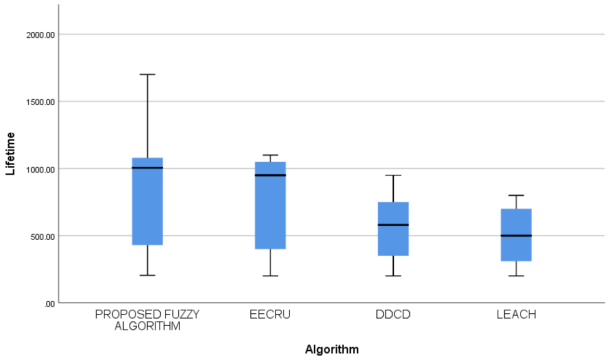

Figure 4. Boxplot representing the performance of algorithms.

As shown in Table 3, the lifetime of the network is estimated by varying the number of iterations. The mean value shows that the proposed algorithm sustains more than other algorithms do.

Table 3. Descriptive statistics of network lifetime.

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum Lifetime	Maximum Lifetime
					Lower Bound	Upper Bound		
Proposed Fuzzy-Based Energy-Efficient Algorithm	10	847.5000	474.73531	150.12449	507.8948	1187.1052	205.00	1700.00
Energy-Efficient Clustering with Correlation and Random Update (EECRU)	10	747.0000	369.11456	116.72427	482.9514	1011.0486	200.00	1100.00
Data Density Correlation Degree (DDCD)	10	553.0000	254.16749	80.37482	371.1795	734.8205	200.00	950.00
Low-energy Adaptive Clustering Hierarchy (LEACH)	10	503.0000	226.17840	71.52389	341.2017	664.7983	200.00	800.00

8. Conclusions and Future Work

The productive method for energy utilization in wireless sensor networks increased network lifetime. This paper recommended an energy-centric approach with the application of fuzzy logic. The proposed method highlighted the challenge of improving network lifetime even as the consumption of energy was impartially dispersed among all the sensor nodes. The method also emphasized the expense of energy for sensing and transmission across clusters. The method addressed the identification of attacks from neighbor nodes during the exchange of initialization messages. The proposed algorithm made use of energy-based methods for simulation results and the calculation of network lifetime. The algorithm can be extended to mobile sensor networks and underwater sensor networks, where the location and environmental factors of the nodes are concerned. The algorithm can also be improved with prediction-based methods and applied machine-learning data reduction, and this can be the subject of future research.

Author Contributions: S.R.: research concept, methodology, and writing—original draft preparation; K.A.: supervision; C.K.: review and editing; W.-C.L.: investigation, funding acquisition; S.R.S.: validation. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been funded by the National Yunlin University of Science and Technology, Douliu.

Data Availability Statement: The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

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

References

1. Xing, S.; Wang, C.; Zhao, C.; Gao, J. Traffic Shaped Network Coding Aware Routing for Wireless Sensor Networks. *IEEE Access* **2018**, *6*, 71767–71782. [CrossRef]
2. Juan, L.; Hu, J.; Wu, D.; Li, R. Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2015**, *11*, 112–121. [CrossRef]
3. Al Islam, A.A.; Hossain, M.S.; Raghunathan, V.; Hu, Y.C. Backpacking: Energy-Efficient Deployment of Heterogeneous Radios in Multi-Radio High-Data-Rate Wireless Sensor Networks. *IEEE Access* **2014**, *2*, 1281–1306. [CrossRef]
4. Niayesh, G.; Al-Otaibi, Y.D.; Butt, S.A.; Sahar, G.; Rahim, S. Energy-Efficient and Coverage-Guaranteed Unequal-Sized Clustering for Wireless Sensor Networks. *IEEE Access* **2019**, *7*, 157883–157891. [CrossRef]
5. Sayad Haghighi, M.; Mohamedpour, K.; Varadharajan, V.; Quinn, B.G. Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 1185–1199. [CrossRef]
6. Mughees, A.; Tahir, M.; Sheikh, M.A.; Ahad, A. Towards Energy Efficient 5G Networks Using Machine Learning: Taxonomy, Research Challenges, and Future Research Directions. *IEEE Access* **2020**, *8*, 187498–1187522. [CrossRef]
7. Giannopoulos, A.; Spantideas, S.; Kapsalis, N.; Karkazis, P.; Trakadas, P. Deep reinforcement learning for energy-efficient multi-channel transmissions in 5G cognitive hetnets: Centralized, decentralized and transfer learning based solutions. *IEEE Access* **2021**, *9*, 129358–129374. [CrossRef]
8. Mohanty, S.N.; Lydia, E.L.; Elhoseny, M.; Al Otaibi, M.M.G.; Shankar, K. Deep learning with LSTM based distributed data mining model for energy efficient wireless sensor networks. *Phys. Commun.* **2020**, *40*, 101097. [CrossRef]
9. Mini, S.; Tandon, A.; Narayan, S.; Bhushan, B. Classification and Analysis of Security Attacks in WSNs and IEEE 802.15.4 Standards: A Survey. In Proceedings of the 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall), Dehradun, India, 15–16 September 2017. [CrossRef]
10. Parushi, M.; Singh, Y.; Anand, P.; Bangotra, D.K.; Singh, P.K.; Hong, W.C. Internet of Things: Evolution, Concerns and Security Challenges. *Sensors* **2021**, *21*, 1809. [CrossRef]
11. David, M.; Guyennet, H. Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey. In Proceedings of the 2010 13th International Conference on Network-Based Information Systems, Takayama, Japan, 14–16 September 2010. [CrossRef]
12. Virendra, P.; Ukey, A.S.A.; Jain, S. Signal Strength Based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks. *Int. J. Comput. Appl.* **2013**, *62*, 0975–8887. [CrossRef]
13. Matthew, B.; Jhumka, A. Understanding Source Location Privacy Protocols in Sensor Networks via Perturbation of Time Series. In Proceedings of the IEEE INFOCOM 2017—IEEE Conference on Computer Communications, Atlanta, GA, USA, 1–4 May 2017. [CrossRef]
14. Vidushi, S.; Pughat, A. *Energy-Efficient Wireless Sensor Networks*; CRC Press: Boca Raton, FL, USA, 2017.
15. Kim, S.G.; Kumoh National Institute of Technology, Gumi, and Korea. Reliable Random Key Pre-Distribution Schemes for Wireless Sensor Networks. *Int. J. Inf. Educ. Technol.* **2015**, *5*, 645. [CrossRef]
16. Hao, F.; Liu, Y.; Dong, Z.; Wu, Y. A Data Clustering Algorithm for Detecting Selective Forwarding Attack in Cluster-Based Wireless Sensor Networks. *Sensors* **2019**, *20*, 23. [CrossRef]
17. Zhu, F.; Liu, X.; Wen, J.; Xie, L.; Peng, L. Distributed Robust Filtering for Wireless Sensor Networks with Markov Switching Topologies and Deception Attacks. *Sensors* **2020**, *20*, 1948. [CrossRef]
18. Daniel, C.; Figuerêdo, S.; Oliveira, G. Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions. *Cryptography* **2017**, *1*, 4. [CrossRef]
19. Mani, V.; Kavitha, C.; Band, S.S.; Mosavi, A.; Hollins, P.; Palanisamy, S. A Recommendation System Based on AI for Storing Block Data in the Electronic Health Repository. *Front. Public Health* **2022**, *9*, 831404. [CrossRef]
20. Kupwade, P.H.; Szygenda, S.A. *Security for Wireless Sensor Networks Using Identity-Based Cryptography*; CRC Press: Boca Raton, FL, USA, 2012.
21. Kavitha, C.; Anita, X.; Selvan, S. Improving the efficiency of speculative execution strategy in hadoop using amazon elasticache for redis. *J. Eng. Sci. Technol. (JESTEC)* **2021**, *16*, 4864–4878.
22. Yassine, M.; Ezzati, A.; Belaissaoui, M. *Security and Privacy in Smart Sensor Networks*; IGI Global: Hershey, PA, USA, 2018.
23. Paris, K. *Security in RFID and Sensor Networks*; CRC Press: Boca Raton, FL, USA, 2016.
24. Kumar, S.S.; Bhushan, B.; Debnath, N.C. *Security and Privacy Issues in IoT Devices and Sensor Networks*; Academic Press: Cambridge, MA, USA, 2020.
25. Yongjin, K.; Helmy, A. Attacker Traceback in Mobile Multi-Hop Networks. *Handb. Secur. Netw.* **2011**, 169–190. [CrossRef]
26. Kavitha, C.; Mani, V.; Srividhya, S.R.; Khalaf, O.I.; Tavera Romero, C.A. Early-Stage Alzheimer's Disease Prediction Using Machine Learning Models. *Front. Public Health* **2022**, *10*, 853294. [CrossRef]
27. Dev, K.; Maddikunta, P.K.R.; Gadekallu, T.R.; Bhattacharya, S.; Hegde, P.; Singh, S. Energy Optimization for Green Communication in IoT Using Harris Hawks Optimization. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 685–694. [CrossRef]

28. Roy, A.K.; Nath, K.; Srivastava, G.; Gadekallu, T.R.; Lin, J.C.-W. Privacy Preserving Multi-Party Key Exchange Protocol for Wireless Mesh Networks. *Sensors* **2022**, *22*, 1958. [CrossRef]
29. Mamoun, A.; Kuruva, L.; Thippa, G.; Quoc-Viet, P.; Praveen, R. Multi-objective cluster head selection using fitness averaged rider optimization algorithm for IoT networks in smart cities. *Sustain. Energy Technol. Assess.* **2021**, *43*, 100973.
30. Radhika, S.; Rangarajan, P. On improving the lifespan of wireless sensor networks with fuzzy based clustering and machine learning based data reduction. *Appl. Soft Comput.* **2019**, *89*, 105610. [CrossRef]
31. Radhika, S.; Rangarajan, P. Fuzzy based sleep scheduling algorithm with machine learning techniques to enhance energy efficiency in wireless sensor networks. *Wirel. Pers. Commun.* **2021**, *118*, 3025–3044. [CrossRef]
32. Yakshana, P.; Anitha, K.; Chilambuchelvan, A. A fuzzy svm classification approach for content based image retrieval. *Int. J. Appl. Eng. Res.* **2015**, *10*, 17458–17462.
33. Anitha, K.; Naresh, K.; Rukmani Devi, D. A framework to reduce category proliferation in fuzzy ARTMAP classifiers adopted for image retrieval using differential evolution algorithm. *Multimed. Tools Appl.* **2021**, *79*, 4217–4238. [CrossRef]
34. Kavitha, C.; Anita, X. Task failure resilience technique for improving the performance of MapReduce in Hadoop. *ETRI J.* **2020**, *42*, 748–760.
35. Numan, M.; Subhan, F.; Khan, W.Z.; Hakak, S.; Haider, S.; Reddy, G.T.; Jolfaei, A.; Alazab, M. A Systematic Review on Clone Node Detection in Static Wireless Sensor Networks. *IEEE Access* **2020**, *8*, 65450–65461. [CrossRef]