International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: 10 September 2023 Revised: 20 October 2023 Accepted: 30 October 2023

Swarm Intelligence-Optimized Energy Management for Prolonging the Lifetime of Wireless Sensor Networks

[1]Amuthavalli L, [2]Dr.K.Muthuramalingam

[1]Research Scholar, Department of Computer Science, Bharathidasan University, Tiruchirappalli, Tamil Nadu, India – 620023.
[2] Assistant Professor, Department of Computer Science, Bharathidasan University, Tiruchirappalli, Tamil Nadu, India – 620023.

Abstract
Recent technological and industrial progress has enabled the development of small, high-performing, energy-saving, affordable sensor nodes that possess the potential to adapt, be self-aware, and self-organize. These nodes are designed for versatile communications applications. Sensor networks for sustainable development focus on the ways in which sensor network technology can enhance social development and improve living standards without causing harm to the environment or depleting natural resources. Wireless sensor networks (WSNs) offer undeniable benefits in various fields, including the military, healthcare, traffic monitoring, and remote image sensing. Given the constraints of sensor networks, varying degrees of security are necessary for these critical applications, posing difficulties in the implementation of conventional algorithms. The issue of security has emerged as a primary concern in the context of IoT and smart city applications. Sensor networks are often regarded as the fundamental building blocks of IoTs and smart cities. The WSN encompasses a routing algorithm, network strength, packet loss, energy loss, and various other intricate considerations. The WSN also addresses intricate matters such as energy usage, a proficient approach for picking cluster heads, and various other concerns. The recent growth of Wireless Sensor Networks (WSNs) has made it increasingly difficult to ensure the trustworthiness and reliability of data due to the distinct features and limitations of nodes. Hostile nodes can easily damage the integrity of the network by inserting fake and malicious data, as well as launching internal attacks. Trust-based security is employed to detect and identify rogue nodes, providing a robust and adaptable protection mechanism. Trust evaluation models are crucial security-enhancement mechanisms that enhance the reliability and collaboration of sensor nodes in wireless sensor networks. This study recommends the use of DFA UTrust, a unique trust technique, to effectively satisfy the security requirements of WSNs.
Keywords: Trust, Dragonfly, K-means, Lifetime enhancement, Sustainability.

1. INTRODUCTION

A wireless sensor network utilises a collection of sensor nodes to transmit the necessary data for the network. Wireless Sensor Networks (WSN) find extensive use in several domains including weather forecasting, military operations, underwater research, and more, to collect and store reliable data. The user's text consists of three consecutive references: [1], [2], and [3]. A sensor node comprises a transceiver, external memory, microcontroller, power source, and one or more sensors. After being deployed, it is not possible to replace the battery of the sensor node. As the energy level decreases, the performance of the node also decreases. Ultimately, the sensor node that has depleted its battery ceases to function, resulting in the termination of all communication with other nodes in the network. An overview of the duration of network operation as a result of increased energy consumption [4][5].

Conserving energy is crucial for enhancing network efficiency and hence extending the network's lifespan. There exist multiple approaches to enhance longevity and energy efficiency. Trust management is a strategic approach.

1.2 Trust Management Model Working

In the trust management paradigm, it is a key principle that each node employs a scale referred to as the "Trust Scale" in some manner. Three key values that can be taken into account with respect to this scale are a trust level node that is completely reliable and can be trusted 100%, the initial trust level, and the threshold level [11]. The term "initial trust level" denotes the level of confidence assigned to a node upon its entry into the network, in the absence of any additional data regarding its reliability from its trustors. The threshold at which a node is considered unreliable is referred to as the "cut-off level". Every node must actively participate in the trust management process and consistently update its records of other nodes' reputations. The Trust Table is generated as a result of this particular data structure. Each record in the trust database is assigned a trust value based on the trust scale. Table1 can be utilised to exhibit a fabricated illustration of a trust table derived from the provided network example for node1.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: 10 September 2023 Revised: 20 October 2023 Accepted: 30 October 2023

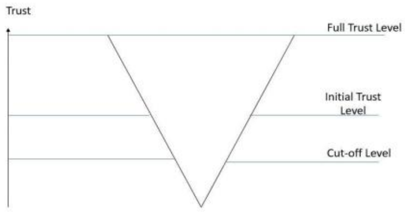

Figure 2: The Trust Scale

Table 1: Dummy example of Trust values of different nodes in the network

ID of Node	Value of Trust
9	0.51
11	0.66
13	0.74
17	0.48

A node has the ability to grant approval to any other node, excluding itself, by referencing the entries in the trust table. The method is referred to as "Recommendation" [6]. Based on this, it is possible to construct a model that generates a trust table that includes information about each node in the network. The following entities, which can serve as components of the trust table, also include each node, message, trust table item, and node's reputation. The model is executed using cycles, each of which comprises two distinct phases: the data phase and the recommendation phase.

The following is a summary of the contributions made by this paper:

i. The literature suggests that both SI algorithm architecture and machine learning architecture can be used to enhance trust in sensor nodes.

ii. The report presents the proposed work design and execution, together with the trust model built for the sensor nodes.

iii. The objective is to establish a network characterised by a high level of trust, hence minimising resource wastage and ensuring the network's longevity.

The suggested technique is assessed by comparing it to reward-based routing strategies, employing QoS metrics like as throughput, PDR, and latency.

The rest of the article is written in the following way. Section 2 illustrates the related work. Section 3 states the problem statement. Section 4 presents the detailed work architecture of the proposed algorithm. Section 5 contains the result and analysis. Section 6 gives the conclusion and future scope.

2. RELATED WORK

WSN sensors have seen a significant revolution in their design throughout time. The consideration of sensor development encompasses factors such as their lightweight nature, compact dimensions, and minimal energy consumption. Battery depletion remains a significant issue, leading to delays in data sensing and transmission. The study on methods to ensure network stability and minimise energy consumption and end-to-end delay during data transfer has intensified due to the increasing impact of Wireless Sensor Networks (WSN) in real-world applications. The concept of trust management has also been significant over time. The current research demonstrates the diverse trust management strategies and models employed in the domain of Wireless Sensor Networks (WSN).

The author explored the notion of trust models, which can be categorised into three distinct types: "centralised," where the primary emphasis is on the central node of the network, which assesses the reliability of a node based on the trust data it has collected independently or from other nodes in the network; secondly, "hierarchical," where the network is divided into clusters or groups, and the cluster head is responsible for evaluating the trustworthiness of a node; and This study provides a concise overview of the potential dangers and limitations associated with the lifespan, network capacity, and capabilities of nodes in a network. It also highlights the restrictions and hazards related to the network's lifetime and bandwidth. The purpose of this study is to develop and apply a trust model that enhances security [12].

In addition to the achievements WSN has achieved with its trust model, there are also several attacks that target these trusted models. These attacks diminish the efficacy of the trust paradigm. Examples of attacks include "defamation," "intermittent reinforcement," "discriminatory behaviour," "dissociative identity disorder," and "novice," among others. An explanation of the trust model for Wireless Sensor Networks (WSN) is provided, along with a collection of recommended procedures that are considered to be the most effective. Optimal methods involve considering trustworthiness and credibility, trust in the central hub, gathering primary and secondary information, initial values, level of detail, updating and deterioration, risk and significance, as well as trustworthiness and credibility. Through the analysis of different trust management strategies, it has been established that a set of optimal practices should be considered when developing a successful trust model for WSN [13]. The authors analysed the different trust models used in conventional WSNs and clustered WSNs. There are two types of trust models available for popular Wireless Sensor Networks (WSNs): Node trust models and Data trust models [14].

The authors introduced a novel approach called ESRT. This is a unique routing system that uses trust and energy as key factors to ensure efficient routing and adaptability in the presence of malfunctioning nodes and their actions during packet forwarding. This approach takes into account confidence that is spread out or scattered. When exposed to different quantities of problematic nodes and fluctuating network demand, the simulation demonstrates that ESRT outperforms existing methods such as R-AODV and TLB-AODV [15].

The authors presented their research on the data trust model and outlined their approach to identifying defects and restoring data using data correlation techniques. The user's text is "[16]." This study introduces the concept of AF-TNS as a means to improve network security in resource-limited Wireless Sensor Networks (WSNs). The AF-TNS operates in two distinct phases: trust assessment utilising limited energy and node appraisal based on metrics. This guarantees the preservation of the neighbours' level of reliability. The Tran sigmoid function employs a reliable node to guarantee network operation and an unreliable node to streamline the complex decision-making process in the AF. The simulation's results demonstrate that AF-TNS has the dual effect of prolonging the lifespan of networks and enhancing the likelihood of detecting detrimental behaviour. The testing results demonstrate that the AF-TNS technique ensures a minimum delay of 8.5 seconds, energy consumption of 8.53 J, throughput of 149 kbps, and network lifetime of 390 seconds for the delivery of network information. Additionally, it has a lower rate of false detection, standing at a just 1.5%. The text is referenced by the number 17.

This paper introduces the novel secure routing algorithm EATSRA to enhance the routing efficiency and security of WSNs. This approach utilises trust ratings to enhance the identification of attackers in Wireless Sensor Networks (WSN), while employing a decision tree-based routing algorithm to determine the optimal and most secure route. Moreover, the utilisation of spatial-temporal restrictions has been employed to enhance the determination of route choices. Simulation-based testing has demonstrated that the recommended EATSRA performs more effectively by consuming less energy and improving security and packet delivery ratio [18].

The research [20] proposes a robust BTEM technique to mitigate internal attacks and vulnerabilities in nodes. Bayesian estimation is employed to gather both the direct and indirect trust ratings of each sensor node. Subsequently, data correlation is performed to more precisely identify the subset of dependable nodes from which data packets can be transferred. Simulation data indicates that the rate of false positive detection is elevated while identifying and isolating problematic nodes. It possesses a higher level of defensive capability compared to other algorithms such as AF-TNS [17] and Trust Doc [19].

By combining data trust with encryption methods, communication becomes more reliable. In order to minimise the transmission overhead, the proposed solution employed both intra-cluster (CM) and inter-cluster (CH) methods [21]. The HRFCHE via Semi-Markov method is a prediction approach that enhances network lifetime by integrating energy and trust assessment. HRFCHE surpasses competing cluster head election processes [22] by extending network longevity and reducing energy usage by 28% and 34% respectively.

The suggested Multi-Parameter Opportunistic Task Force Evaluation Method (MPOTFEM) is a reliable approach for choosing the suitable Candidate Hub (CH) by utilising an opportunistic parameter. The proposed MPOTFEM system incorporates both the Markov chain and the Preventive Maintenance (PM) concept to evaluate the quality of network maintenance. Our findings indicate that nodes with malicious intent do not become Cluster Heads (CHs) when the number of CH elections is restricted. The simulation results demonstrate that the suggested methodology outperforms the existing ones in maintaining the network's average percentages of active and inactive nodes at 10.82% and 11.36%, correspondingly. The results indicate that the suggested approach yields average enhancements in Packet Delivery Ratio (PDR) and Throughput of 9.14% and 10.56% respectively, in comparison to the commonly employed Cluster Head (CH) election methods [23].

The simulation findings indicate that LEACH-TM outperforms LEACH-SWDN and LEACH in terms of prolonging network lifespan and managing energy usage. Based on an analysis of transmitted data packets, the incorporation of trust value in the Beta-based trust control framework can efficiently reduce the influence of compromised nodes on the selection of cluster heads and maintain the security of third-party routing nodes. This enhancement greatly enhances network security [24].

A trust list can be dynamically generated and simultaneously updated by a trust evaluation process. When utilising the trust list, the data fusion process exclusively considers data from a reliable node. This approach helps reduce transmission expenses and minimise energy consumption. The simulation findings in OMNET++ indicate that the trust model has the ability to enhance the survival duration of nodes and offer a more precise representation of their condition. In addition, the trust model has a greater rate of anomaly identification when compared to the LDTS model. The authors expect that our approach for assessing trust will enhance the precision of sensor data [25].

In addition, the authors proposed the use of data aggregation and a multi-hopping technique, along with a unique ribbon structure that is related to C-MAC. Reducing the time intervals for data aggregation increases the level of energy conservation. The suggested study can likewise be employed for event detection [41].

The authors suggested an enhanced method for finding a path using the Q learning model from reinforcement learning. This is employed to strengthen the reward-based learning mechanism, which improves the quality of service (QoS) characteristics and decreases the observed delay in general wireless sensor network (WSN) connection [42].

The presence of a dispersed network or cloud highlights the importance of trust in providing security, privacy, and dependable communication in the network [43].

An EEPC protocol has been introduced [44] to enhance network longevity and facilitate environmental tracking and monitoring.

The system utilises improved Particle Swarm Optimisation (PSO) and integrates data from several sensors. A novel strategy is proposed to mitigate the prevalent selfish behaviour in the network by distributing credit across nodes. An agent is assigned to handle credits based on the trust value of each node [45].

3. THE PROBLEM FORMULATION

A network is a grouping of sensor nodes that are spread in a random manner. Certain sensors are categorised as transmission sources, whereas others serve as intermediate nodes. Malicious sensors attempt to hinder network performance by participating in route establishment activities. Each sensor is required to actively engage in the routing process. Each sensor possesses a preventative log containing nodes that exhibit improper behaviour, as well as a dependable register that stores the trustworthy values of these nodes. The routing table of each node will be expanded to include additional entries that consider the dependability of other nodes.

The issues can be summed up by asking the questions below:

i. According to the query, which nodes in the deployed network can be considered trustworthy?

ii. What is the method for establishing an accurate trust threshold that can effectively differentiate between reliable and malicious nodes?

iii. How may misbehaving nodes in a network be detected?

iv. Which nodes should be considered as the most optimal next hop in the route to reduce power usage and enhance the longevity of the network?

4. THE PROPOSED WORK OF THE SYSTEM

A proposed model can be utilised to ascertain the underlying reasons for enhancing the longevity of the network by augmenting the security and trust aspect. The model outlines the relationship between the service consumer and service provider. By submitting a path Request, the service user seeks the optimal route from the service provider to effectively transmit their information to the desired destination with dependability. If there is a reliable path available to transmit the data at the designated time, the service provider will notify the service consumer by sending an acknowledgment instead. There are numerous occupations being executed within the service provider's vicinity. The phrase "Service Layer Structure" denotes the act of associating a specific number of nodes in a Node List with this particular structure. The term "service-oriented architecture" is derived from the fact that all information exchanges are conducted through services, which meet specific demands and facilitate effective communication. The contribution The architecture of interconnected nodes in a service-oriented manner involves the use of provisioning blocks, and consumers initiate requests for data access. The suggested technique involves equipping each sensor node with a diverse range of sensing and buffer capabilities. These nodes are then deployed in a heterogeneous environment. The source nodes refer to the specific nodes that store the data requested by the user. The trustworthiness of the node is assessed based on the evaluated quality of service (QoS) metrics. Implementing the trust value at the node level is tricky due to the fact that each node initially has a trust value of zero and participates in many

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

route forms. The study utilised the swarm intelligence algorithm, which was selected from the list of algorithms in the appropriate task area. The project has been exclusively simulated using MATLAB due to its readily available tools for wireless simulations.

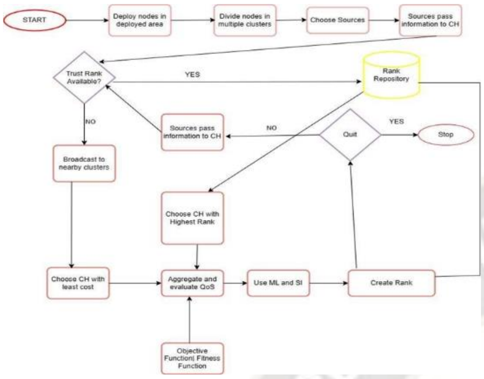

Figure 3: Proposed Work Flow of the System

The work flow of the entire procedure has been discussed in figure 3.

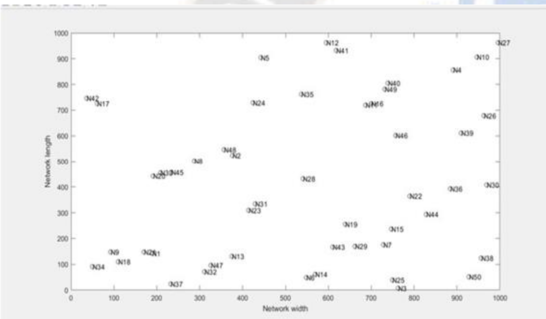

Figure 4: Deployment of network 1000*1000

The LEACH protocol is designed with a cluster-based sensor architecture, where one sensor is designated as the cluster head (CH). Each node has a probability of 1/P to serve as the cluster head again. Every non-cluster head node selects the nearest cluster head and becomes a part of that cluster at the end of each round. Subsequently, the cluster head formulates a transmission schedule for every individual node inside the cluster. Source node and destination node has to be found out in the deployed network. CHs of corresponding source node and destination node is taken in consideration.

The AODV protocol only establishes routes between nodes when requested by source nodes. Consequently, AODV is considered an on-demand method that does not introduce additional network traffic for communication. The routes are maintained as long as the sources necessitate them. In order to establish connections between the members of a multicast group, they also create hierarchical structures known as trees. AODV utilises sequence numbers to ensure the freshness of routes. These systems can adapt to various mobile nodes and are capable of initiating themselves without external assistance. Additionally, they ensure that there are no loops in the network. AODV networks remain inactive until connections are established. Network nodes seeking connections post connection requests.

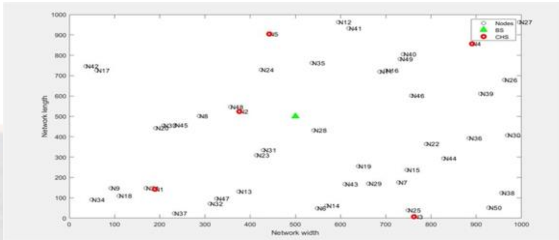

Figure 5: Deployment of 5 Cluster Heads and Base Station

The message is sent by the other AODV nodes, who also record the node that initiated the connection request. Consequently, they construct many temporary pathways to the node that is making the request. The process of transmitting a reverse message over temporary pathways to the inquiring node is carried out by a node that receives such messages and maintains a route to the intended node. The node that initiated the request selects the route with the minimum number of intermediate nodes. Unused entries in routing tables are eventually recycled. If a link fails, the process is repeated and the routing error is returned to the transmitting node.

Route Discovery occurs between the source node and the destination node. The parameters are computed individually for every route. The characteristics include throughput, packet delivery ratio (PDR), power consumption (PC), and delay.

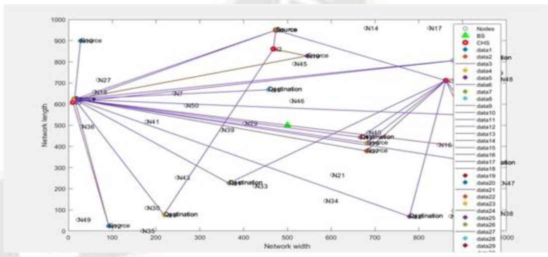

Figure 6: Route Discovery

Due to the existence of various routes and the potential for a single node to be present in multiple routes, it is not possible to determine a definitive dependable route or node. In order to distinguish the best and worst parameters, it is necessary to divide all four parameters into three clusters each.

This can be accomplished using the K-Means technique. K-Means clustering is an unsupervised learning approach that partitions an unlabeled dataset into many clusters. In this scenario, K represents the minimum number of predetermined clusters that must be made during the process. For example, if K=2, it implies that two clusters will be created. Similarly, if K=3, it signifies that three clusters will be formed, and so

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
***Article Received:** 10 September 2023 **Revised:** 20 October 2023 **Accepted:** 30 October 2023*

forth. An iterative approach is employed to partition the unlabelled dataset into K distinct groups. Each cluster consists of only one dataset and possesses a distinct set of attributes. Optimised Sampling is launched based on the Mean Square Error criterion, and subsequently, the Swarm Intelligence technique is employed.

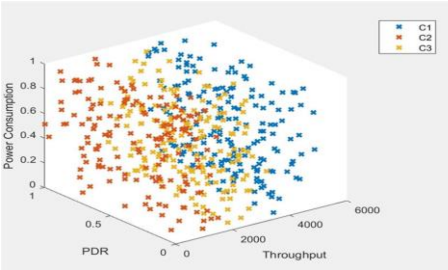

Figure 7: Formation of 3 centroids

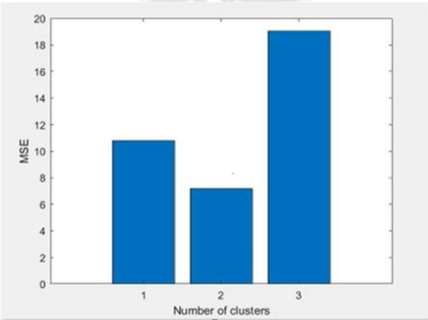

Figure 8: Calculation of Mean Square Error

Sample size selection is classified and then trained by neural network. For sample size selection, Dragon Fly algorithm (DA) is initiated along with its modified behaviour.

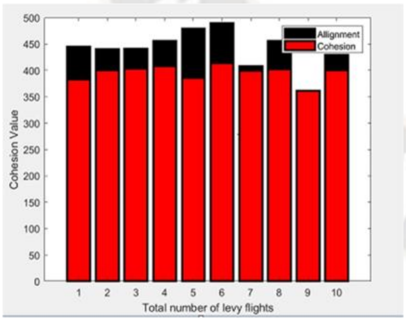

Figure 9: Dragon Fly algorithm initiation

The nodes with high ranks are to be taken into consideration and low ranked nodes are to be avoided. In this way, Trust management is done.

Figure 10: Neural Network

5. EXPERIMENTAL RESULTS AND ANALYSIS

When the proposed algorithm is compared with [41,42], an improvement is seen in terms of throughput, PDR and delay.

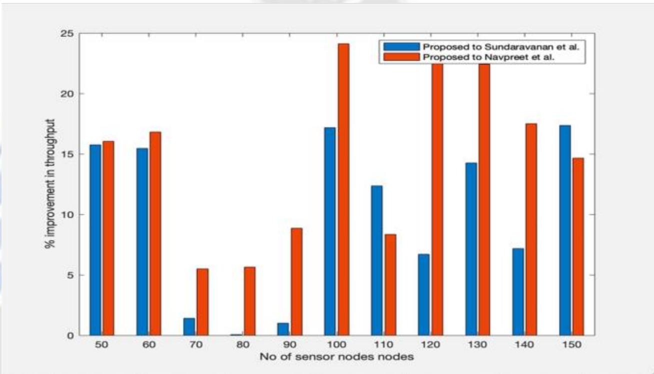

Figure 13: Improvement in Throughput when compared with [41,42]

Delay is the total time taken by the data packets to be delivered from source to destination.

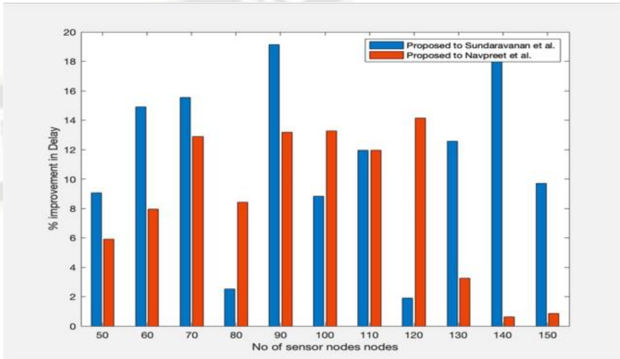

Figure 14: Improvement in Delay when compared with [41,42]

PDR is the packet delivery ratio. It means percentage of packets lost with respect to the number of packets sent.

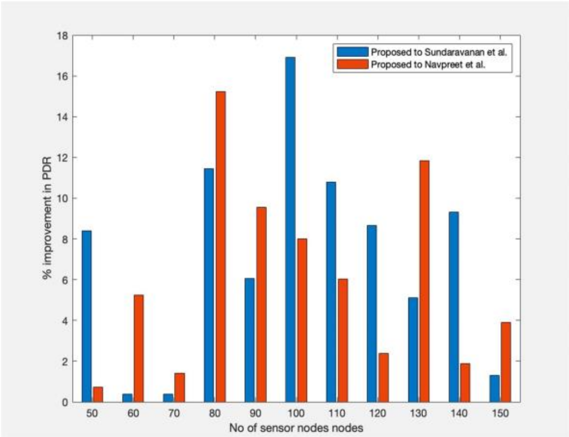

Figure 15: Improvement in PDR when compared with [41,42]

no of sensor nodes'	'Throughput proposed p/s'	'PDR proposed'	'Delay Proposed sec'	'Throughput Sundaravanan et al. '	'PDR Sundaravanan et al. '	'Delay Sundaravanan et al. sec'	Throughput Navpreet et al p/s'	PDR Navpreet et al'	'Delay Navpreet et al.'
50	8844.544879	0.91205625	3.79881182	7641.903609	0.84151247	4.17735199	7620.77881	0.90552069	4.03809015
60	8574.534596	0.90191432	3.36181751	7425.582719	0.89853008	3.9506128	7339.97458	0.85699217	3.65205082
70	8796.24778	0.90780271	4.50327189	8674.522342	0.90439363	5.33236634	8339.52615	0.89520036	5.16913824
80	8579.786218	0.88092129	5.39486525	8575.569183	0.79040063	5.53429395	8120.91973	0.76448992	5.89177732
90	8646.26203	0.94153323	5.0187617	8558.940553	0.88773952	6.20639096	7942.32084	0.85953255	5.780502
100	8595.880611	0.92576351	5.81094482	7335.905099	0.79180179	6.37318216	6926.91579	0.85718281	6.69915441
110	8777.150043	0.97276425	5.52580552	7812.382346	0.87809838	6.27712107	8100.22212	0.91742549	6.27623824
120	9041.196238	0.98590326	6.43220233	8474.935701	0.90740542	6.55678867	7281.67792	0.96295194	7.49239436
130	8790.67638	0.97	7.91017091	7693.470177	0.92276872	9.04699541	7180.47175	0.86739212	8.17655908
140	9085.769704	0.91364862	8.41734818	8476.572381	0.83588307	10.4274356	7733.2252	0.89680793	8.46948661
150	8922.167248	0.90576428	8.29761353	7602.067847	0.89416858	9.19110494	7781.45555	0.87176029	8.36961493

Figure 16: Results after comparison of the proposed with [41,42]

7. CONCLUSION

The trust table and trust management system provide a clear and unambiguous way to visualise the functioning of each node. To maintain the smooth operation of the network, the removal of faulty nodes can be determined based on their position within the network [6]. Optimal functioning of the nodes enhances the durability and energy efficiency of the network. Conviction management systems employ diverse algorithms. The problem's specifications can influence the algorithm's selection. The study article utilises SI to ascertain reputation and trust management. The Levenberg Marquardt algorithm is employed for training the network. When estimating the future scope, it is important to consider the following variables.:

i. Node-level load balancing is a viable alternative. This takes into consideration forecasting algorithms.

ii. The Long Short-Term Memory (LSTM) approach serves as the fundamental basis for deep neural networks. The prediction method relies on temporal forecasting

REFERENCES

[1] Ryu, J. H., Irfan, M., & Reyaz, A. (2015). A review on sensor network issues and robotics. Journal of Sensors, 2015.

[2] Carlos, L. R., Manuel, Z. R. V., del Rocio, O. L. V., & Gerardo, M. L. (2018). Wireless sensor networks applications for monitoring environmental variables using evolutionary algorithms. In Intelligent Data Sensing and Processing for Health and Well-Being Applications (pp. 257-281). Academic Press.

[3] (Karl, H., & Willig, A. (2007). Protocols and architectures for wireless sensor networks. John Wiley & Sons.

[4] Alkhatib, A. A. A., & Baicher, G. S. (2012). Wireless sensor network architecture. In 2012 International Conference on Computer Networks and Communication Systems (CNCS 2012).

[5] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. IEEE Communications magazine, 40(8), 102-114.

[6] Lopez, J., Roman, R., Agudo, I. and Fernandez-Gago, C., 2010. Trust management systems for wireless sensor networks: Best practices. Computer Communications, 33(9), pp.1086-1093.

[7] G. Han et al., Management and applications of trust in Wireless Sensor Networks:

[8] A survey, J. Comput. System Sci. (2013),

[9] http://dx.doi.org/10.1016/j.jcss.2013.06.014

[10] Ahmed, A., Bakar, K.A., Channa, M.I., Khan, A.W. and Haseeb, K., 2017. Energyaware and secure routing with trust for disaster response wireless sensor network. Peer-to-Peer Networking and Applications, 10(1), pp.216-237.

[11] Dhulipala, V.R. and Karthik, N., 2017. Trust management technique in wireless sensor networks: challenges and issues for reliable communication: a review. CSI Transactions on ICT, 5(3), pp.281-294.

[12] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H. and Kannan, A., 2019. An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wireless Personal Communications, 105(4), pp.1475-1490.

[13] Khan, T. and Singh, K., 2019. Resource management based secure trust model for WSN. Journal of Discrete Mathematical Sciences and Cryptography, 22(8), pp.1453-1462.

[14] T. Zahariadis, H. C. Leligou, P. Trakadas, and S. Voliotis, "Trust management in wireless sensor networks," European Transactions on Telecommunications, vol. 21, no. 4, pp. n/a–395, 2010.

[15] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust Management Systems for Wireless Sensor Networks: Best practices", Computer Communications, vol. 33, pp. 0140- 3664, 2010.

[16] G. Han et al., Management and applications of trust in Wireless Sensor Networks: A survey, J. Comput. System Sci. (2013), http://dx.doi.org/10.1016/j.jcss.2013.06.014

[17] Ahmed, A., Bakar, K.A., Channa, M.I., Khan, A.W. and Haseeb, K., 2017. Energy-aware and secure routing with trust for disaster response wireless sensor network. Peer-to-Peer Networking and Applications, 10(1), pp.216-237.

[18] Karthik, N. and Ananthanarayana, V.S., 2017, March. Data trust model for event detection in wireless sensor networks using data correlation techniques. In 2017 fourth international conference on signal processing, communication and networking (ICSCN) (pp. 1-5). IEEE.

[19] AlFarraj, O., AlZubi, A. and Tolba, A., 2018. Trust-based neighbor selection using activation function for secure

routing in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, pp.1-11.

[20] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Khannah Nehemiah, H. and Kannan, A., 2019. An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wireless Personal Communications, 105(4), pp.1475-1490.

[21] Nie, S. (2017). A novel trust model of dynamic optimization based on entropy method in wireless sensor networks. Cluster Computing, 1-10.

[22] R.W. Anwar, A. Zainal, F. Outay et al., BTEM: Belief based trust evaluvation mechanism for wireless sensor networks, Future Generation Computer Systems (2019), https://doi.org/10.1016/j.future.2019.02.004

[23] Tayyab Khan & Karan Singh (2019) Resource management based secure trust model for WSN, Journal of Discrete Mathematical Sciences and Cryptography, 22:8, 1453-1462, DOI: 10.1080/09720529.2019.1695897

[24] Amuthan, A. and Arulmurugan, A., 2021. Semi-Markov inspired hybrid trust prediction scheme for prolonging lifetime through reliable cluster head selection in

[25] WSNs. Journal of King Saud University-Computer and Information Sciences, 33(8), pp.936-946.

[26] Janakiraman, S., Priya, M.D., Devi, S.S., Sandhya, G., Nivedhitha, G. and Padmavathi, S., 2021. A Markov process-based opportunistic trust factor estimation mechanism for efficient cluster head selection and extending the lifetime of wireless sensor networks. EAI Endorsed Transactions on Energy Web, 8(35), pp.e5-e5.

[27] Fang, W., Zhang, W., Yang, W., Li, Z., Gao, W. and Yang, Y., 2021. Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. Digital Communications and Networks, 7(4), pp.470-478.

[28] Chen, Z., Tian, L. and Lin, C., 2017. Trust model of wireless sensor networks and its application in data fusion. Sensors, 17(4), p.703.

[29] Boukerche A, Li X, El-Khatib K (2007) Trust-based security for wireless ad hoc and sensor networks. Comput Commun 30:2413–2427.

[30] Yao Z, Kim D, Doh Y (2006) PLUS: parameterized and localized trust management scheme for sensor networks security. In: Proceedings of the third IEEE international conference on mobile adhoc and sensor systems (MASS'06), pp 437–446.

[31] Liu K, Abu-Ghazaleh N, Kang K-D (2007) Location Verification and Trust Management for Resilient Geographic Routing. J. Parallel and Distributed Computing 67(2):215–228.

[32] Hung K-S, Lui K-S, Kwok Y-K (2007) A trust-based geographical routing scheme in sensor networks. In: Proceedings of WCNC 2007

[33] Probst MJ, Kasera SK (2007) Statistical trust establishment in wireless sensor networks. In: International conference on parallel and distributed systems, vol 2

[34] Kim TK, Seo HS (2008) A trust model using fuzzy logic in wireless sensor network.

[35] World academy of science and engineering and Technology 42:63–66

[36] Momani M, Challa S, Alhmouz R (2008) BNWSN: bayesian network trust model for wireless sensor networks. In: Mosharaka international conference on communications, computers and applications (MIC-CCA '08), Amman, Jordan.

[37] Ganeriwal S, Srivastava MB (2004) Reputation-based framework for high integrity sensor networks. In: Proceedings ACM workshop security of ad hoc and sensor networks (SASN'04), pp 66–67.

[38] Song F, Zhao B (2008) Trust-based LEACH protocol for wireless sensor networks. In: Second international conference on future generation communication and networking, FGCN '08.

[39] Zhou M-Z, Zhang Y, Wang J, Zhao S-Y (2009) A reputation model based on behavior trust in wireless sensor networks. In: Eighth IEEE international conference on scalable computing and communications.

[40] Chen H (2009) Task-based trust management for wireless sensor networks. International Journal of Security and Its Applications 3(2):21–26.

[41] Gritzalis S, Aivaloglou E (2010) Hybrid trust and reputation management for sensor networks. Journal of Wireless Networks 16(5):1493–1510.

[42] Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song Y-J (2009) Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans Parallel Distrib Syst 20(11):1698–1712.

[43] Karthik N, Ananthanarayana VS (2016) Data trustworthiness in wireless sensor networks. Trustcom/BigDataSE/ISPA, 2016 IEEE. IEEE

[44] Dhulipala, V.R. and Karthik, N., 2017. Trust management technique in wireless sensor networks: challenges and issues for reliable communication: a review. CSI Transactions on ICT, 5(3), pp.281-294.

[45] S. Jothiprakasam, C. Muthial, A Method to Enhance Lifetime in Data Aggregation for Multi-hop Wireless Sensor Networks, International Journal of Electronics and Communications (2018), doi: https:// doi.org/10.1016/j.aeue.2018.01.004.

[46] Kaur, N., Aulakh, I.K., Tharewal, S., Keshta, I., Rahmani, A.W. and Ta, T.D., 2022. Enhanced Route Discovery Mechanism Using Improved CH Selection Using QLearning to Minimize Delay. Scientific Programming.

[47] Rani, S., 2022, February. Mitigating Security Problems in Fog Computing System. In Innovations in Bio-Inspired Computing and Applications: Proceedings of the 12th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2021) Held During December 16–18, 2021 (pp. 612-622). Cham: Springer International Publishing.

[48] Guleria, K., Verma, A. K., Goyal, N., Sharma, A. K., Benslimane, A., & Singh, A. (2021). An enhanced energy proficient clustering (EEPC) algorithm for relay selection in heterogeneous WSNs. Ad Hoc Networks, 116, 102473.

[49] Sharma, A., Goyal, N., & Guleria, K. (2021). Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes. The Journal of Supercomputing, 77(6), 6036-6055.