Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

# Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks

G. Sudha & C. Tharini

**To cite this article:** G. Sudha & C. Tharini (2023) Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks, Automatika, 64:3, 634-641, DOI: 10.1080/00051144.2023.2208462

**To link to this article:** https://doi.org/10.1080/00051144.2023.2208462



Published online: 04 May 2023.

AUTOMATIKA
2023, VOL. 64, NO. 3, 634–641
https://doi.org/10.1080/00051144.2023.2208462

REGULAR PAPER

OPEN ACCESS Check for updates

# Trust-based clustering and best route selection strategy for energy efficient wireless sensor networks

G. Sudha[a,b] and C. Tharini[a]

[a]Department of Electronics and Communication Engineering, B. S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India; [b]Department of Electronics and Communication Engineering, Sri Sairam Engineering College, Chennai, India

**ABSTRACT**

Energy efficiency is one of the most researchable topics of the energy constrained Wireless Sensor Networks (WSN). Due to the widespread usage of WSN in real-time applications, network lifetime is the serious concern and numerous research solutions are presented in the literature for handling this issue. Several techniques are employed to handle energy consumption and the most promising techniques are clustering and routing other than data compression. Hence, this paper presents a clustering and routing-based solution for energy efficient WSN with trust notion as its base. The nodes are clustered with the help of Dempster-Shafer Theory (DST), while the best route is selected by employing Lion Optimization Algorithm (LOA). The work efficiency of the proposed work is proven with reasonable outcomes with respect to different performance measures. This work proves an average packet delivery rate of 94.24%, average latency of 13.43 s and 191 alive nodes at the end of 500th second better network lifetime when compared to the existing works.

**ARTICLE HISTORY**
Received 22 February 2023
Accepted 25 April 2023

**KEYWORDS**
Trust; energy efficiency; routing; DS theory; LOA

## 1. Introduction

A Wireless Sensor Network (WSN) is built up by a huge count of individual sensor nodes. These sensors are low-cost and can be used for a variety of purposes, yet inherently have limited resources. The sensors have the ability to sense, manipulate, and commune with the other nodes that make up the network. In order to monitor or collect data about the surrounding environment, these sensors can be installed in places that are inaccessible to the humans. Real-time applications can be developed using sensors in many different domains, such as remote healthcare, environment monitoring and other surveillance systems [1]. Sensors are useful to society in all of the aforementioned applications without any trouble. The restrictions of its resources are, however, the most crucial aspect to take into consideration.

Sensors can be able to fulfil their function when resource limitations are well managed, which refers to energy or battery backup. Energy is the sensors' life support, and so it can satisfy the purpose for which the network is designed. Because it is not always practical to replace the batteries in a sensor network, it is critical to effectively manage the network's energy usage. Enhancement of energy efficiency paves way for prolonging the lifespan of the network, however it is highly challenging.

Energy conservation can be accomplished by the utilization of a variety of strategies, such as clustering, scheduling sleep cycles, routing, incorporating sink nodes, and many more. The recommended strategies for cutting down on energy usage to the fullest extent possible are clustering and routing [2,3]. This insight prompted the proposal of this work, in which energy conservation is attained. Clustering helps to save power by utilizing a Cluster Head (CH) node that efficiently handles the nodes that make up the cluster. This CH gathers the data that is sensed by the Cluster's Member (MN) nodes and then forwarding it to the Base Station (BS).

Clustering is developed with the primary purpose of lowering the overall energy usage, which can be accomplished by the following ways. As all the data is delivered to the CH node, the concept of redundancy is rendered obsolete. Additionally, the routing cost can be avoided by enforcing the constraint that communication may only take place between the CH node and the BS. This keeps all communications within the network within the same network. Additionally, it ensures that the sensors' communication bandwidth is maintained. Obviously, these characteristics lengthen the network's lifespan. The objective of the proposed T-CBRSS is to extend the network's lifetime by enforcing clustering and routing techniques, with trust as the underlying

**CONTACT** C. Tharini tharini.ece@outlook.com, tharini@crescent.education Department of ECE, B. S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, India

model, as they have been demonstrated to be efficient and effective. The outcomes of this project are deemed adequate. The key points of this work are listed.

- Two different approaches such as clustering and the best route selection are enforced to ensure energy efficiency of WSN.
- Clustering is done by Dempster Shafer Theory (DST), which requires no prior knowledge about nodes and the best route is selected by Lion Optimization Algorithm (LOA), where the fitness value is fixed on the basis of trust metrics.
- The energy efficiency of the work is enhanced and so the network lifetime, which is proven by experimental results.

The subsequent sections of this paper are organized under subheadings. Section 2 includes the literature review; Section 3 contains the recommended technique; and Section 4 evaluates the execution of the proposed effort. Finally, section 5 contains the final observations.

## 2. Review of literature

The related works concerning clustering and routing mechanisms are reviewed in this section.

The paper [4] proposes a safe routing protocol for WSN that is referred to as "Realisable Secure Aware Routing" (RSAR). The approach's primary focus is on improving energy efficiency through the accumulation of data. This work determines the trustworthiness of each of the sensor nodes in the network. After that, an optimization approach for conditional tug of war is implemented, followed by an best trust inference model. The flow of data is minimized, and any unneeded data is removed from the system. After all of the information has been collected, it is subsequently sent to the receiving side.

On the basis of game theory and clustering, the work in [5] presents a method for the behaviour monitoring and trust analysis of relationships. In addition to the incorporation of the idea of clustering, the process of computing the trust factor of the node is known as evidence gathering scheme. An adaptive routing strategy for WSN is proposed in [6], and it is based on trust theory. This study takes into account three distinct varieties of trust values, namely direct, indirect, and witness trust. These calculated trust factors are compared with one another using the paired method. The cross-layer design in [7] analyses the routing policies that are used in green Internet of Things (IoT) networks that are based on WSN. In this article, a mathematical model for computing the Quality of Service (QoS) attributes is described in order to assist data transfer in Internet of Things applications. For the purpose of investigating how multi-hop communication influences outcomes, a Markov discrete-time M/M/1 queuing model is applied. The analytical model and the critical path-loss model are accountable for calculating the trust level associated with the nodes that are used the most frequently. Analyses are performed on the data transmission in hop-by-hop and end-to-end modes respectively.

In [8], an Internet of Things (IoT) spatial routing system that is protected against Denial of Service (DoS) assaults is described. This protocol is based on selective authentication. The wireless links are analysed using the statistical state information, and then the trust model is constructed using this information as its foundation. In order to guarantee the accuracy of the data and reduce the amount of time spent on computing, a technique that is selectively authenticated using entropy is used. Through the efforts of these people, redundant data transmission and signature checking processes have been eradicated. A trustworthy strategy for Internet of Things-based mobile wireless networks is provided in reference [9]. The routing, data integrity, and confidentiality issues are the primary objectives of this work. In order to provide efficient and reliable data routing, the best possible network parameters and measurements of the wireless channel are selected. The distance vector is used, at regular intervals, to determine where the nodes are located in the network. Cryptography utilizing both public and private keys is utilized in order to ensure the safety of this work.

In [10], many qualities are used to present a trust aware routing system. This protocol takes into account data transfer, data, power, and recommendation. This work makes advantage of a sliding time window in order to identify aberrant user behaviour. A safe routing algorithm for WSN is provided in [11], which is based on whale optimization clustering. This work determines which reliable node should serve as the cluster head by taking into account factors such as energy, distance to the cluster, delay, transmission rate, and density.

The article [12] presents a trust model-based routing method that is based on Reinforcement Learning (RL). This notion works better when it comes to cluster size management. The RL is responsible for keeping tabs on the behaviours of the users, and by varying the size of the clusters in a dynamic manner, system security is significantly improved. In the paper [13], an efficient routing for WSN that is based on compressive sensing is proposed. The Kronecker representation is used to handle the transmission of the data, and the Fractional Earthworm Optimization (FEWO) algorithm is applied for determining the CH. The cluster head creates many pathways by taking into consideration factors such as energy, trust, delay, and distance.

A self-healing secure key distribution strategy for the Internet of Things (IoT) is described in [14]. A key distribution strategy for IoT gadgets is provided alongside

a self-healing mechanism that consists of two levels. The first layer is in charge of providing access control and security, and it does so in a manner that is based on polynomial techniques. The self-healing-based key distribution and Singular Value Decomposition (SVD) based authentication are presented in the second layer of the protocol. On the basis of Exponential Cat Swarm Optimization (ECSO) and fuzzy optimization, a multipath data transfer technique is given in [15]. The Penguin Fuzzy-based Ant Colony Optimization, also known as PFuzzyACO, is responsible for electing the CH node, whereas ECSO is in charge of routing. Different factors such as trust, distance, energy, traffic and delay.

A trust-based opportunistic routing method for the social IoT is provided in [16]. The optimal stopping concept is used in this study to pick the nodes that will be used for data forwarding, and the network coding approach will be used for the transmission of the data. Game theory is utilized in order to determine who gets access to the trustworthy channel. In [17], a safe multi-path reactive protocol for the IoT is described. Trust is the foundation of the multipath routing strategy that is presented in this body of work. A probabilistic model takes into consideration both the movability and the behaviour of the nodes in its network. The article [18] presents a routing protocol that is based on density clusters, and the authors believe that their work is appropriate for use in emergency sensor applications.

A technique for the secure selection of cluster heads for WSN is provided in [19]. This technique assesses the trust level of individual nodes. Calculating the behaviour of sensor nodes requires taking into account a number of different trust types. The questionable cluster heads have been located, and they have been taken out of service. In [20], a trust-aware cooperative routing strategy designed to protect the Internet of Things is described. When factors like as energy consumption, throughput, the rate at which packets are delivered, and so on are taken into consideration, a trust-based routing topology construction can be given.

Inspired by these existing works, this paper presents a trustworthy clustered routing selection strategy for WSN, which ensures energy efficiency and Quality of Service (QoS). Reliable data transmission consumes more energy, which seriously affects the network lifetime. Hence, the choice of right route is mandatory for achieving energy efficiency, which is carried out in this work.

## 3. Proposed trust-based clustering and best route selection strategy (T-CBRSS)

This work clubs two energy harvesting techniques such as clustering and best route selection for data transmission. The concept of clustering brings in the features of modularity and easy-to-manage operation. All the nodes are a part of cluster and every cluster of nodes is managed by a central authority called CH, while the remaining nodes are termed as MN. As the CH node manages communication between the nodes, energy efficiency is attained. As an added advantage, the optimal choice of route is performed by LOA. Both the phases of clustering and best route selection are based on the concept of trust, which paves way to attain reliability. The overall flow diagram is illustrated in Figure 1. The following sections discuss the cluster formation and best route selection strategy.

### 3.1. Cluster formation and CH node assignment

This work builds cluster by encircling 20 nodes in a specific location and assigns the potential node as CH. The number 20 is chosen by trial-and-error method, as the functions are performed better. The CH node selection is the most significant process involved and is carried out by DST, which is also referred as evidence theory [21]. In contrast to Bayes' theorem, the DST does not require prior understanding of probabilistic methods.

In this phase, the trust rates computed by the two surrounding nodes are considered, so as to ensure correctness. The decision made by a single node is not fruitful always, as the authenticity of the node is doubtful. Hence, this work considers the decisions of two surrounding nodes, such that the final decision is better.

A node can either be trustworthy or untrustworthy and it can be stated as

$$x : \Omega = \{T, \bar{T}\} \tag{1}$$

$T$ implies that the node $x$ is trustworthy, whereas $\bar{T}$ indicates that it is not. This is further explained by the hypothesis, as indicated below.

$$HP = \{T\} \tag{2}$$

$$\overline{HP} = \bar{T} \tag{3}$$

$$UC = \Omega \tag{4}$$

Equations (2) and (3) indicate that the node is trustable and not trustable respectively. Equation (4) suggests that the node is either trustable or not trustable.

Suppose the probability of a node's trustworthiness is provided by $\mu$, then

$$\begin{cases} A1(HP) = \mu \\ A1(\overline{HP}) = 0 \\ A1(UC) = 1 - \mu \end{cases} \tag{5}$$

The probability function of untrustworthiness of a node is given by (6).

$$\begin{cases} A1(HP) = 0 \\ A1(\overline{HP}) = \mu \\ A1(UC) = 1 - \mu \end{cases} \tag{6}$$

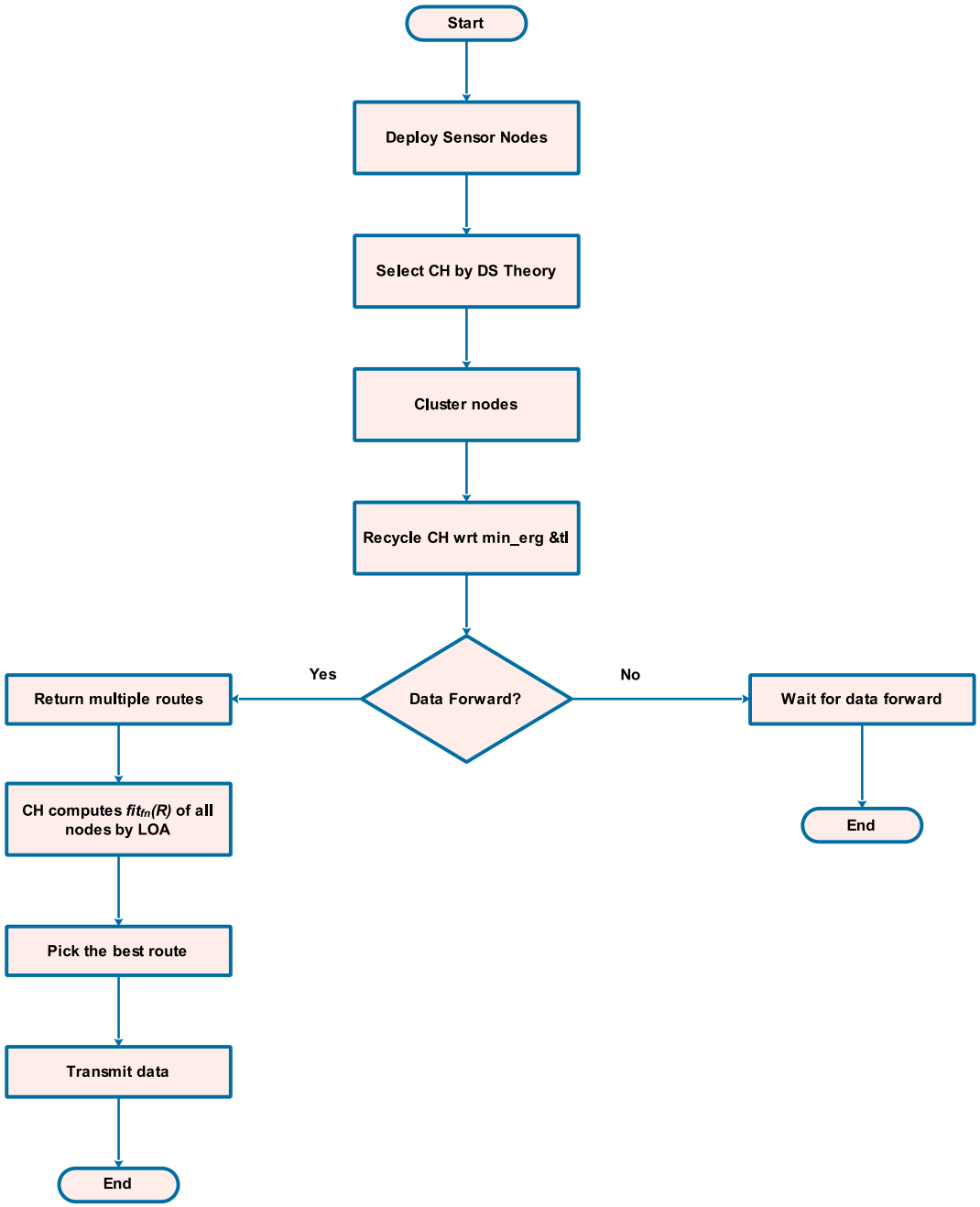


**Figure 1.** Flowchart of T-CBRSS.

In the next step, the trust rate is computed by the surrounding nodes. In this case, there is no need to check for the trustworthiness of surrounding node, as decisions from two surrounding nodes are considered. The individual decisions made are combined as follows. There are three possible cases.

- Both the decisions of surrounding nodes show that the node is trustable, as represented in Equation (7) is the first case.

$$\begin{aligned} &A1(HP) \oplus A2(HP) \\ &= \frac{1}{w}[A1(HP)A2(HP) + A1(HP)A2(UC) \\ &\quad + A1(UC)A2(HP)] \end{aligned} \tag{7}$$

- In the second case, both decisions of surrounding nodes show that the node is not trustable and is shown in Equation (8).

$$\begin{aligned} &A1(\overline{HP}) \oplus A2(\overline{HP}) \\ &= \frac{1}{w}[A1(\overline{HP})A2(\overline{HP}) + A1(\overline{HP})A2(UC) \\ &\quad + A1(UC)A2(\overline{HP})] \end{aligned} \tag{8}$$

- In the final case, the node can either be trustable or not trustable and is shown in the following equation.

$$A1(UC) \oplus A2(UC) = \frac{1}{w}A1(UC)A2(UC) \tag{9}$$

where $w$ in Equations (7–9) indicate

$$\begin{aligned} w = {} & A1(HP)A2(HP) + A1(HP)A2(UC) \\ & + A1(UC)A2(HP) + A1(\overline{HP})A2(\overline{HP}) \\ & + A1(\bar{H}P)A2(UC) + A1(UC)A2(\bar{H}P) \end{aligned}$$

$$+ A1(UC)A2(UC) \tag{10}$$

The authentic trust rate ranges from 0 to 1. A node is claimed to be completely trustable, when its trust rate is 1. A trust score of 0.5 indicates that a node is either trustable or not trustable. The final case represents that the node is not trustable with the trust score of 0. The node with good trust rate is chosen as CH node and is retained for a specific period of time. However, the same node cannot continue to function as CH for a longer period of time, as its energy gets drained faster. Thus, it is necessary to recycle the node periodically, as discussed below.

#### 3.1.1. Recycling CH node

The goal of this phase is to prevent overloading the CH node to the point of sudden depletion of its energy. The CH node must have an appropriate supply of energy to carry out all of its duties properly. As a result, it is widely known that a single node cannot continue to be the CH, due to the faster energy depletion. The CH is identical to the other nodes except for its greater trust score. As a result, the node's battery may deteriorate more quickly than the batteries of other nodes.

The suggested technique for selecting CHs includes a threshold for *min_erg* (minimal energy) and *tl* (time to live). The *min_erg* and *tl* thresholds are set at 0.6 and 60 s, respectively. The CH node's battery backup is checked every sixty seconds. If the battery backup capacity is more than *min_erg*, the CH retains its place. Conversely, if the backup runs out before to the expiration of *tl*, the CH must be recycled in its entirety. Thus, if one of the requirements is met, the primary node is recycled. This method conserves energy significantly due to the fact that no single node is overburdened and an unbiased energy contribution scheme is used.

### 3.2. Best route selection strategy

Routing is the process that consumes more energy, which can be reduced when a best route is chosen [22–27]. As far as this work is concerned, best route indicates the route with more number of trustworthy nodes. The choice of best route helps in reliable data transmission and this work chooses the best route by LOA. The basics of LOA are explained as follows.

#### 3.2.1. Basics of LOA

The LO algorithm is a bio-inspired algorithm that recreates the actions carried out by the wild lion population. When looking into the life policy of lions, one thing that becomes apparent is that there are two distinct types of lions: resident lions and nomadic lions [28,29]. Each pride of resident lions consists of approximately four to five female lions, their cubs, and one or two male lions. The term "pride" refers to the group of lions that live together. The young animals will mature into full-grown adults when some time has passed. When things reach this point, the younger male lions are kicked out of the pride. These juvenile lions don't have any company, so they just walk around aimlessly without following any particular code. However, if a nomadic lion is successful in defeating an adult lion that is already part of a pride, it will be invited to join the pride. At this point, a switch takes place within a pride, and it is possible for this to take place at any point in time. As a result, a lion's membership in a pride is only temporary at best. The LOA procedure as a whole is broken down into the following steps.

```
LOA
Produce initial population of lions N_p
Declare the count of prides and nomadic lions
    Choose the percent of nomadic lions from N_p randomly and number of prides;
    Choose the gender rate of lions in each pride;
For each pride do
    Select a lioness randomly for hunting;
    Assign the remaining lionesses a position from the territory;
    Set the roaming percent of each male lion in the pride and the mating probability;
    Expel the weakest lion from the pride;
For each nomadic lion do
    Both the male and female nomadic lions wander randomly;
    Set the mating probability of nomadic female lion with the male lion;
    Nomadic lions attack the pride randomly;
For each pride do
    Fix the percentage of lioness that can become nomad;
Do
    Sort the nomad lions with respect to the gender;
    Choose best lionesses and distribute to fulfil the pride;
    Check the completeness of all the available prides;
    Eliminate the lions with minimal fitness value;
While (termination condition);
```

Lionesses engage in behaviours that are significantly distinct from those of male lions, such as the pursuit of prey, which is often carried out by the lionesses rather than the lions. Each group of lions, known as a pride, is confined to a certain area. As a first step in the hunt, the lionesses surround the animal they intend to hunt and encircle it. This algorithm requires as its input parameters the beginning population along with the associated percentage of nomadic and residential lions. The best answer to an issue can be discovered by sorting the nomadic lions in accordance with the level of fitness they possess. When the lions' fitness value is lower than what is considered acceptable, they are removed from consideration. Therefore, the lion needs to get in better shape in order to earn a spot in the pride. In addition, there is the possibility that the healthier lions are the only ones who deserve a place in the pride. This procedure will continue until the optimal options have been identified.

#### 3.2.2. Trustworthy route selection

The best route for data transmission is carried out by LOA. Here, the fitness value of LOA is set by a combination of different trust metrics such as battery backup, packet forwarding capacity, distance and latency.

$$Fit_{fn}(R) = \frac{SN_e \times SN_{pt}}{SN_d \times SN_{dn} \times SN_{cdis}} \tag{11}$$

Here, $SN_e$ and $SN_{pt}$ stand for remaining energy of the node after the completion of data transmission. $SN_d$ denotes the delay being experienced during data

transmission and $SN_{dn}$ represents the density of nodes, which is the total count of MN in a cluster. $SN_{cdis}$ is the cluster distance of a node from other nodes in the cluster and this is computed as follows.

$$SN_{cdis} = \frac{\sum_{i=1}^{TN-1}(Dis(CL_S, CL_D))}{TN} \quad (12)$$

In the above equation, $TN$ is the total count of nodes exists along a route. $Dis(CL_S, CL_D)$ denotes the distance between a sender node $S$ and the recipient nodes. All the nodes along a route are processed by LOA. Hence, the route consisting nodes with greatest $Fit_{fn}(R)$ among all possible routes is chosen. The performance of the proposed work is evaluated in the following section.

## 4. Results and discussion

The proposed optimized cluster-based trustworthy routing scheme is simulated by considering an area of 100m × 100m dimension with 200 nodes. Certain abnormal nodes are randomly distributed, which do not show interest in data forwarding. The initial energy of the sensor nodes is 0.1 Joules. The sensor nodes are mobile by employing random mobility model. Here, the sensor node starts from a specific location and reaches the destination. The BS remains static and does not move. Table 1 shows the simulation parameters employed by this work.

The performance of the proposed work is analysed with respect to the performance measures such as packet delivery rate, average latency, energy consumption and network lifetime. The performance of the work is compared with the existing approaches such as trust based [6], multipath data [15] and secure WSN [19] respectively. The attained results are shown in Figures 2–5.

### 4.1. Packet delivery rate analysis

The primary purpose of routing is to ensure the delivery of data packets from their point of origin to their final destination without interruption. Nevertheless, there are circumstances in which the sensor node might not exhibit interest in forwarding the packet, which results in a lower rate of packet delivery. When the rate at which packets are delivered by the node is low, it makes perfect sense for it not to forward any incoming packets. The findings are depicted in Figure 2.

When carrying out this study, the number of nodes is varied from 25 to 200. According to the findings, it is

**Table 1.** Simulation parameters.

| Simulation parameters | Values |
|---|---|
| Packet Length | 4496 bits |
| Utilized energy for data transmission and reception | 50 nJ/bit |
| Utilized energy for data collection | $5*10^{-9}$ J |
| Pause time interval | 0.01 s |

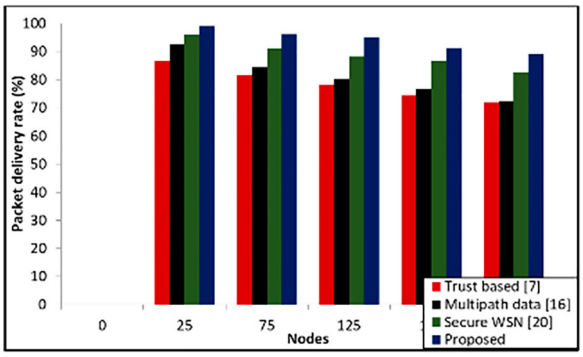


**Figure 2.** Packet delivery rate analysis.

clear that the proposed work has an acceptable packet delivery rate, in contrast to the existing works. It has been noticed that the delivery rate slows down as the number of nodes rises; this, however, is acceptable. The following illustration provides an examination of the latency caused by the proposed work.

### 4.2. Average latency rate analysis

This section provides an analysis of the latency rate of the work that is being suggested. Latency refers to the amount of time it takes to send a packet to its intended location. In order to improve routing performance, it is important that any routing algorithm experiences just a minimal amount of latency. The results of the latency test are shown in Figure 3.

The analysis of latency is carried out by adjusting the number of nodes in the network from 25 to 200, with the latency being measured in seconds. The rate of latency grows proportionally with the number of sensor nodes in a network. However, the delay is somewhat manageable in contrast to other works. When there are 200 nodes, the network experiences a delay rate that is 19.2 s at its longest point.

### 4.3. Energy consumption analysis

In order to lengthen the lifespan of the network, the energy consumption of the routing algorithm must be

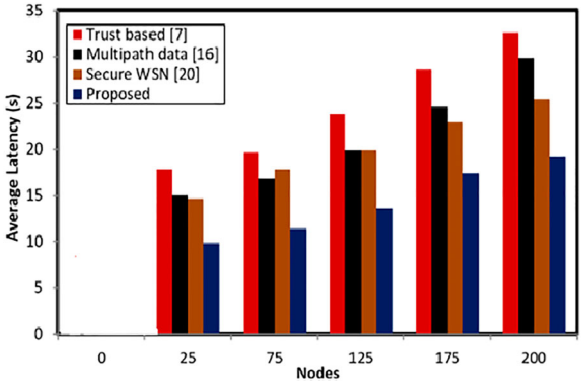


**Figure 3.** Average latency rate analysis.

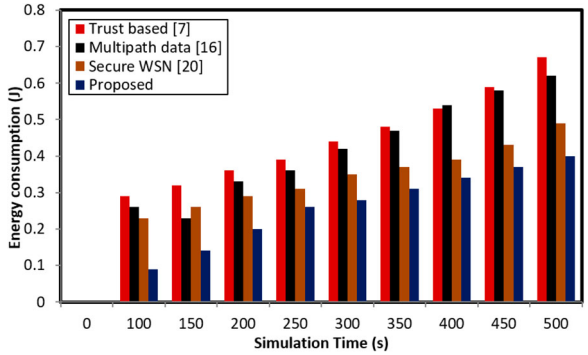


**Figure 4.** Energy consumption analysis.

kept to a minimum. At the beginning, all of the nodes are given the same amount of energy, and the rate at which their energy decreases is determined by the tasks that have been assigned to them. When calculating the amount of energy used, the number of seconds spent running the simulation is taken into account. Figure 4 presents the findings on the amount of energy that was consumed.

The work that is being proposed has an energy consumption of 0.4 joule at the 500th second, which is closely followed by the use of secure WSN. The longer the network can function with a lower overall energy consumption, the more reliable it will be. The discussion of the lifetime analysis will continue in the next section.

### *4.4. Network lifetime analysis*

The lifetime of the network needs to be as long as it can possibly be. It is possible to extend the lifetime of a network by utilizing a variety of approaches, some of which include clustering, duty cycling, sleep cycle scheduling and so forth. The lifetime analysis of the network is analysed, and the results are shown in Figure 5.

Figure 5 provides an analysis of the network lifetime of the work by calculating the total number of alive nodes in relation to the amount of time spent simulating. When the simulation time is increased, the number of live nodes will decrease proportionately. In

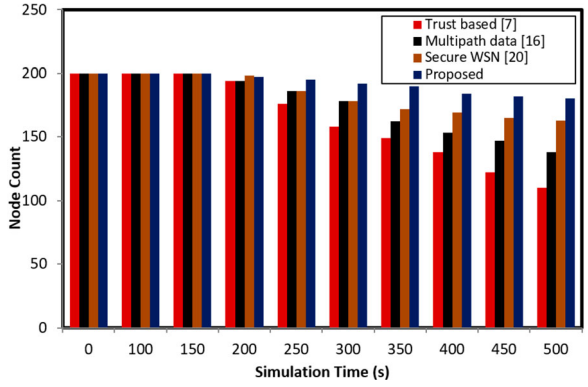


**Figure 5.** Network lifetime analysis.

contrast to the methods that have been used previously, the proposed study results in a significantly lower rate of death among the network's nodes. The solution that has been suggested utilizes 180 nodes during the 500th second of simulation. As a result, the work that has been proposed guarantees reliable routing with improved network lifetime.

## 5. Conclusions

This article presents an energy efficient solution for WSN by imposing clustering and routing techniques with trust as the base model. Energy efficiency is the major necessity of WSN, due to its energy stringent nature. As lifetime of the network crucially depends on energy efficiency, intelligent and reliable ideas are evergreen requirements of WSN. This work achieves the goal by implementing two phases such as clustering and best route selection. The CH node of clusters is chosen by DS theory and LOA is employed for selecting the best route. The fitness of LOA is determined by the trust score of available routes. The best route is chosen for data transmission and the work's performance is evaluated in terms of packet delivery rate, latency, energy consumption and network lifetime, which proves the efficacy. In future, the energy efficiency of WSN can be improved by enforcing sleep cycle scheduling and topology management with trust metrics.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## References

[1] Majid M, Habib S, Javed AR, et al. Applications of wireless sensor networks and Internet of Things frameworks in the industry revolution 4.0: a systematic literature review. Sensors. 2022;22(6):2087.
[2] Gulati K, Boddu RSK, Kapila D, et al. A review paper on wireless sensor network techniques in Internet of Things (IoT). Mater Today Proc. 2022;51:161–165.
[3] Zhai D, Wang C, Zhang R, et al. Energy-saving deployment optimization and resource management for UAV-assisted wireless sensor networks with NOMA. IEEE Trans Veh Technol. 2022;71(6):6609–6623.
[4] Basha AR. Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network. IET Wirel Sens Syst. 2020;10:166–174. doi:10.1049/iet-wss.2019.0178.
[5] Yang L, Lu Y, Liu S, et al. A dynamic behavior monitoring game-based trust evaluation scheme for clustering in wireless sensor networks. IEEE Access. 2018;6:71404–71412. doi:10.1109/ACCESS.2018.2879360.
[6] Khalid NA, Bai Q, Al-Anbuky A. Adaptive trust-based routing protocol for large scale WSNs. IEEE Access. 2019;7:143539–143549. doi:10.1109/ACCESS.2019.2944648.
[7] Hasan MZ, Al-Turjman F, Al-Rizzo H. Analysis of cross-layer design of quality-of-service forward geographic wireless sensor network routing strategies in

green Internet of Things. IEEE Access. 2018;6:20371–20389. doi:10.1109/ACCESS.2018.2822551.
[8] Lyu C, Zhang X, Liu Z, et al. Selective authentication based geographic opportunistic routing in wireless sensor networks for Internet of Things against DoS attacks. IEEE Access. 2019;7:31068–31082. doi:10.1109/ACCESS.2019.2902843.
[9] Haseeb K, Din IU, Almogren A, et al. RTS: A robust and trusted scheme for IoT-based mobile wireless mesh networks. IEEE Access. 2020;8:68379–68390. doi:10.1109/ACCESS.2020.2985851.
[10] Sun B, Li D. A comprehensive trust-aware routing protocol with multi-attributes for WSNs. IEEE Access. 2017;6:4725–4741. doi:10.1109/ACCESS.2017.2786944.
[11] Sharma R, Vashisht V, Singh U. WOATCA: a secure and energy aware scheme based on whale optimisation in clustered wireless sensor networks. IET Commun. 2020;14(8):1199–1208. doi:10.1049/iet-com.2019.0359.
[12] Ling MH, Yau KLA, Qadir J, et al. A reinforcement learning-based trust model for cluster size adjustment scheme in distributed cognitive radio networks. IEEE Trans Cogn Commun Netw. 2018;5(1):28–43. doi:10.1109/TCCN.2018.2881135.
[13] Pasupuleti VR, Balaswamy C. Optimised routing and compressive sensing-based data communication in wireless sensor network. IET Commun. 2020;14(6):982–993. doi:10.1049/iet-com.2019.0130.
[14] Han S, Gu M, Yang B, et al. A secure trust-based key distribution with self-healing for Internet of Things. IEEE Access. 2019;7:114060–114076. doi:10.1109/ACCESS.2019.2935797.
[15] Kulkarni PKH, Jesudason PM. Multipath data transmission in WSN using exponential cat swarm and fuzzy optimisation. IET Commun. 2019;13(11):1685–1695. doi:10.1049/iet-com.2018.5708.
[16] Wang X, Zhong X, Li L, et al. TOT: trust aware opportunistic transmission in cognitive radio social Internet of Things. Comput Commun. 2020;162:1–11. doi:10.1016/j.comcom.2020.08.007.
[17] Hammi B, Zeadally S, Labiod H, et al. A secure multipath reactive protocol for routing in IoT and HANETs. Ad Hoc Netw. 2020;102118. doi:10.1016/j.adhoc.2020.102118.
[18] Al-Kahtani MS, Karim L, Khan N. ODCR: energy efficient and reliable density clustered-based routing protocol for emergency sensor applications. Appl Comput Inform. 2020. doi:10.1016/j.aci.2020.03.003.
[19] Saidi A, Benahmed K. Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks. Ad Hoc Netw. 2020;106:102215. doi:10.1016/j.adhoc.2020.102215.
[20] Djedjig N, Tandjaoui D, Medjek F, et al. Trust-aware and cooperative routing protocol for IoT security. J Inf Secur Appl. 2020;52:102467. doi:10.1016/j.jisa.2020.102467.
[21] Dempster AP. Upper and lower probabilities induced by a multivalued mapping. Ann Math Stat. 1967;38(2):325–339.
[22] Wan J, Chen J. AHP based relay selection strategy for energy harvesting wireless sensor networks. Future Gener Comput Syst. 2022;128:36–44.
[23] Kumar A, Webber JL, Haq MA, et al. Optimal cluster head selection for energy efficient wireless sensor network using hybrid competitive swarm optimization and harmony search algorithm. Sustain Energy Technol Assess. 2022;52:102243.
[24] Abualkishik AZ, Alwan AA. Trust aware aquila optimizer based secure data transmission for information management in wireless sensor networks. J Cybersecur Inf Manag. 2022;9(1):40–51.
[25] Altowaijri SM. Efficient next-hop selection in multihop routing for IoT enabled wireless sensor networks. Future Internet. 2022;14(2):35.
[26] Lakshmanna K, Subramani N, Alotaibi Y, et al. Improved metaheuristic-driven energy-aware cluster-based routing scheme for IoT-assisted wireless sensor networks. Sustainability. 2022;14(13):7712.
[27] Esmaeili H, Bidgoli BM, Hakami V. CMML: combined metaheuristic machine learning for adaptable routing in clustered wireless sensor networks. Appl Soft Comput. 2022;118:108477.
[28] Mccomb K, Pusey A, Packer C, et al. Female lions can identify potentially infanticidal males from their roars. Proc R Soc Lond Ser B Biol Sci. 1993;252(1333):59–64.
[29] Schaller GB. The serengeti lion: a study of predator–prey relations. Wildlife behavior and ecology series. Chicago (IL): University of Chicago Press; 1972.