IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 September 2023, accepted 15 September 2023, date of publication 22 September 2023,
date of current version 4 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3318005

RESEARCH ARTICLE

State-Based Energy Calculation Scheme for Internet of Things Networks

RAJA WASEEM ANWAR[1], **FATMA OUTAY**[2], **KASHIF NASEER QURESHI**[3], **SALEEM IQBAL**[4], **AND KAYHAN ZRAR GHAFOOR**[5]

[1]Faculty of Computer Science, German University of Technology (GuTech), Muscat 130, Oman
[2]College of Interdisciplinary Studies, Zayed University, Dubai, United Arab Emirates
[3]Department of Electronic and Computer Engineering, University of Limerick, Limerick, V94 T9PX Ireland
[4]Department of Computer Science, Allama Iqbal Open University (AIOU), Islamabad 44000, Pakistan
[5]Department of Computer Science, Knowledge University, University Park, Erbil 446015, Iraq

Corresponding author: Fatma Outay (fatma.outay@zu.ac.ae)

This work was supported by the College of Technical Innovation (CTI), Zayed University, Dubai, United Arab Emirates.

ABSTRACT The Internet of Things (IoT) is an emerging and groundbreaking technology in which devices, individuals, and processes seamlessly exchange substantial volume of data without causing disruption. This paradigm offers a wide range of services like healthcare, transportation, education, and smart home operations. However, owing to factors like deployment unpredictability, battery-operated nature, and the intricate nature of IoT networks, the energy levels of these diminutive sensor nodes are rapidly depleted, significantly curtailing the network's overall lifespan. Moreover, energy utilization and reputation assessment are pivotal in establishing dependability, reliability, and collaboration among sensor nodes, thereby profoundly influencing the decision-making framework. In response to these challenges, this paper introduces a State-based Energy Calculation Scheme (SECS) that leverages nodes' statuses and the functions encompassing direct and indirect energy utilization. The scheme identifies energy-depleted nodes, segregating them within the context of end-to-end reliable path selection, all while minimizing control broadcasts. Empirical results underscore the enhanced performance of the proposed scheme, as evidenced by augmented network throughput, elevated packet delivery ratios, diminished node energy utilization, and truncated end-to-end delays.

INDEX TERMS IoT, energy, lifetime, wireless sensor networks, throughput.

I. INTRODUCTION

Internet of Things (IoT) is an emerging and trending paradigm in the field of information and communications technology that gains popularity due to the combination of both intelligence and smartness autonomously, where a number of sensing devices integrate into various applications (e.g., smart cities, smart manufacturing, healthcare, transportation, and smart agriculture) and interact with each other [1]. These networks are made with Wireless Sensor Networks (WSN) for monitoring those areas where the physical presence of objects is difficult. Given the heterogeneous and complex environment, these networks are usually deployed randomly and without human intervention or physical protection in remote areas for longer durations to monitor the phenomenon and collaboratively collect the information, which is then sent back to the Base Station (BS) for further processing and decision-making [2]. However, the deployed sensor nodes are battery-operated and have constrained re-sources, energy, and compute power with unreliable communication over the broad-cast medium. The limited battery power of sensors is utilized during sensing and communication activities in the network. Besides, it is often difficult to change or re-place the batteries after their initial deployment, and such constraints have had a huge effect on the network's lifespan [3]. Despite the numerous benefits that the IoT offers, there are still a series of challenges that obstruct their operation, such as energy-depleted and malicious nodes, congestion, and security concerns that adversely impact network lifetime. However, limited energy sufficiency is the main constraint that impacts node operational capabilities and, thus, the gradual elimination of the overall lifetime.

The associate editor coordinating the review of this manuscript and approving it for publication was Bijoy Chand Chatterjee.

Therefore, a system for efficient energy conservation that assesses the node's energy level is needed. In sensor networks with limited resources, employing the sleep/awake technique could lower sensor nodes' power consumption and save energy [4], [5]. The process of consuming energy during communication is a general one; nodes with higher energy levels extend the network lifetime, whereas nodes with lower energy levels shorten it [6]. The energy of sensors is dissipated during the reception (Rx) and transmission (Tx) processes. Moreover, the radio transceivers consume a significant amount of computational power compared to any other component [7], [8], [9]. Be-sides, a node gathers and processes data that is related to its ambient conditions.

WSN is an important building block and a foundational technology where a wide variety of sophisticated sensors serve as the IoT's main building blocks, but limited re-sources, stability, and energy efficiency have not only challenged its vision but become a primary issue. Energy use is a crucial element that affects the network's ability to last for a long time [10]. An energy-efficient network not only improves the reliability of communication among nodes but also influences the overall performance of the network. As the performance of the application depends on the energy consumed by the sensor nodes, which are necessary for a variety of applications to operate efficiently and for longer periods of time (such as border surveillance, health monitoring, environment control, and protection) [11]. However, malicious energy drain nodes can impair the device's performance and accuracy in processing data. Although there are various solutions [12] in place to extend the network lifetime and reliability, including clustering [13], selection of routing protocols [14], scheduling such as Time Division Multiple Access (TDMA), and sleep/wake strategies [15], which improve communication and preserve node residual energy level [16], [17], these solutions can work well up to a certain extent, but due to the limited constraints of nodes, efficient energy management is more desired in sensor based networks.

In this paper, we propose a State-based Energy Calculation Scheme (SECS) by virtue of using the node's behavioral aspects, such as sleep and wake, which limit control messages and consequently reduce the communication cost. Moreover, the identification of energy-depleted malicious nodes helps prolong the network's lifetime. To maintain an energy-efficient network environment, it is mandatory that every subject node have the minimum required energy level to remain as recommended for communication. This approach involves each node assessing the state and energy level of neighboring nodes through energy computation and then making decisions about whether nodes should be recommended through the integration of cumulative decisions and threshold value assessment. The use of direct and indirect energy evaluation provides a cumulative value for energy, which is then compared against a predefined threshold to determine whether the node should be recommended for communication. The node's reputation repository is maintained at the Cluster Head (CH) to lessen the impact of erroneous assessments and dishonest suggestions when calculating the direct and indirect energy levels of nodes. To minimize the number of dishonest recommendations from neighboring nodes, uniform weights are assigned to both direct and indirect energy values. Node with negative reputation received from its neighboring node it weight is decreased by half and the left-over weights are uniformly assigned to the remaining neighbors. However, in a case where the negative reputation of a neigh-boring sensor node reaches a predefined threshold value three times consecutively, the weight of the neighboring node is set to zero and not recommended for communication. These uniform weights are maintained in the reputation repository and then compared against the threshold values. This evaluation cycle continues until a subjective node finds an energy-efficient node for data forwarding. Existing energy-based mechanisms improve node energy levels through clustering, duty-cycling, and cross-layer solutions that incur higher overhead and increase communication costs [18], [19], [20], [21]. It is also important to consider that malicious and energy-depleted node could be selected as CH by periodically sending false information, enabling them to display a higher energy level to other nodes [22], [23]. In essence, the management of energy resources and the evaluation of reputation among sensor nodes are cornerstones that underpin the stability, reliability, and functionality of IoT networks. These aspects not only impact the technical performance of the network but also have far-reaching implications for the user experience, operational efficiency, and the realization of the IoT's transformative potential across various domains. To counter this kind of challenges and false reporting, SECS uses behavioral aspects using both direct and indirect methods so that the node's energy level can be calculated without incurring additional communication costs and overhead.

The proposed SECS scheme aims to improve communication between nodes and extend the network lifetime by analyzing node energy levels directly and indirectly, which helps in detecting energy-exhausted nodes. By keeping this motivation in mind, the key contributions of this study are, in essence, as follows:

- By utilizing the node's behavioral aspects (using the sleep/wake strategy), reduces the communication cost and improves the network's lifetime.
- During the routing process, evaluating the nodes' direct and indirect energy levels helps to avoid making false recommendations.
- Evaluation of the node's remaining energy level motivates the nodes to maintain their reliability, since if they don't, they will be identified as malicious nodes and therefore isolated and not recommended for communication.
- The effectiveness of SECS is evaluated by considering various performance metrics, and the efficacy of the

proposed approach is compared to numerous widely used techniques.

The remainder of the paper is organized as follows: The main energy evaluation methods and schemes that have been presented in this field are covered in Section II. The concept of the suggested SECS scheme is presented in Section III, and its implementation is covered in Section IV. Section V discusses simulations and experimental findings. The paper concludes in Section VI.

II. RELATED WORKS

Within this section, we provide a succinct analysis of various energy conservation schemes in IoT-based WSNs. Prolonging the network's lifetime has always been an is-sue of concern in the IoT. These networks' sensor nodes are subject to energy and computational limitations. Therefore, securing the node's energy level is a demanding and challenging task. In addition, to transmit the sensory information to the base station, multiple pieces of information are required to flow from the participating nodes. Because of that, there is a higher probability of data redundancy, which results in excessive energy consumption and inefficient resource management. Consequently, during the data dissemination process, the selection of an appropriate node with sufficient energy levels is required toward the destination. This has an impact on the net-work's lifetime and data delivery performance.

Recently, authors in [24], developed the Energy Balancing and Optimal Routing-Based Secure Data Transmission (EBORDT) protocol designed to extend the net-work's life. In the proposed protocol, a density-aware clustering mechanism is deployed, which ensures the reliable transmission of data. Moreover, to enhance the network lifetime, an Ant Colony Optimization (ACO) technique is incorporated, which selects the optimal head of the cluster. Furthermore, reliability, bandwidth, and energy parameters are also considered in the selection of the optimum path. A Dynamic Multi-hop Energy Efficient Routing Protocol (DMEERP) is proposed in [25] for maximizing energy efficiency in cluster-based networks. DMEERP balances the path reliability ratio and energy consumption of the nodes. Moreover, the proposed scheme is divided into three phases, where a cluster is formed in the first phase and then a supercluster head (SCH) is selected to maintain the cluster and member node information based on a weight factor. Similarly, the path reliability ratio is estimated in the second phase, while the energy and channel capacity models are implemented in the last phase. Although the use of clustering and the selection of superclusters enables the method to preserve some energy, it incurs higher overhead due to frequent exchanges of control messages.

In another work [26], an Energy-Proficient Hybrid Secure Scheme (EPHSS) was suggested that provides secure and energy-efficient data transfer in the Internet of Things using clustering, which efficiently manages the node's energy level during communication. Besides, security is provided using Elliptical Curve Cryptography (ECC), where graded coprime keys are generated and assigned to each node for validation. Although the proposed scheme improves the security measures, it increases energy consumption, which reduces the network's lifetime. The authors in [27], proposed Efficient Dynamic Authentication and Key Management (EDAK), a protocol for a variety of WSNs that transfers data securely between the base station and nodes. The proposed protocol uses a dynamic mechanism called the dynamic matrix key in the identification of node energy levels and isolates the other nodes. This method provides faster communication with reduced complexity but increases network overhead and end-to-end transmission delay.

In a similar vein, the authors in [28] suggest an Adoption Broadcast Radius-based Code Dissemination (ABRCD) method for the IoT that improves energy efficiency with reduced delay and enhanced duty cycle. The proposed scheme uses a larger broadcast area with more energy so that the deployed program codes can reach the edges of the network with a lesser number of broadcasts. Besides, the ABRCD is based on the code dispersal approach with a different broadcast radius, which balances energy usage and improves the network lifetime. In this scheme, a tree-structure-based network is deployed where a sink node is used as the main contact point for code diffusion. The sink node, acting as a parent node, will send the data to a child node, which wakes up and acknowledges the parent node. If this process fails, then the sink (parent) node will send the data again in the next duty cycle. This will be repeated until the data reaches its destination. Not only can the nodes receive the data in their active time slot, but they can also transmit the data in any of the available wake time slots. However, the proposed ABRCD remains vulnerable to higher energy consumption due to unnecessary message broadcasts, which increase network overhead and delay.

In [29], the authors suggested a unique Distributed Energy-efficient Adaptive Clustering Protocol (DEACP) for load balancing with data gathering capabilities. The proposed protocol uses a key queue overflow strategy between cluster heads and nodes, which not only reduces the packet-dropping probability but also consumes less energy. Additionally, node sleep scheduling is set up to disable the radio module of the node, extending the lifetime of the network. The authors in [30], proposed an Energy-Efficient Broadcasting (EeB) scheme for smart industrial wireless sensor networks. The suggested scheme's methodology is based on a configurable broadcasting radius that is propagated to other nodes by a sink node to increase performance and reliability. In addition, the proposed scheme can handle the energy hole phenomenon using an adjustable radius. Moreover, it uses energy in accordance with the node's remaining energy level. Although the proposed scheme can conserve the energy of the node up to a certain extent, the continued transmission and monitoring mode decreases the net-work's performance and lowers its lifetime.

In another paper [31], an Imperialist Completion-based Algorithm (ICA) is suggested as a strategy for extending a network's lifespan. Initially, the ICA algorithm is used for setting up the clusters using essential parameters, where the energy level of the node is taken into account. Also, the cluster head maintains the node energy consumption uniformly and performs the compression operation. In a similar vein, the authors in [32] proposed an Attack-Resistant Power Management (A-RPM) structure that preserves the energy between deployed sensor nodes and lengthens the lifetime of the network. The working mechanism of the proposed scheme is based on a sleep mode where each node turns on periodically and participates in the communication process. A-RPM efficiently decreases energy use and lengthens the life of the network. The simulation results demonstrate the scheme's effectiveness in comparison with other methods.

In order to increase the lifetime and data delivery performance of cluster-ing-based WSNs, a Fault-Tolerant Energy-Efficient Clustering (FT-EEC) protocol was presented in [33] that seeks to enhance the performance of data delivery and lifetime. The network is initially partitioned into a number of remote clusters, and the CH is chosen from among the nodes with the highest energy level. Additionally, CH must compile the data gathered from other non-CH nodes before sending it to BS. The pro-posed protocol preserves the node's energy level through the implementation of a sleep/wake mechanism where the sleeping node is given higher priority due to its available residual energy and the number of sleep rounds. Despite the fact that the proposed protocol increases the network's lifespan effectiveness, it ignores incorporating the communication cost. This incurs an additional overhead for the network due to the excessive broadcast of energy status frames from CH.

An efficient energy-aware framework was presented in [34] for the IoT, which aims to lower energy consumption and prolong the network lifetime. The proposed framework consists of three main components: network architecture, inter-cluster communication protocol, and a deployment planner using square and hexagonal grid-based deployment. The implemented algorithm conducts the overall analysis of WSNs and efficiently manages the node sleep and wake schedule, which increases the data flow when the transmission becomes unreliable. Although the proposed frame-work reduces energy consumption through the sleep/wake mechanism, the propagation of data packets to all the deployed nodes requires a longer time, which is a major constraint of the proposed framework.

Trustworthiness management, energy management, and physical-aware coalition formation for smart IoT applications were proposed in [39], which addresses the issue of uncertainty and suggests various strategies in order to establish trustworthiness among the nodes and to identify and isolate the malicious nodes hampering the net-work lifetime. Authors in [40], proposed a dynamic hierarchical energy-efficient solution for WSN networks. This protocol designed based on combinatorial optimization method to balance the energy consumption of sensor nodes and improve the energy level of network. However, this solution is purely tackled the energy without any security and trust aspect. Another study [41], discussed the multi-objectives optimization solutions for WSN networks. Multi-objective optimization is used in this research. Although this paper elaborated many existing solutions, open challenges and future direction but not considered the trust and nodes reliability issues in network. Authors in [42], proposed an algorithm by using machine learning and genetic algorithm. Multi-objective optimization model is developed to address the energy hole based clustering issue of the network. This solution is evaluated with other existing solutions and improved the complexity issue. However, the node behavior analysis is one of the significant factor for overall network performance.

The energy consumption of a node in its active working state without data reception and transmission is critical for the longevity of the network. To increase the lifespan of the network, it is crucial to develop effective energy-saving and assessment techniques for sensor nodes. Developing energy conservation schemes to prolong the network lifetime in resource-constrained wireless sensor networks is still a big challenge. This is even more critical in applications where the sensors are unattended with a limited power supply. Existing solutions like clustering, scheduling using Time Division Multiple Access (TDMA), and sleep/aware mechanisms can conserve the node's energy level up to a certain level. However, periodic re-evaluation of node energy levels minimizes delay and overhead while increasing throughput and network longevity. As IoT systems become more widespread and interconnected, managing computational complexity becomes essential for ensuring efficient, responsive, and reliable operations. Addressing computational complexity involves optimizing algorithms, using efficient data structures, leveraging distributed computing strategies, and sometimes offloading tasks to more powerful computing resources in the cloud. Balancing computational demands with the capabilities of IoT devices is crucial to achieving the desired performance and functionality in IoT applications. The proposed SCES overcomes the issues by incorporating and evaluating the node's direct and indirect energy while isolating the energy-exhausted nodes.

III. PROPOSED SCHEME

Energy conservation is an essential ingredient for sensor nodes. However, the various restricted constraints, computational capabilities, storage, memory, and energy depletion during data gathering impose challenges to the network. The primary goal of the suggested research is to create an energy-efficient scheme that evaluates node energy levels and protects the network from malicious and energy-depleted nodes. Fig. 1 depicts the design of a state-based energy calculation scheme.

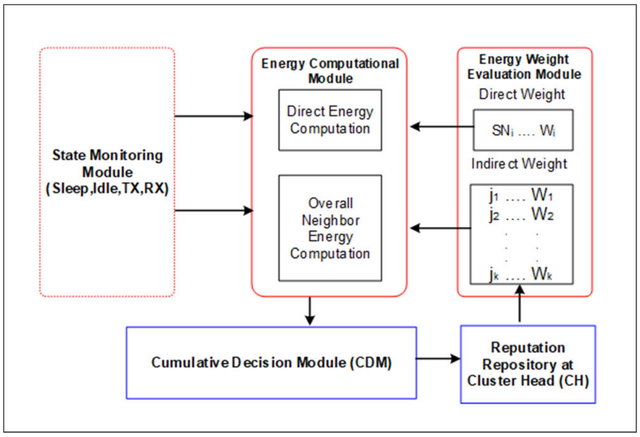

State Monitoring Module (Sleep,Idle,TX,RX)
Energy Computational Module
Direct Energy Computation
Overall Neighbor Energy Computation
Energy Weight Evaluation Module
Direct Weight
SN$_i$ .... W$_i$
Indirect Weight
j$_1$ .... W$_1$
j$_2$ .... W$_2$
j$_k$ .... W$_k$
Cumulative Decision Module (CDM)
Reputation Repository at Cluster Head (CH)

FIGURE 1. Block diagram of SECS scheme.

TABLE 1. List of notations.

Notations	Definitions
CH	Cluster Head
SNi	Current state of sensor node as input
Dei	Direct energy
IDEi-j	Indirect energy
CEi	Cumulative energy
IdWi	Indirect weight
Ei	Energy value
CIDEi	Cumulative indirect energy value
TEi	Total energy
INi	Immediate neighbor
RIN	Reputed Immediate neighbor
Th	Threshold value
TI	Time interval
PREQ	Route Request
PREP	Route Response
PERR	Route Error
ESI	Energy Status Index
CIDE	Cumulative Indirect Energy Value
W	weight
Tx	Transmit
Rx	Receive

SECS consists of five modules which are: state monitoring module, energy computational module, energy weight evaluation module, cumulative decision module, and reputation repository. Table 1 illustrates the list of notations used in the SECS.

A. NETWORK ASSUMPTIONS

Before discussing the proposed SECS, some network assumptions are highlighted as follows:

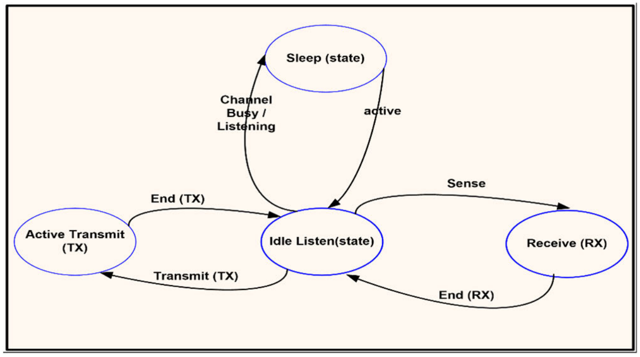


FIGURE 2. Node states.

- Nodes are deployed at random, are immobile, and communicate via a common wireless channel in both directions while within their communication range.
- Nodes cannot be added or deleted after being deployed, and once their initial energy has been used up, they cannot be recharged.
- Each node has identical initial energy, storage, computing, and communication capacities and is isomorphic.
- The reputation repository is maintained at the Cluster Head (CH) to archive the information.

The following subsections present details about each module of the proposed SECS scheme.

B. STATE MONITORING MODULE

A sensor node in a network usually performs a variety of operations, such as sensing data, routing, and reporting. In contrast to sensing and data processing, sending and receiving data consume almost all of the node's energy [35]. As shown in Figure 1, the state monitoring module observes node states such as sleep, idle or active, receive (Rx), and transmit (Tx) to preserve energy. Active nodes are those nodes that are currently interacting with other neighboring nodes, while sleeping or inactive nodes are those nodes that are not currently participating in the communication and are in an idle state. The various states of nodes are shown in Fig. 2.

As depicted in Figure 2, the various behavioral states of sensor nodes help in energy conservation through switching between transmit (Tx), receive (Rx), idle, and sleep states to ensure the efficient control of transmission power, node energy consumption, and efficient routing. The sensor node remains in the listening state, sometimes referred to as the idle state, when there is no event. The node changes from listening mode to transmission mode when an event happens, then back to listening mode after the event is over. Similarly, the node changes its mode to receiving mode if any of its neighboring nodes sends a data packet, and after forwarding the message, the node returns to an idle state. Also, if there is no activity in the network, to save energy, the node enters sleep mode.

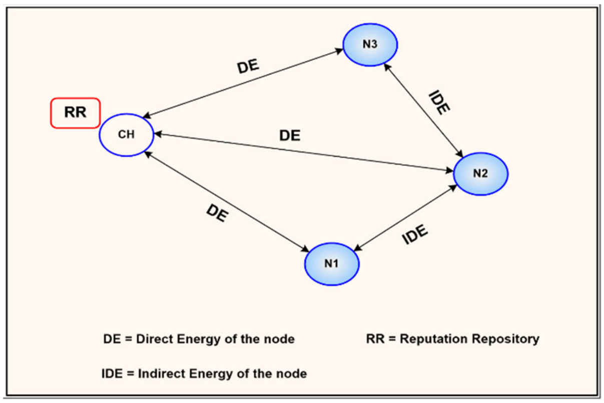

RR
CH
N1
N2
N3
DE
DE
DE
IDE
IDE
DE = Direct Energy of the node
RR = Reputation Repository
IDE = Indirect Energy of the node

FIGURE 3. SECS – Network Topology Scenario.

C. ENERGY COMPUTATIONAL MODULE

Like the state monitoring module, the energy computational module is responsible for calculating the node's energy level. This module calculates both the direct and indirect energy levels of a sensor node. While the neighbors of the candidate sensor node calculate the indirect energy, the cluster head independently estimates the direct energy of the node. This information is conveyed to the cluster head as presented in Fig. 3.

The cluster head maintains the node energy information in the reputation repository. The cluster head determines the node's direct energy, while the sensor node's indirect energy comes from its nearby nodes (N1, N2, and N3) in the form of recommendations. Recommendation means the node has an energy level above the defined threshold (0.5) and is trustworthy for communication since this information is maintained at Cluster Head (CH). Therefore, the cluster head has access to both direct and indirect energy levels. The mathematical representation of the direct energy level of the node is given in Equation 1.

$$\mathrm{DE_i} = \mathrm{E_i X DW_i} \tag{1}$$

where, DE_i is the direct energy of sensor node 'i' calculated by the cluster head node, whereas E_i is the energy of a sensor node 'i' and DW_i is the weight assigned to that sensor node 'i'. Similarly, the cumulative indirect energy value (CIDEi) of sensor node 'i' is calculated by all the neighbor nodes of 'i', the neighbors being represented with 'j'. Equation. 2, represents the cumulative indirect energy calculation, where IdEi−j is the indirect energy of the node 'i' calculated by node 'j' and IdWj is the weight assigned to sensor node 'j'.

$$\mathrm{CIDE_i} \sum\nolimits_{j=0}^{k} \mathrm{IdE_{i-j} x IdW_j} \tag{2}$$

The value of weight (W) for energy calculation is set to 1, where half (0.5) of the weight is reserved for direct energy calculation and is represented as $\mathrm{DE_i}$, whereas the remaining half (0.5), which is represented as, $\mathrm{IdW_j}$ is used for the neighbor nodes of the sensor node under consideration. However, the distribution of weights among neighbors may not be uniform, as it depends on the reputation of those neighbors. The total energy ($\mathrm{TE_i}$) obtained directly or indirectly is used jointly to assess whether the node is recommended for communication. Mathematically, it is represented in Equation 3.

$$\mathrm{TE_i} = \mathrm{DE_i} + \mathrm{CIDEv_i} \tag{3}$$

D. ENERGY WEIGHT EVALUATION MODULE

The energy weight evaluation module evaluates both the direct and indirect energy levels of a sensor node. The CH determines the direct energy, whereas the sensor node's indirect energy comes from the nearby nodes in the form of a recommendation for the particular node. The CH maintains the reputation repository and stores all the necessary information regarding the node's energy levels. In this research, the reputation of the neighboring sensor node depends on the number of times it has been identified as unrecommended. On each occurrence of negative repute for this neighbor, its weight is decreased by half, and the left-over weights are uniformly assigned to the remaining neighbors. However, in a case where the negative reputation of a neighboring sensor node reaches a predefined threshold value three times consecutively, the weight of the neighboring node is set to zero.

E. CUMULATIVE DECISION MODULE

This module determines whether a sensor node is recommended or not. This decision is based on comparing the node's total energy level with the threshold value, which is 0.5. Based on this threshold, the node is identified as recommended or not recommended for communication.

F. REPUTATION REPOSITORY

The reputation repository is maintained at the CH level to archive the information (recommended or not recommended) received from the cumulative decision module. This repository helps determine the reputation of the neighboring node. This reputation is used in assigning weights to the neighboring nodes while calculating the indirect energy level of the node. Hence, the nodes that have a bad reputation will not be assigned any weights at all. Hence, the nodes that have a bad reputation will not be assigned any weights at all. This strategy reduces the information overhead, system complexity and communication cost.

G. AODV PROTOCOL

The Ad-hoc On-Demand Distance Vector (AODV) is one of the main routing protocols in WSN due to its on-demand and reactive nature. The working mechanism of AODV is based on the concept of a routing table, where each node in the network maintains its own routing table, which consists of route information from source to destination along with distance to other nodes [43]. AODV uses control packets of Route Request (PREQ), Route Response (PREP), and Route

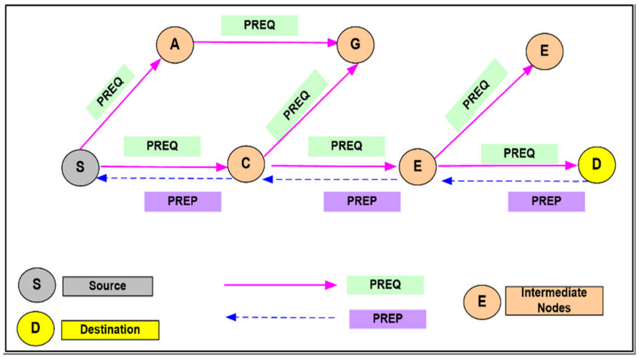
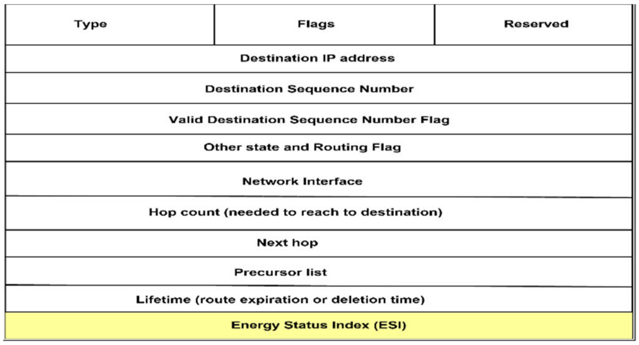


FIGURE 4. Routing process in AODV protocol.



Type	Flags	Reserved
Destination IP address		
Destination Sequence Number		
Valid Destination Sequence Number Flag		
Other state and Routing Flag		
Network Interface		
Hop count (needed to reach to destination)		
Next hop		
Precursor list		
Lifetime (route expiration or deletion time)		
Energy Status Index (ESI)		

FIGURE 5. SECS version of AODV with Energy Status Index field.

Error (RERR) to determine the feasible route. The routing process of AODV is depicted in Fig. 4.

In the route discovery process, the source node broadcasts the PREQ packet to its neighboring node, whereas each of the neighboring nodes maintains an active route between the source and the destination in its routing table and notifies the source node by sending the PREP packet. Alternatively, each node broadcasts the PREQ packet to its neighbors. This process is repeated until the PREQ reaches the destination or an intermediate node of an active route to the destination with a sequence number greater than or equal to the PREQ sequence. After completing the PREQ broadcast step, the PREP is sent from the destination node in the reverse routing of the intermediate nodes to the source node. However, when a node loses connectivity to its next hop, it invalidates its route by sending PERR to all nodes that could potentially receive its PREP. Similarly, in the maintenance process, each node can inform its neighboring node using a broadcast, also known as Hello packets, as all message exchanges among the nodes are in the form of hello or control data packets.

During the route request whenever the source node finds a route to new destination it broadcasts PREQ. SECS modifies the default AODV protocol by including the additional one-bit field known as Energy Status Index (ESI), in PREQ packet to carry ESI information as shown in Fig. 5. ES maintains the energy status of node and share this information with the neighboring nodes.

IV. IMPLEMENTATION OF PROPOSED SCHEME

Algorithms 1 and 2 were used for the calculation of node energy and weight, respectively. Algorithm 1 takes the current state of a sensor node (SNi) as input, whereas the second input parameter is the Time Interval (TI). The change of mode for any sensor node depends on the application or domain in which the wireless sensor networks are deployed. However, this switching of the mode is mostly periodic; in our experiments, a 40-second interval was considered [36], [37]. This periodic value is also used to determine the state mode of the respective sensor node. In Algorithm 1, the direct energy is evaluated from lines 1 to 6, whereas lines 8 to 16 evaluate the indirect energy of the node. For direct energy, the state is evaluated in line 1 of the algorithm. A sensor node's initial energy value (Ei) is set to one, provided that the state of the sensor node lies in multiples of a given periodic interval. Otherwise, Ei is set to zero to represent the irregularities in the modes of those sensor nodes. In this research, these irregularities represent the untruthful behavior of the sensor node. The irregularities may have some other reasons, such as the node being under malicious attack; however, these are not within the scope of current research. The subsequent step is to multiply Ei by the corresponding energy weight (Wi), which Algorithm 2 has calculated. In lines 8-15, the energy value of the sensor node (SNi) is also obtained from its immediate neighbors. Like direct energy, indirect energy estimation is multiplied by their respective weights, as shown in line 16 of the algorithm. In the next line, the overall neighbor energy value (CIDEi) is obtained by summing up all the individual neighbor energy values (NEi). The direct and indirect energy levels are then combined in line 18 to obtain the cumulative energy value (CEi). In lines 19-25, the CEi-j is assessed in comparison to the set threshold value (Th) to identify the sensor node as recommended or not recommended for communication. This recommendation is then saved in the repository to obtain the reputation of any sensor nodes, which is required in Algorithm 2 for the calculation of the weights.

Similarly, Algorithm 2 (Weight Calculation) dynamically calculates the weight required as input in Algorithm 1. Algorithm 2 takes two parameters as input, which are:

- The number of immediate neighbors (INi) of SNi
- Their respective reputation values (RPi)

In this research, the weight values range from 0 to 1, and both the direct (DW) and indirect (IdW) weights are set to exactly half, forming a total of 1. At the initialization of the experiment, there is no reputation available in the repository; therefore, in this phase, the (IdW) is uniformly distributed among the Immediate Neighbors (IN). However, afterward, the IdW is recalculated based on the reputation of the neighbors. Therefore, rather than uniformly distributing the weight among the neighbors, it is allocated among the reputed neighbors only. This reputation is obtained from Algorithm 1. Lines 8-13 of Algorithm 2 record the number

Algorithm 1 Energy Calculation

Input: Current State of Sensor Node CS(SNi), Timer Interval (TI), Weight (W)
Output: Decision of SN recommendation

```
1:   If CS(SNi) is Wake
2:   If CurrentTime is multiple of TI (SNi)
3:   Ei = 1 // Energy Value (Ei)of SNi
4:   Else
5:   Ei = 0
6:   end if
7:   end if
8:   DEi = Wi × Ei // Direct Energy (DEi) of SNi
9:   CIDEi = 0 // initialization of all neighbor's energy
      value of
                 //Sensor Node i (SNi) calculated from
      neighbor Node j (SNj)
10:    for each neighbor SNj of SNi
11:    {
12:    if CS(SNi-j) is Wake
13:    if CurrentTime is multiple of TI(SNi)
14:    IdEi-j = 1 // Indirect Energy (Evi)of SNi
      //calculated from SNj
15:    Else
16:    IdEi-j = 0
17:    end if
18:    end if
19:    NEi-i = IdEi-j × Wi-j // Neighbor Energy (NE) of SNi
20:    CIDEi-j = CIDEi-j + NEi-i
21:    }
22:    TEi = DEi + CIDEi // Total Energy (TEi) of SNi
23:    if TEi > Th
24:    mark SNi as recommended
25:    save its reputation
26:    Else
27:    mark SNi as un-recommended
28:    save its reputation
29:    end if
```

Algorithm 2 Weight Calculation

Input: Number of immediate neighbors of SNi (INi), Reputation of immediate neighbors of SNi (RPi-j)
Output: Energy Weight

```
1:   DWi = 0.5
2:   IdWi = 0.5
      Network Startup
3:   for (j = 0; j < INj ; j++)
4:   {
5:   IdWi-j = IdWi / INi
6:   }
      Afterwards
7:   RIN = 0 // initialization of Reputed Immediate
      Neighbors (RIN)
8:   for (j = 0; j < INj ; j++)
9:   {
10:    if RPi-j is recommended
11:    Increment RIN
12:    end if
13:    }
14:    for (j = 0; j < RINj ; j++)
15:    {
16:    IdWi-j = IdWi /RIN
17:    }
```

of Reputed Immediate Neighbors (RIN) that are initialized on line 7. Fig. 6 displays the proposed SECS flowchart.

Thereafter, the weight is uniformly distributed among these reputed immediate neighbors, as shown on lines 14 to 17 of the algorithm.

The steps of the algorithm are as follows:

- **Step 1:** The CH gets the node state value from its neighbors, both directly and indirectly.
- **Step 2:** The cumulative energy value of the questioned node is determined using its direct, indirect, and weight values.
- **Step 3:** Communication is recommended if the node's total cumulative energy value is above the threshold.
- **Step 4:** The node reputation is updated.
- **Step 5:** The reputation repository at CH is updated accordingly.

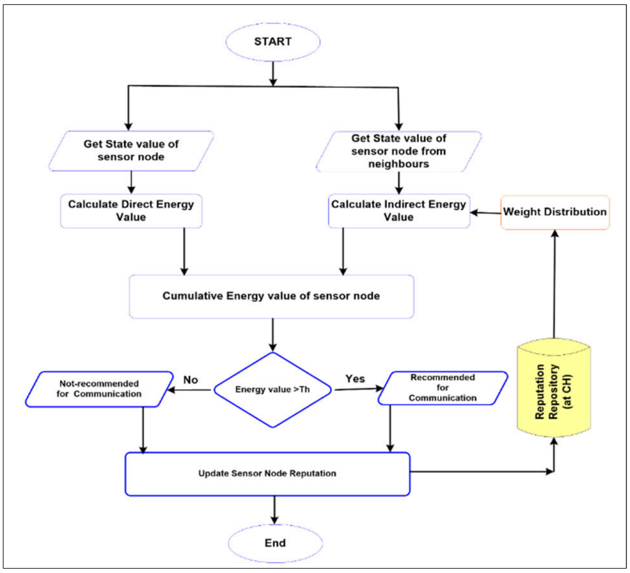

START
Get State value of sensor node
Get State value of sensor node from neighbours
Calculate Direct Energy Value
Calculate Indirect Energy Value
Weight Distribution
Cumulative Energy value of sensor node
Reputation Repository (at CH)
Not-recommended for Communication
No
Energy value >Th
Yes
Recommended for Communication
Update Sensor Node Reputation
End

FIGURE 6. Flow diagram of the proposed SECS.

V. RESULTS AND DISCUSSION

The SECS is implemented in the discrete event simulator OMNET++, which has a graphical user interface. Also, it deals with the modeling of traffic, protocols, queuing, and various hardware and complex software-based networks and systems. The sensor nodes are randomly placed in a 100 m by 100 m field. The starting energy, processing, and storage capacities of the sink and sensor nodes are equivalent. For various experiments, the simulation time varies between

TABLE 2. Parameters for simulation.

Parameters	Value
Area	100m x 100m
Placement of nodes	Random
Simulated period	200 – 1000 seconds
Traffic pattern	UDP
Packet size	50 Bytes
Physical requirement	IEEE 802.15.4
Traffic volume	CBR
No. of nodes	10 – 50
Queue type	Drop tail
Routing protocol	AODV
ESI	1 bit

200 and 1000 seconds. The traffic flow on the network is of the constant bit rate (CBR) type, and the packet size is set to 50 bytes. The Ad-hoc On-Demand Distance Vector Routing (AODV) routing protocol is regarded as a basic routing protocol because of its reactive and on-demand characteristics. Table 2 displays SECS's simulation options.

Additionally, the proposed technique is evaluated in a simulator using the set of performance parameters listed below:

Impact of Residual Energy (RE): Between the node's initial and final energy levels, there is an average difference called residual energy. The increased use of residual energy shortens the lifespan of the network.

Impact of Communication Cost (CC): The term ''communication cost'' refers to the typical energy usage during data packet transmission. The energy level of a node is quickly depleted by false reporting or the presence of malicious nodes, which shortens the network's lifetime. The overhead and computational cost are directly linked with communication cost because information overhead represents the extra data or metadata associated with the communication process due to any malicious activity in the network. Whereas the computational complexity refers to the computational resources needed to solve a problem or perform an algorithm and linked with all performance parameters. All three factors play a role in evaluating the performance, efficiency, and scalability of systems and algorithms.

Packet Delivery Ratio (PDR): When compared to the total number of transmitted packets that are expected to reach the recipient, this metric shows how many packets are successfully received. The average packet delivery ratio is the sum of all the receivers' ratios for packet delivery.

Impact of Average Network Throughput: The average throughput, which is a network performance indicator, is the sum of the data (measured in bits) received by the receiver and the total time (the period between the first and last packets received). Bits per second (bps) is the unit used to measure network throughput.

End-to-End Delay Analysis: The end-to-end delay metric measures how long it takes a data packet to travel across a network, taking into account both the time it takes for the packet to leave its origin and arrive at its destination as well as any delay caused by a cache used to build the route, queue waiting, and MAC layer relay time. The performance of the network is improved by reducing the end-to-end delay.

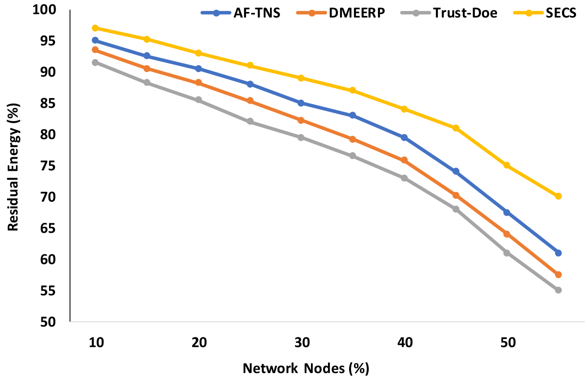


FIGURE 7. Energy consumption comparison.

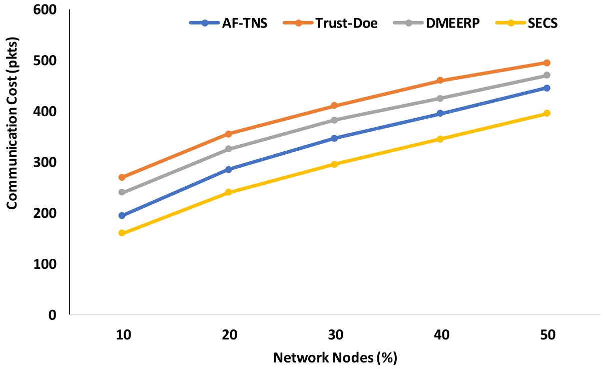


FIGURE 8. Communication cost comparison.

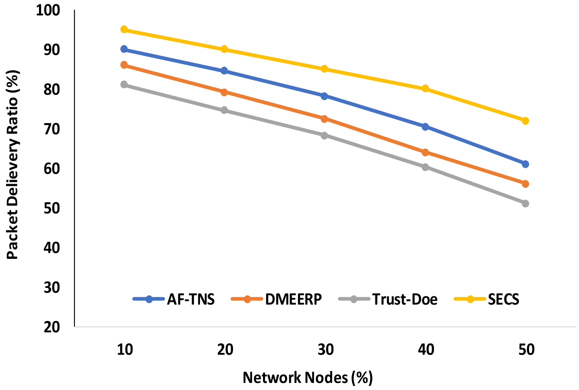


FIGURE 9. Packet delivery ratio.

A. IMPACT OF RESIDUAL ENERGY

Since a node's ability to survive and complete a task on time is directly tied to its residual energy, that node's residual energy is assessed in the first set of experiments. The node's energy usage affects how long the network will last. The network's lifespan decreases with increasing energy use. The average energy consumption of nodes in the proposed SECS is shown

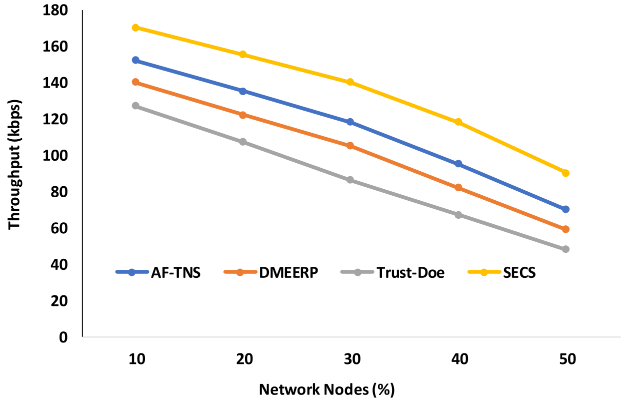


FIGURE 10. Average network throughput.

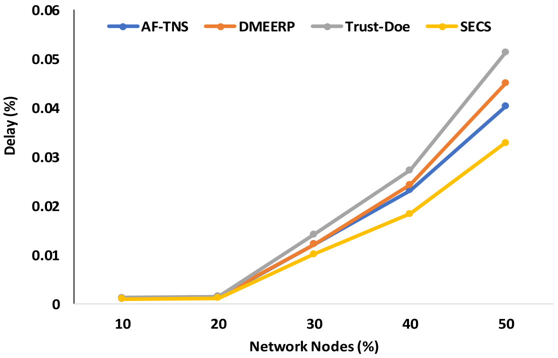


FIGURE 11. End-to-end delay.

in Figure 7, shows how much energy each node in the proposed SECS uses on average. This is compared with an activation function-based trusted neighbor selection (AF-TNS) [22], a dynamic multi-hop energy-efficient routing protocol (DMEERP) [25], and a trust model of dynamic optimization based on the entropy technique (Trust-Doe) [23]. Unlike other schemes, the SECS preserves better energy levels through the selection of trustworthy and energy-conserving nodes in its design and by keeping track of the nodes' remaining energy levels. In comparison to AF-TNS, DMEERP, and Trust-Doe, SECS conserves energy by 27.18%, 25.26%, and 13.30%, respectively. This is because it takes into account node behavioral aspects like sleep and wake states, propagates fewer control packets, and takes into account the node energy level, which reduces overhead and lengthens network lifetime.

B. IMPACT OF COMMUNICATION COST

In the second scenario, the proposed SECS's communication costs are assessed. The quantity of control packets exchanged between nodes and the energy expended when transmitting packets are referred to as the "communication cost" [38]. The communication cost is conventionally an important component of the operational costs in sensor networks due to its effect on the node residual energy level and the detection time [39].

If malicious or low-energy nodes remain undetected for a long time, they can perform malicious activity through false reporting or by dropping packets, which reduces the network's lifetime. Figure 8 depicts the communication cost graph for all schemes with node counts ranging between 10% and 50%. The performance of SECS is better with lower communication costs than the other schemes. This is due to its selection of energy-aware nodes, while the other schemes incur higher communication costs due to the frequent exchange of control messages, false reporting, and a lower capability in the detection of malicious and energy-depleted nodes. Hence, they generate more traffic overhead, which increases the computational cost and shortens the network lifetime. Comparatively, SECS exhibits low communication costs of 27.59%, 25.16%, and 23.01%, compared to AF-TNS [22], DMEERP [25], and Trust-Doe [23], respectively.

C. IMPACT OF PACKET DELIVERY RATIO

The third set of analyses examined the impact of the packet delivery ratio (PDR) metric. The average number of successfully sent packets from the source to the destination node is calculated using the packet delivery ratio. Moreover, the packet delivery ratio (PDR) shows whether the ability and performance of the proposed protocol are affected due to the inclusion of malicious and energy-depleted nodes. Fig. 9 represents a plot of the packet delivery ratio (PDR). The graph represents that when there is a smaller number of nodes in the network (e.g., 10%), almost all three approaches behave similarly and yield a packet delivery ratio (PDR) between 80% and 95%. However, when the number of nodes increases (20%–50%), the nodes start depleting the energy level and dropping the packets. The performance of SECS is still better due to its ability to identify energy-depleted nodes, thus avoiding them in the selection of the end-to-end path. The average packet delivery ratio (PDR) achieved by SECS, AF-TNS [22], DMEERP [25], and Trust-Doe [23] is 82.44%, 78.65%, 74.75%, and 66.76%, respectively.

D. IMPACT OF AVERAGE NETWORK THROUGHPUT

By displaying the network with energy-depleted nodes, this experiment examines the impact on throughput. The main objective of this experiment is to confirm the optimal performance of the proposed SECS. Fig. 10 shows the comparison of average network throughput. The graph shows that the proposed SECS offers a higher throughput when there are 10% energy-depleted nodes as compared to AF-TNS [22], DMEERP [25], and Trust-Doe [23]. Similarly, when the ratio of the energy-depleted nodes increases to 20%–50%, the throughput of our proposed method is still higher than AF-TNS, DMEERP, and Trust-Doe due to the exclusion of energy-exhausted nodes. However, with the increase of energy-depleted nodes up to 50%, a throughput decrease is witnessed, but the SECS still achieved a considerably higher throughput than AF-TNS, DMEERP, and Trust-Doe. The consistency in consideration of node energy level evaluation

TABLE 3. Performance comparison.

Parameters	Value				
Scheme / Technique	Residual Energy (%)	Communication Cost (pkts)	Packet Delivery Ratio (%)	Network Throughput (kbps)	End-to-End delay (s)
AF-TNS	89	495	81	127	0.41
DMEERP	92	470	86	140	0.39
Trust-Doe	95	445	90	152	0.35
SECS	97	395	95	170	0.21

accommodates seamless transmission and retention of the throughput of the network by constructing stable routes. As a result, SECS's average throughput is 25.69%, 30.68%, and 38.06% greater than those of AF-TNS, DMEERP, and Trust-Doe, respectively.

E. END-TO-END DELAY ANALYSIS

The typical network delay is examined in this case. This metric's primary goal is to investigate the impact of malicious and energy-starved nodes. A range of packets transmitted per second was utilized to calculate the overall time (in seconds), taking into account the data queue and route discovery process delays. The graph in Fig. 11 depicts the degree of performance comparison. It is observed that SECS, AF-TNS [22], and DMEERP [25] encounter almost similar delay levels when the total number of nodes is 10%. However, when the number of nodes increases to 20% and onward, the delay between both starts increasing, whereas SECS behaves slightly differently from the other three schemes (AF-TNS, DMEERP, and Trust-Doe).

The performance comparison of SECS is done with related work such as AF-TNS [22], DMEERP [25], and Trust-Doe [23], which are summarized in Table 3.

From Table 3, it can be observed that the overall performance of the proposed SECS is better when compared with AF-TNS [22], DMEERP [25], and Trust-Doe [23], which is due to the use of node behavioral aspects and hence increased network lifetime with enhanced throughput and packet delivery rates, while lowering latency.

VI. CONCLUSION AND FUTURE WORK

Energy efficiency is highly desirable and an important ingredient in resource-constrained IoT. The use of energy-efficient methods not only extends the life of the network but also improves its reliability. In this research, a state-based energy calculation scheme (SECS) is proposed that evaluates the node's energy levels directly and indirectly and isolates the energy-depleted nodes. Simulations show that the SECS is effective at improving network lifetime, lowering communication costs, and increasing network throughput between nodes. This is because of how it is built and because it takes into account node behaviors like sleeping and waking states. We intend to improve SECS' performance in the future by including other metrics in the real-world testbed environment, such as node mobility, stability period, Quality of Service (QoS), and other behavioral aspects, using cross-layer and other methods. This solution is feasible for the IoT networks where the energy is one of the main concern. The proposed solution also useful for a wide range of services starting from healthcare, transportation, education, and smart home applications. In the future work, we tested the proposed solution in a test-bed environment to check its efficacy and robustness in the larger environments.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] X. Li, B. Keegan, F. Mtenzi, T. Weise, and M. Tan, "Energy-efficient load balancing ant based routing algorithm for wireless sensor networks," *IEEE Access*, vol. 7, pp. 113182–113196, 2019.

[2] R. W. Anwar, K. N. Qureshi, W. Nagmeldin, A. Abdelmaboud, K. Z. Ghafoor, I. T. Javed, and N. Crespi, "Data analytics, self-organization, and security provisioning for smart monitoring systems," *Sensors*, vol. 22, no. 19, p. 7201, Sep. 2022.

[3] S. Gopinath, K. V. Kumar, P. Elayaraja, A. Parameswari, S. Balakrishnan, and M. Thiruppathi, "SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks," *Mater. Today, Proc.*, vol. 45, pp. 3579–3584, Jan. 2021.

[4] C. Nakas, D. Kandris, and G. Visvardis, "Energy efficient routing in wireless sensor networks: A comprehensive survey," *Algorithms*, vol. 13, no. 3, p. 72, Mar. 2020.

[5] R. W. Anwar, A. Zainal, F. Outay, A. Yasar, and S. Iqbal, "BTEM: Belief based trust evaluation mechanism for wireless sensor networks," *Future Gener. Comput. Syst.*, vol. 96, pp. 605–616, Jul. 2019.

[6] H. Mostafaei, "Energy-efficient algorithm for reliable routing of wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 66, no. 7, pp. 5567–5575, Jul. 2019.

[7] M. Elshrkawey, S. M. Elsherif, and M. E. Wahed, "An enhancement approach for reducing the energy consumption in wireless sensor networks," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 30, no. 2, pp. 259–267, Apr. 2018.

[8] R. Wan, N. Xiong, and N. T. Loc, "An energy-efficient sleep scheduling mechanism with similarity measure for wireless sensor networks," *Hum.-Centric Comput. Inf. Sci.*, vol. 8, no. 1, pp. 1–22, Dec. 2018.

[9] G. Thahniyath and M. Jayaprasad, "Secure and load balanced routing model for wireless sensor networks," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 34, no. 7, pp. 4209–4218, Jul. 2022.

[10] M. Ilyas, Z. Ullah, F. A. Khan, M. H. Chaudary, M. S. A. Malik, Z. Zaheer, and H. U. R. Durrani, "Trust-based energy-efficient routing protocol for Internet of Things-based sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 10, 2020, Art. no. 1550147720964358.

[11] K. Gulati, R. S. Kumar Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, "A review paper on wireless sensor network techniques in Internet of Things (IoT)," *Mater. Today, Proc.*, vol. 51, pp. 161–165, Jan. 2022.

[12] K. A. Darabkh, N. J. Al-Maaitah, I. F. Jafar, and A. F. Khalifeh, "EA-CRP: A novel energy-aware clustering and routing protocol in wireless sensor networks," *Comput. Electr. Eng.*, vol. 72, pp. 702–718, Nov. 2018.

[13] S. El Khediri, R. U. Khan, N. Nasri, and A. Kachouri, "Energy efficient adaptive clustering hierarchy approach for wireless sensor networks," *Int. J. Electron.*, vol. 108, no. 1, pp. 67–86, Jan. 2021.

[14] D.-G. Zhang, H. Wu, P.-Z. Zhao, X.-H. Liu, Y.-Y. Cui, L. Chen, and T. Zhang, "New approach of multi-path reliable transmission for marginal wireless sensor network," *Wireless Netw.*, vol. 26, no. 2, pp. 1503–1517, Feb. 2020.

[15] S. Iqbal, H. Maryam, K. N. Qureshi, I. T. Javed, and N. Crespi, "Automised flow rule formation by using machine learning in software defined networks based edge computing," *Egyptian Informat. J.*, vol. 23, no. 1, pp. 149–157, Mar. 2022.

[16] F. Engmann, F. A. Katsriku, J.-D. Abdulai, K. S. Adu-Manu, and F. K. Banaseka, ''Prolonging the lifetime of wireless sensor networks: A review of current techniques,'' *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–23, Aug. 2018.

[17] N. R. Roy and P. Chandra, ''Energy dissipation model for wireless sensor networks: A survey,'' *Int. J. Inf. Technol.*, vol. 12, no. 4, pp. 1343–1353, Dec. 2020.

[18] M. Ghribi and A. Meddeb, ''Survey and taxonomy of MAC, routing and cross layer protocols using wake-up radio,'' *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102465.

[19] S. Basagni, G. Koutsandria, and C. Petrioli, ''A comparative performance evaluation of wake-up radio-based data forwarding for green wireless networks,'' in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–9.

[20] R. Piyare, A. L. Murphy, C. Kiraly, P. Tosato, and D. Brunelli, ''Ultra low power wake-up radios: A hardware and networking survey,'' *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2117–2157, 4th Quart., 2017.

[21] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, and K. N. Qureshi, ''Security issues and attacks in wireless sensor network,'' *World Appl. Sci. J.*, vol. 30, no. 10, pp. 1224–1227, 2014.

[22] O. AlFarraj, A. AlZubi, and A. Tolba, ''Trust-based neighbor selection using activation function for secure routing in wireless sensor networks,'' *J. Ambient Intell. Humanized Comput.*, pp. 1–11, Jun. 2018.

[23] S. Nie, ''A novel trust model of dynamic optimization based on entropy method in wireless sensor networks,'' *Cluster Comput.*, vol. 22, no. S5, pp. 11153–11162, Sep. 2019.

[24] B. Mohankumar and K. Karuppasamy, ''Network lifetime improved optimal routing in wireless sensor network environment,'' *Wireless Pers. Commun.*, vol. 117, pp. 3449–3468, Feb. 2021.

[25] V. Nivedhitha, A. G. Saminathan, and P. Thirumurugan, ''DMEERP: A dynamic multi-hop energy efficient routing protocol for WSN,'' *Microprocessors Microsyst.*, vol. 79, Nov. 2020, Art. no. 103291.

[26] M. Yuvaraju and K. Pranesh, ''Energy proficient hybrid secure scheme for wireless sensor networks,'' *Wireless Pers. Commun.*, vol. 117, pp. 747–767, Nov. 2020.

[27] S. Athmani, A. Bilami, and D. E. Boubiche, ''EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs,'' *Future Gener. Comput. Syst.*, vol. 92, pp. 789–799, Mar. 2019.

[28] S. Yu, X. Liu, A. Liu, N. Xiong, Z. Cai, and T. Wang, ''An adaption broadcast radius-based code dissemination scheme for low energy wireless sensor networks,'' *Sensors*, vol. 18, no. 5, p. 1509, May 2018.

[29] C. Gherbi, Z. Aliouat, and M. Benmohammed, ''A novel load balancing scheduling algorithm for wireless sensor networks,'' *J. Netw. Syst. Manage.*, vol. 27, no. 2, pp. 430–462, Apr. 2019.

[30] S. Nakamura, M. Sugino, and M. Takizawa, ''Algorithms for energy-efficient broadcasting messages in wireless networks,'' *J. High Speed Netw.*, vol. 24, no. 1, pp. 1–15, Jan. 2018.

[31] A. S. Rostami, M. Badkoobe, F. Mohanna, A. A. R. Hosseinabadi, and V. E. Balas, ''Imperialist competition based clustering algorithm to improve the lifetime of wireless sensor network,'' in *Proc. Int. Workshop Soft Comput. Appl.* Cham, Switzerland: Springer, 2016, pp. 189–202.

[32] K.-L. Tsai, M. Ye, S.-H. Tsai, Y.-Y. Wang, and Y.-H. Zhuang, ''Attack-resistant power management scheme for wireless sensor network,'' in *Proc. Int. Conf. Adv. Robot. Intell. Syst. (ARIS)*, May 2015, pp. 1–4.

[33] L. Karim, N. Nasser, and T. Sheltami, ''A fault-tolerant energy-efficient clustering protocol of a wireless sensor network,'' *Wireless Commun. Mobile Comput.*, vol. 14, no. 2, pp. 175–185, Feb. 2014.

[34] A. Jain, M. Mishra, S. K. Peddoju, and N. Jain, ''Energy efficient computing-green cloud computing,'' in *Proc. Int. Conf. Energy Efficient Technol. Sustainability*, Apr. 2013, pp. 978–982.

[35] M. Shobana, R. Sabitha, and S. Karthik, ''Cluster-based systematic data aggregation model (CSDAM) for real-time data processing in large-scale WSN,'' *Wireless Pers. Commun.*, vol. 117, no. 4, pp. 2865–2883, Apr. 2021.

[36] J. Jiang, G. Han, F. Wang, L. Shu, and M. Guizani, ''An efficient distributed trust model for wireless sensor networks,'' *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1228–1237, May 2015.

[37] F. Zawaideh and M. Salamah, ''An efficient weighted trust-based malicious node detection scheme for wireless sensor networks,'' *Int. J. Commun. Syst.*, vol. 32, no. 3, Feb. 2019, Art. no. e3878.

[38] C. Wang, J. Li, Y. Yang, and F. Ye, ''Combining solar energy harvesting with wireless charging for hybrid wireless sensor networks,'' *IEEE Trans. Mobile Comput.*, vol. 17, no. 3, pp. 560–576, Mar. 2018.

[39] E. E. Tsiropoulou, S. T. Paruchuri, and J. S. Baras, ''Interest, energy and physical-aware coalition formation and resource allocation in smart IoT applications,'' in *Proc. 51st Annu. Conf. Inf. Sci. Syst. (CISS)*, Mar. 2017, pp. 1–6.

[40] Y. Chang, H. Tang, Y. Cheng, Q. Zhao, and B. Yuan, ''Dynamic hierarchical energy-efficient method based on combinatorial optimization for wireless sensor networks,'' *Sensors*, vol. 17, no. 7, p. 1665, Jul. 2017.

[41] Z. Fei, B. Li, S. Yang, C. Xing, H. Chen, and L. Hanzo, ''A survey of multi-objective optimization in wireless sensor networks: Metrics, algorithms, and open problems,'' *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 550–586, 1st Quart., 2017.

[42] Y. Chang, X. Yuan, B. Li, D. Niyato, and N. Al-Dhahir, ''Machine-learning-based parallel genetic algorithms for multi-objective optimization in ultra-reliable low-latency WSNs,'' *IEEE Access*, vol. 7, pp. 4913–4926, 2019.

[43] I. D. Chakeres and E. M. Belding-Royer, ''AODV routing protocol implementation design,'' in *Proc. 24th Int. Conf. Distrib. Comput. Syst. Workshops*, Mar. 2004, pp. 698–703.

RAJA WASEEM ANWAR received the Ph.D. degree from Universiti Teknologi Malaysia (UTM), Malaysia. Currently, he is an Assistant Professor in cybersecurity with the Department of Computer Science, German University of Technology (GUTech), Muscat, Oman. His research interests include information security, cyber security for cyber physical systems, trust and security in wireless sensor networks, machine learning, and the IoT. In addition, he received a number of awards in teaching, research, and academic excellence. He has been invited to serve in many international conferences, journals, and program committees.

FATMA OUTAY received the M.S. degree in networks and telecommunications from the National Engineering School of Tunis El Manar and the Ph.D. degree in wireless mobile networks and telecommunications from the University of Paris Sud 11, Orsay, France. She is currently a senior researcher in computer science and wireless mobile networks and telecommunications. During the Ph.D. degree and a postdoctoral research with Telecoms Sud Paris, France, she has participated in several national and international research projects in wireless and mobile networks, in collaboration with Alcatel Lucent, Thales, Orange Laboratories, and other academic institutions in Europe. Prior to her current position with Zayed University, United Arab Emirates, as an Associate Professor, she has joined Bouygues Telecoms, in 2012, which is one of the three main telecoms operators/ISPs in France as a ''Wi-Fi Expert/Architect'' for three years enabling negotiation of SLA agreements and defining technical support and incident management processes with different contributors and suppliers implementing internal and external processes as per ITIL recommendations.

KASHIF NASEER QURESHI received the master's degree in computer science and in information technologies and the Ph.D. degree in wireless communication, in 2016. He is currently an Associate Professor with the Department of Electronic and Computer Engineering, University of Limerick, and a part of the cyber skills project. He has been involved as a principal investigator in a government funded cybersecurity project, since 2019. His name is included in the top 2% of scientists in the world from Stanford University, USA. He received best researcher awards, from 2020 to 2022. He has 14 years of teaching and research experience in leading academic institutes. He worked on several projects in collaboration with industrial/academic partners in the U.K., Canada, South Korea, Malaysia, and China. These projects were mainly in the areas of cyber security, wireless communication, smart cities, the IoT, artificial intelligence, intelligent transportation systems, ad-hoc networks, and cyber-physical systems. He has published around 174 research articles with a cumulative more than 400 impact factor score in international journals. His recent scientific contributions are on cybersecurity, trust-based edge or cloud solutions, the secure Internet of Connected Vehicles, secure drone-enabled networking, electrical vehicle charging management, and secure healthcare systems, where he find out more about his work on Google Scholar. He is also an Associate Editor and a Guest Editor in SCI journals and special issues, including IEEE Sensors, MDPI journals, and Hindawi. He has graduated number of master's and Ph.D. students in the general area of the security for Internet of Things (IoT), long range area networks, trust model for wireless sensor networks (WSNs), and security solutions of wired and wireless networks.

SALEEM IQBAL received the B.S. and M.S. degrees in computer science from the COMSATS, Pakistan, and the Ph.D. degree from the PCRG Laboratory, Faculty of Computing, UTM, Malaysia, in 2015. He is currently an Associate Professor with the Department of Computer Science, Allama Iqbal Open University (AIOU), Islamabad, Pakistan. Previously, he was with the Department of Computing Science, COMSATS, as a Lecturer, from 2003 to 2007. He worked for four years in Pakistan federal government for deployment of ICT projects. His research interests include medium access control and network layer for heterogeneous wireless networks. To his credit, there are ten publications.

KAYHAN ZRAR GHAFOOR received the B.Sc. degree in electrical engineering from Salahaddin University, in 2003, the M.Sc. degree in remote weather monitoring from Koya University, in 2006, and the Ph.D. degree in wireless networks from University Technology Malaysia, in 2011. He is currently with the Department of Computer Science, Knowledge University, University Park, Erbil, Iraq. His current research interests include the vehicular communication Internet of Things, big data in VANET, and software defined networks. He is a member of IEEE Vehicular Technology Society, IEEE Communications Society, Internet Technical Committee (ITC), and International Association of Engineers (IAENG).