International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-12 Issue-2, July 2023

Energy Efficient Data Aggregation Approach for Sensor Network using Trust Mechanism

Ayush Sharma, Sunny Arora

Abstract: ***A wireless sensor network consists of numerous sensor nodes which are capable of entering and departing from the network according to their wish. The implementation of sensor networks is done at far places and they are small-sized. Thus, energy consumption becomes the main issue of WSN. Due to the limited energy of sensor nodes, the data that is collected from the intended environment is sent directly to the main station. The sink node receives the data that several sensor nodes send. The decision-making process is implemented by identifying and removing similarities between the data from various sensor nodes. In addition, the sink makes the deployment of obtained data locally as well as transmits these data to the networks which are executed far away. The existing research work employs CTNR, an energy-efficient protocol that is capable of enhancing the duration of WSN. The CTNR protocol consists of two-level hierarchies for mitigating the energy utilized in WSN. This protocol assists in choosing the CHs (cluster heads) on the basis of distance and energy. This work will focus on enhancing the CTNR routing algorithm so that the life span of the network can be prolonged.***

Keywords: IoT, WSN, CTNR, Routing, Multi-level Hierarchy

I. INTRODUCTION

The academic community worldwide has shown a keen interest in the Internet of Things (IoT) due to its wide-ranging capabilities and offerings. As a key IoT invention, the utilization of wireless sensor networks (WSNs) is relatively well known. WSN-assisted IoT is used to gather environmental data and identify specific real-world events that are significant. By its uses, such as environment monitoring, combat tracking, and medical monitoring, it can significantly improve people's lives [1]. With the analysis of the information provided by the devices put on it, the actual value of these IoT smart applications may be determined. According to the 2020 conceptual framework, there are 4 essential elements in the framework of the Internet of Things, which are expressed as:

Manuscript received on 11 June 2023 | Revised Manuscript received on 20 June 2023 | Manuscript Accepted on 15 July 2023 | Manuscript published on 30 July 2023.

*Correspondence Author(s)

Ayush Sharma*, Department of Computer Science & Engineering, Guru Kashi University, Talwandi Sabo Bathinda (Punjab) India. E-mail: ayush.sharma468@gmail.com, ORCID ID: 0009-0006-3881-1636

Dr. Sunny Arora, Department of Computer Science & Engineering, Guru Kashi University, Talwandi Sabo Bathinda (Punjab) India. E-mail: ddit@gku.ac.in, ORCID ID: 0000-0003-1971-7514

IoT = Services + Data + Networks + Sensors

WSNs (Wireless Sensor Networks) are made up of information sources known as sensors. They make up the main parts of the Internet of Things. The bottom layer is employed for locating the sensors. The data is produced and utilized in the purview of this layer. The fog layer is another name for the edge layer. To make sure the data is accessible, reliable, and appropriate for its clients, this layer uses edge devices for a sizable amount of computing, storage, and information sharing. Data mining is carried out by the cloud layer with the assistance of powerful machines placed there. Applications for the Internet of Things offer services to users globally [2].

A. Trust-Based Information Fusion

The inability of smart apps to address issues with the dependability of their data sources is caused by the lack of benchmarking techniques. To reap the full rewards of smart applications, the major focus is on managing the reliability of data sources. To illustrate, the data suppliers lead to transmit forged or deceptive information and become unauthentic. In this case, the traditional security methods are ineffective in mitigating such an issue. Unlike security, trust is defined as the features related to the sensors, such as their reputation, accuracy, and sincerity. By combining several, possibly contradicting pieces of information from many sources of information, the process of information fusion makes it possible to forecast and evaluate scenarios [3]. The major goal of this strategy is to combine data from these various data sources to produce an explicit, inclusive, and yet integrated estimation of the situation. Sensors generate information as an information source. This data is gathered by the sink node(s), which then fuses the data. Alteration, decreasing, integration, and replacement are all possible steps in the information fusion process. Ultimately, a product is created that is more valuable than what might be anticipated from a single information source.

The biggest difficulties in resolving behavioural concerns like the dependability, integrity [4], and correctness of information sources come up during the information fusion process. These difficulties are numerous. First, a sink node or information source may not be trustworthy. This implies that they may purposefully alter combined or agglomerated datasets. Next, a dishonest information source may deliberately lie to present false information for their own interest. Furthermore, accurate rates of information from reliable sources can vary depending on the personal trust characteristics that are difficult to define.

There are diverse accuracy rates because nodes may estimate the same circumstance in different ways. The principle of accuracy permits review-based systems to function with approximate metrics by design. So, before relying on the fused information, certain criteria including the dependability, integrity, and correctness of the information sources and the sink nodes must be guaranteed [5]. Figure 1 is utilized to illustrate the structure of the trust-based data fusion model. There are three main layers that make up this system.

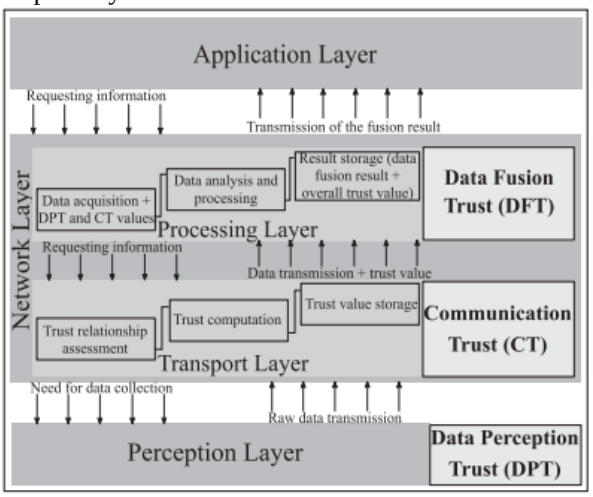

Fig. 1.Trust-oriented data fusion architecture overview

Each layer's data fusion viewpoint has been covered below:

1) Perception Layer: Many technologies, including RFID and sensors, are included in this layer. The RFID technique focuses on locating and tracking things, whereas the sensor nodes are employed to find and collect data on ambient conditions [6]. The Data Perception Trust (DPT) in this layer needs to be estimated. Each sensor must assess the accuracy of its own sensed data in order to identify any inaccurate calculations. In fact, a number of internal and external factors, such as resource scarcity and environmental conditions, among others, might affect the quality of sensed data. Each node must therefore address these issues and evaluate the accuracy of its readings before engaging in communication. In the network, only the most trustworthy data needs to be transferred. In order to protect the reputation of the sensor and keep the same degree of trust in it, the DPT guarantee primarily enables the detection of unexpected dangers.

2) Network Layer: This layer makes it possible to broadcast, examine, and analyse data [7]. The transport layer and the processing layer are the two sub-layers that typically make up this layer. The divide is done to give each sub-layer convenient trust levels

a) Transport Layer: Nodes in this layer are constantly exchanging data with one another. To ensure that data may transfer between nodes without being affected or changed, the communication trust between objects must be assessed. Assessment of communication trust between nodes often depends on their interaction and communication over time. This trust level can be used to identify selfish and malicious nodes that deliberately refuse to connect with nearby nodes in an effort to trick the network [8]. Data trust and object trust are both parts of communication trust. The object trust is usually the focus of current trust management stages. The entity trust typically piques the interest of current trust management plans. Individuals consider that if an object has a high level of trust, then the information it reports must be reliable..

b) Processing layer: To provide an output that is dependable and trustworthy, the main emphasis is on analysing, and integrating the data obtained from this layer. A notion is considered which implies that the Data Fusion Trust determines whether the fusion strategy is effective to lay impact on the trust in the information or not. Therefore, a few conditions must be met to guarantee the output of the fusion is of excellent quality. First, only reliable nodes ought to be chosen as data aggregators. Second, in the context of fusing DPT and CT, only trusted nodes should participate in the fusion. Third, the data quality should be enhanced through the data fusion procedure.

3) Application Layer: The ultimate clients receive a wide range of intelligent services from this tier. According to the users' needs, different information can be extracted from the same detected data. The necessary Internet of Things services must precisely meet consumers' needs at the appropriate time and location [9]. The accuracy of the fusion result and the calibre of the sensed data are the two key determinants of service quality. Several businesses, such as logistics management, location-based services, the environment, transportation, healthcare, public safety, etc., may benefit from these facilities.

To guarantee the trustworthiness of the provided information, a level of trust surety is not enough. Henceforth, the avoidance of evaluating the trust at any level leads to impact the reliability of the information.

B. Data fusion trust assurance in the IoT

Even though, the surety of Data Perception Trust and CT is given, maintaining the accuracy of the data is required for Data Fusion Trust. In terms of security, energy usage, compute, and storage capacity, fusion node performance has a significant impact on the DFT. The following is a discussion of well-known DFT systems which are employed in Wireless Sensor Network assisted IoT:

1) Witness-based approach: This method presupposes that in addition to the witness nodes, the network also consists of sensor nodes and data aggregators. To confirm or deny the outcome of the data aggregator, a witness might act as a node in a data fusion network [10]. A data aggregator gathers testimony from witnesses to confirm the validity of the outcome. Each witness serves as a gauge for the achieved fusion outcome's Message Authentication Code (MAC). The witness ID, the key, and the fusion outcome make up the MAC. With the sink node, each witness exchanges a special secret key. As witnesses cannot directly communicate with sink nodes, the key goal is to prevent the fusion node from formulating the data whose aggregation is done. Afterwards, the n-out-of-(m+1) approach is adopted in this method for validating the accuracy.

Retrieval Number: 100.1/ijrte.B78090712223
DOI: 10.35940/ijrte.B7809.0712223
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

2) Weighted-trust evaluation (WTE): It stands for a node's credibility and shows how each report affects the final judgement. Three layers make up the IoT architecture. Sensor nodes make up the top layer [11]. The next layer is made up of forwarding nodes, which are responsible for updating the weights of each sensor node in the cluster, computing the results of the fusion, and passing the information on to the following layer. In fact, the sensor node will be penalised and have its WTE reduced if the fusion result does not match the data it provided. The number of nodes producing distinct reports and the total number of sensor nodes in the same cluster are what determine the penalty level.The involved entity will be labelled as hostile if WTE falls below a predetermined limit. The last layer eventually consists of APs to check the validity of the data received. Each forwarding node (FN) is given a weight by the APs, who then deduct the newly acquired outcome prior to transmit it to the wired network.

3) Double Cluster Heads Model (DCHM): MCH and VCH are necessary for this framework to function. These two objects are used to combine the data and store the outliers in two different indexes. This data will then be transmitted to the base station for evaluating the dissimilarity coefficient amid 2 outcomes so that the perfection of cluster head and vice-cluster head function is computed. The fundamental goal of this model is to choose reliable CHs. This model based on the idea of transmission of re-selected message within the cluster, whenever a CH or VCH's remaining energy drops to a specific threshold [12]. Hence, the CH and VCH positions will be filled by the two individuals with the highest levels of trust and energy left.Several responsibilities are always played by aggregation nodes. But, it must first evaluate how reliable the fusion outcome is. In order to estimate the reliability and correctness of the fusion outcome in accordance with the earlier allocations, this framework uses a Bayesian data fusion technique.

II. LITERATURE REVIEW

I. Souissi, et.al (2019) suggested a detailed evaluation of TMs (trust models) in accordance with a set of vital criteria such as robustness, overhead and scalability [13]. These frameworks were ineffective in integrating (Data Perception Trust), CT (Communication Trust) and DFT (Data Fusion Trust) methods and meeting the demands of all of the mentioned criteria. Moreover, the major focus was on suggesting novel systems in which the given methods were integrated for improving the process to make decisions based on trust for fusing the data in IoT (Internet of Things). Furthermore, an adaptive TMM (trust management model) was put forward. The suggested approach performed well to adjust the resources of the object concerning the specifications of Internet of Things applications.

Y. Liu, et.al (2022) developed a block chain-based STMS (semi-centralized trust management system) model in single and multiple domains [14]. The cloud servers are exploited to centralize and organize the IoT (Internet of Things) devices. These servers assisted in sustaining a rating data ledger in every domain to build the presented rotation-based consensus protocol in a decentralized way for supporting the cross-domain data exchange. A computational trust system was developed when the direct and indirect trust information was aggregated for evaluating the trust value of dynamic malicious devices. In the end, experiments were carried out for simulating the investigated model in diverse circumstances. The experimental outcomes reported that the investigated model was feasible to recognize the malevolent devices and alleviate their impact of malevolent devices.

N. Li, et.al (2019) presented a novel CAT (context-aware trust) model for lightweight IoT (Internet of Things)devices [15]. A reliable overview of a service provider was offered for which the past behaviour records were not stored. A trustor was capable of deciding the importance of context items. Consequently, the distinctive decisions were obtained under a similar trustworthiness record. Diverse assaults were launched to compute the presented model. The results validated the resistance of the presented model against various assaults, namely bad-mouthing attacks and on-off attacks. Moreover, the impact of some significant metrics was also defined.

A. A. Adewuyi, et.al (2019) introduced a new framework known as CTRUST [16]. This framework was utilized to parametrize the trust in a precise way and deployed belief functions for computing the recommendations. A study was conducted on the impact of trust decay and maturity on the procedure of evaluating trust. Suitable mathematical functions were employed to model every trust element. The utility derived and its trust accuracy, convergence, and resiliency are considered to simulate the introduced framework in a collaborative download application. The results demonstrated that the introduced framework was effective concerning efficacy and security.

A. Kavitha, et.al (2022) projected a secure and sustainable trust mechanism [17]. This system was useful for recognizing the malevolent nodes and enhancing the cooperation of motes. The direct and indirect trust is utilized to distinguish the authentic nodes from the malevolent ones. The packet-forwarding behaviour of a node was considered to evaluate the direct trust. A novel two-hop model was put forward for observing the packet forwarding behaviour of neighbours. The weighted D-S theory helped to evaluate the indirect trust when the recommendations were aggregated. In this theory, a new similarity system of correlating the recommendations, provided by diverse neighbours, was implemented to measure the weight. Various interactions are employed for counting the dynamic weight computation. The results depicted that the projected mechanism was efficient and resilient against packet drop/modification assaults, bad-mouthing, on-off attacks, and collusion assaults on the NS-2 simulator.

B. Shala, et.al (2020) developed an optimized trust framework with a MATW (multi-layer adaptive and trust-based weighting) system [18]. Furthermore, the trust was evaluated using dissimilar trust metrics and their mathematical models.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Thereafter, an innovative technique was suggested for executing incentivization procedures in the IoT marketplace. For this, control loops and smart contracts were employed. The major aim was to encourage the participants to continuously enhance their behaviour. In the end, the reliability of the developed framework was proved. The experimental outcomes indicated that the developed framework was robust against a number of assaults in comparison with the traditional methods in dissimilar scenarios. W. Ma, et.al (2021) designed an ML (machine learning) empowered TE (trust evaluation) technique [19]. ADL (deep learning) algorithm implemented for aggregating the trust properties of network QoS (Quality of Service) for constructing a behavioural framework for a given IoT (Internet of Things) device. The behavioural framework predicted the similarity between real network and network behaviours which was further computed to measure the trust. Trust values were capable of illustrating the trust status of a device and helped to make the decision. At last, the designed technique was quantified in the experimentation. The results reported that the designed technique was efficient.

N. Javaid, et.al (2022) recommended a blockchain-based trust framework for WSN IoTs (Wireless Sensor Internet of Things) [20]. In addition, the Dijkstra algorithm was implemented for suggesting a routing protocol to establish communication among network nodes efficiently and avoid invalid holes amid ordinary sensor nodes and BS (base station). Besides, transparency was offered in the network by recording the transaction of nodes in the blockchain immutably. PoA (Proof of Authority) consensus algorithm was presented and adopted for validating and adding the transactions in the blocks. The data was stored reliably and cost-effectively using a distributed platform called an interplanetary file system. The simulation outcomes proved that the presented algorithm led to enhance the system by up to 13% as compared to others. Moreover, the recommended framework proved robust concerning gas utilization, throughput, status of nodes and energy usage.

E. M. Abou-Nassar, et.al (2020) formulated a Blockchain DIT (Decentralised Interoperable Trust) model for IoT (Internet of Things) zones [21]. In this, a smart contract ensured that the budgets were authentic and ITIS (Indirect Trust Inference System) assisted in mitigating the semantic gaps and improving TF (trustworthy factor) estimation using the network nodes and edges. A private Blockchain ripple chain is utilized for creating reliable communication. For this, the nodes were validated on the basis of their inter-operable structure to deploy controlled communication for tackling the issues regarding fusion and integration. Moreover, Ethereum and ripple Blockchain are considered for associating and aggregating requests over trusted zones. The formulated model was more scalable, interoperable, mutually authentic, reliable and kept the data confidential and secure as compared to other methods.

G. Joshi, et.al (2021) suggested an L/W- HMT (Light-weight Hidden Markov Model) to evaluate the trust so that the impact of compromised nodes was diminished and the storage of redundant data was constricted for lessening the overhead, memory, and energy consumption [22]. A 2-state HMM (Hidden Markov Model) was presented with a reliable and compromised state. The state was transformed on the basis of the number of packets whose transmission, dropping, modification, and receiving were done. The FLF (forward likelihood function) is implemented for computing the trust value of the node. The simulation results on MATLAB confirmed the supremacy of the suggested approach as it enhanced DR (detection rate) by up to 6%, PDR (packet delivery rate) by up to 8% and energy consumption by around 70%.

M. Ebrahimi, et.al (2022) established a DSTM (decentralized service-oriented trust management) algorithm for healthcare IoT (Internet of Things) [23]. The evidence distance is employed for providing the healthcare information providers and punishing the malevolent units. The context-aware framework was deployed for estimating the trust on the basis of direct experiences and indirect feedback from recommenders. The combinatorial laws of evidence theory and indirect trust values were considered for estimating the trust of a source or service. The security of the established algorithm was proved against bad-mouthing, good-mouthing, and on-off attacks in terms of dynamic metrics. The results depicted that the established algorithm was robust and effective.

F. Li, et.al (2022) presented a trust model for recognizing trusted service providers in a dynamic IoT (Internet of Things) environment prior to negotiating an SLA [24]. This model focused on generating a trusted credit for illustrating the SLA's fulfilment and possible negotiation success rate on the basis of historical information regarding earlier negotiations and the monitored run-time efficacy of the system. Rough Set theory was adopted for forecasting the negotiation success rate. The possibility of SLA violation was assumed using BI (Bayesian Inference) in accordance with the monitored data. The simulation outcomes revealed that the presented model was feasible and efficient.

III. RESEARCH METHODOLOGY

In clustered wireless sensor network, the major necessity is to distribute the nodes randomly. The process of distributing the sensor nodes (SNs) randomly, results in generating the cluster heads (CHs). Consequently, various issues have occurred. Avoiding the disposability of the CH becomes significant because of the occurrence of the issue of energy usage. The next priority is to stop long-distance connectivity in CH and place the nodes underneath them. The proposed standards having inefficiency are not able to choose the nodes and the nodes which are selected are known as CH. The circumstances of the nodes lead to cause complexity in their presence in the network and in remote regions. Hence, unsuitable nodes are created. With the maximization of intra-cluster energy, the nodes are considered as CHs. Unlike the receiver and SNs, authentic motes do not utilize much energy. The generation of a wide spectrum on the system synchronically leads to mitigating the battery energy usage in the nodes. The major concentration is on selecting the parent node for every CH for separating the actions. Afterwards, maximum production is obtained.

Retrieval Number: 100.1/ijrte.B78090712223
DOI: 10.35940/ijrte.B7809.0712223
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Every SN makes the implementation of 2 value functions that assist them in selecting the CH. The degree of nodes is considered for creating the functions, and their distance towards the sink is found for computing the potential of neighbour motes. The generation of the CH requires the construction of nodes with a greater degree. In order to minimize expensive communications, the higher degreed CH can encompass a large number of nodes. After reducing the energy that the nodes need, the network's lifespan is thus lengthened. The first phase focuses on sending a Hello message with an identity. The SS is considered for computing the distance between the sink and every mote. Moreover, its main goal is to transfer an INTIAL-MSG containing an ID and distance amid every node and sink. The computation of distance amid node and adjacent nodes is also performed. The node deploys a computation technique to measure the CH illustrated within eq. (1) as:

$$R_{CH} = R_{min} * [1 + (\frac{d_{BS} - d_{BSmin}}{d_{BSmax} - d_{BSmin}})] \quad (1)$$

In this, R_{min} is used to denote the smallest size of the cluster whose utilization is done as a metric of the protocol, the distance from adjacent mote to sink is represented with d_{BSmin} and d_{BSmax} is used to show the distance from the furthest node to sink. For each mote, a value is computed using the value function so that the node can be informed of its suitability and selected as CH.

$$F_{CH-value} = \alpha * N_{deg} + \frac{\beta}{MSD_{deg}} + \frac{\gamma}{d_{BS}} \quad (2)$$

The constant weights are denoted with α, β and γ and their values are laid within 0 and 1. The same and adjustable values are assigned to all nodes within the networks. The radius R_{CH} of the number of neighbouring nodes is represented with N_{deg} and the mean square distance amid the neighbouring nodes is denoted with MSD_{deg}. The parameter d_{BS} is used to illustrate the distance from the sink to every node. To calculate the total CHs at a given time, the predicted values are used. Consequently, F (CH-value) is the improved value produced for each mote. To acquire the increased values that fall between 0 and 1, each node monitors the other nodes. Every node is also used to generate a random number between 0 and 1. In the case of the value found below $F_{CH-value}$, the node is taken into account as a candidate and its selection is done as a cluster head. After choosing the nodes as CH, the radius and residual energy are used to compare the nodes. A node that has RE is referred to as a CH. This node provides the ID and broadcast code. All of the available motes in the network are aware of CH's stature. A non-CH mote aids in locating the closest CH, which is determined by the strength of the signal. The intra-cluster communication of energy clusters is found in accordance with the applicable elements such as clusters. The energy used for node radio, distance, and cluster communication has been very expensive. As a result, the intra-cluster power is increased. This study also defines centrality as an important tactic. The lowest distance between the receiver node and the center cluster causes the 2nd power average to decline, reducing the intra-cluster energy. A variety of components have an impact on the energy. The proposed standards, namely cache nodes are unable to select the nodes under harsh situations. The chief purpose is to compute the value of each stage for every non-CH node with the objective of selecting any node as a volunteer node.

$$Access\ Time = H * T_c + (1 - H)(T_c + T_m) \quad (3)$$

H illustrates the cache hit ratio, the access time is denoted with T_c and the main memory access is shown with T_m. These CHs are employed to transmit the collected data to the sink.

IV. RESULT AND DISCUSSION

MATLAB is a kind of package using which numerical computations such as addition and subtraction etc. can be done and complex functions can be executed such as technical computation, graphics and animation. The simulations performed are represented in table 1.

Table. 1. Simulation Parameters

Parameter	Description	Value
A	area of network	(0, 0)–(200, 250)
L-BS	BS location	(150, 250)
N	number of nodes in network	100
$E_{initial}$	initial energy of all nodes	0.5 J
E_{fs}	free space channel model	50 nJ/bit
E_{mp}	multi-path fading channel model	0.0013 pJ/bit/m^4
d_0	distance threshold	87 m
E_{DA}	data aggregation energy	5 nJ/bit/signal
DP size	data packet size in bit	4000
CP size	control packet size in bit	200

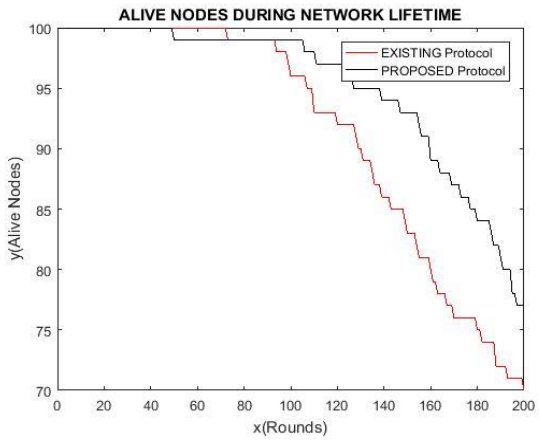

Fig. 2. Alive Nodes Consumption

Figure 2 illustrates that the base paper is compared with the suggested method. The proposed method is the improvement of the CTNR protocol in which gateway nodes are deployed for communication.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

When the energy consumption is reduced number of alive nodes is increased in the network as compared to the CTNR protocol.

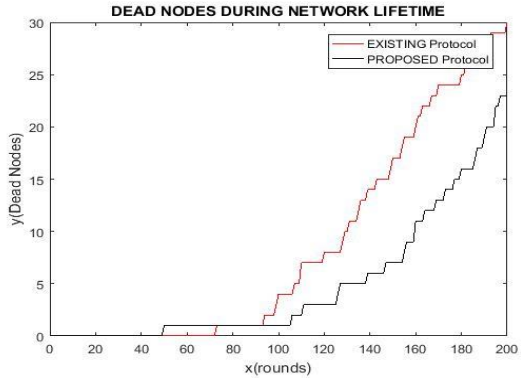

Fig. 3. Number of Dead Node Comparison

Figure 3 revealed that the LEACH protocol is compared with cache technique with regard to the dead nodes. Few dead nodes are comprised in the suggested protocol within the given rounds. The deployment of cache nodes in the network assists in diminishing the energy consumed by the nodes. The reduction in energy consumption of the network results in the mitigation of amount of dead nodes.

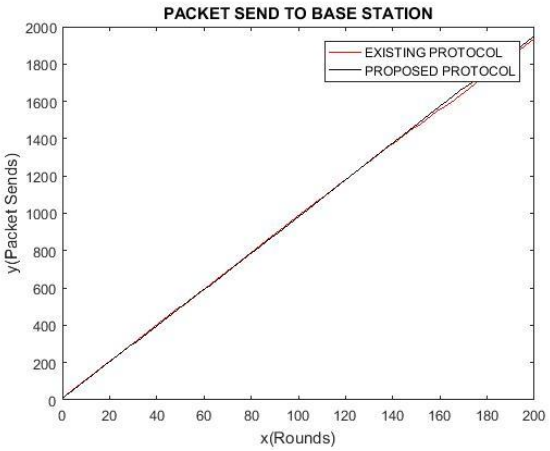

Fig. 4. No of Packets Transmitted

Figure 4 demonstrates the transmission of the number of packets to the sink using the suggested method, which is compared with the base paper, LEACH and cache method. The suggested method is able to transmit a huge number of packets as compared to the other methods. The alleviation of the number of dead nodes in the network leads to transmitting more packets to the sink.

V. CONCLUSION

The CTNR is an energy-efficient routing algorithm that has the potential for enhancing the duration of WSN. In this research work, the CTNR protocol is enhanced using gateway nodes. In the proposed protocol, the whole network will be divided into clusters using location-based clustering. The distance and energy are considered to select CH in each cluster. The sensor node having a shorter distance to sink and maximum energy will be selected as the cluster head. The nodes which are unable to be selected as cluster heads will be elected as leader nodes based on the energy. In the last, the gateway nodes will be deployed in the network. The sensor nodes transmit information to the cluster head which will be later transmitted to leader nodes and leader nodes will transmit information to the gateway node. The gateway node is used for transmitting the information to the sink. MATLAB is executed to simulate the suggested approach and no. of alive nodes, dead nodes and the number of packets transmitted in the network are considered for analysing the outcomes. The results exhibit that the suggested approach is effective for mitigating the no. of dead nodes, and increasing the no. of alive nodes and transmitted packets, as compared to an existing technique.

DECLARATION

Funding/ Grants/ Financial Support	No, I did not receive.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors having equal contribution for this article.

REFERENCES

1. G. Fortino, L. Fotia, F. Messina, D. Rosaci and G. M. L. Sarné, "Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges," in IEEE Access, vol. 8, pp. 60117-60125, 2020 [CrossRef]
2. R. Rani, S. Kumar and U. Dohare, "Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8421-8432, Oct. 2019, [CrossRef]
3. E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O. -Y. Song, A. K. Bashir and A. A. A. El-Latif, "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems," in IEEE Access, vol. 8, pp. 111223-111238, 2020 [CrossRef]
4. M. Bahutair, A. Bouguettaya and A. G. Neiat, "Multi-Perspective Trust Management Framework for Crowdsourced IoT Services," in IEEE Transactions on Services Computing, vol. 15, no. 4, pp. 2396-2409, 1 July-Aug. 2022 [CrossRef]
5. S. V. Shankhpal and S. H. Brahmananda, "Design and Development of trust management scheme for the Internet of Things based on the optimization algorithm," 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 2020, pp. 207-211 [CrossRef]
6. A. Salunke and S. Bhambar, "Comparative Study of Trust and Reputation Security Models in IoT Networks," 2019 International Conference on Intelligent Computing and Control Systems (ICCS), Madurai, India, 2019, pp. 830-835 [CrossRef]
7. Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian and J. Zhang, "A Semi-centralized Trust Management Model Based on Blockchain for Data Exchange in IoT System," in IEEE Transactions on Services Computing
8. S. Asiri and A. Miri, "A Sybil Resistant IoT Trust Model Using Blockchains," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1017-1026 [CrossRef]

9. K. M. Sadique, R. Rahmani and P. Johannesson, "Trust in the Internet of Things: An architecture for the future IoT network," 2018 International Conference on Innovation in Engineering and Technology (ICIET), Dhaka, Bangladesh, 2018, pp. 1-5 [CrossRef]
10. C. V. L. Mendoza and J. H. Kleinschmidt, "Defense for selective attacks in the IoT with a distributed trust management scheme," 2016 IEEE International Symposium on Consumer Electronics (ISCE), Sao Paulo, Brazil, 2016, pp. 53-54 [CrossRef]
11. Z. Lin and L. Dong, "Clarifying Trust in Social Internet of Things," in IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 2, pp. 234-248, 1 Feb. 2018 [CrossRef]
12. C. Lewis, N. Li and V. Varadharajan, "Targeted Context-based Attacks on Trust Management Systems in IoT," 2023 in IEEE Internet of Things Journal [CrossRef]
13. I.Souissi, N. B.Azzouna and L. B. Said, "A multi-level study of information trust models in WSN-assisted IoT", Computer Networks, vol. 151, pp. 12-30, 14 March 2019 [CrossRef]
14. Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian and J. Zhang, "A Semi-centralized Trust Management Model Based on Blockchain for Data Exchange in IoT System," in IEEE Transactions on Services Computing, vol. 24, no. 3, pp. 782-794, 2022
15. N. Li, V. Varadharajan and S. Nepal, "Context-Aware Trust Management System for IoT Applications with Multiple Domains," 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), Dallas, TX, USA, 2019, pp. 1138-1148
16. A. A. Adewuyi, H. Cheng, Q. Shi, J. Cao, Á. MacDermott and X. Wang, "CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5432-5445, June 2019 [CrossRef]
17. A. Kavitha et al., "Security in IoT Mesh Networks Based on Trust Similarity," in IEEE Access, vol. 10, pp. 121712-121724, 2022[CrossRef]
18. B. Shala, U. Trick, A. Lehmann, B. Ghita and S. Shiaeles, "Blockchain and Trust for Secure, End-User-Based and Decentralized IoT Service Provision," in IEEE Access, vol. 8, pp. 119961-119979, 2020 [CrossRef]
19. W. Ma, X. Wang, M. Hu and Q. Zhou, "Machine Learning Empowered Trust Evaluation Method for IoT Devices," in IEEE Access, vol. 9, pp. 65066-65077, 2021 [CrossRef]
20. N. Javaid, "A Secure and Efficient Trust Model for Wireless Sensor IoTs Using Blockchain," in IEEE Access, vol. 10, pp. 4568-4579, 2022 [CrossRef]
21. E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O. -Y. Song, A. K. Bashir and A. A. A. El-Latif, "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems," in IEEE Access, vol. 8, pp. 111223-111238, 2020 [CrossRef]
22. G. Joshi and V. Sharma, "Light-Weight Hidden Markov Trust Evaluation Model for IoT network," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2021, pp. 142-149 [CrossRef]
23. M. Ebrahimi, M. S. Haghighi, A. Jolfaei, N. Shamaeian and M. H. Tadayon, "A Secure and Decentralized Trust Management Scheme for Smart Health Systems," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1961-1968, May 2022 [CrossRef]
24. F. Li, G. White and S. Clarke, "A Trust Model for SLA Negotiation Candidates Selection in a Dynamic IoT Environment," in IEEE Transactions on Services Computing, vol. 15, no. 5, pp. 2565-2578, 1 Sept.-Oct. 2022. [CrossRef]

AUTHORS PROFILE

Mr. Ayush Sharma Pursuing his Ph.D. in Computer Science & Engineering from Guru Kashi University, Talwandi Sabo (Bathinda) Punjab, India. He did his Post graduation, M.Tech in Computer Science and Engineering from SPIET Affiliated to MDU University, Rohtak. Currently, he is working as an Assistant Professor in the Department of Computer Science and Engineering, at Guru Jambheshwar University of Science & Technology, Hisar. His research interest is WSN and IoT.

Dr. Sunny Arora was awarded his Ph.D. in Computer Science & Engineering from Guru Kashi University, Talwandi Sabo (Bathinda) Punjab, India. He did his Post graduation, M.Tech in Information Technology from KSOU, Mysore. Currently, he is working as a Professor in the Department of Computer Science and Engineering, at Guru Kashi University, Talwandi Sabo (Bathinda), Punjab, India. His research interest is WSN and IoT.