International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online) Volume 13, Issue 6, June 2024)

An Improved optimization method for energy reliable in Wireless Sensor network

MR ANSHU KUMAR TRIPATHI
ACADEMIC HEAD
SUNBEAM SUNCITY (SCHOOL & HOSTEL) VARANASI 221011

Abstract— **Modern manufacturing and technical developments have made it feasible to design sensor nodes that are powerful, small, economical, energy-efficient, and "smart" enough to be able to adapt, self-aware, and self-organize. Applications involving generalized communications are the focus of these nodes. Sensor networks for sustainable development examines how these technologies improve living standards and social development while having negligible to no negative impact on the environment or the planet's natural resources. In a wide range of applications, such as the military, healthcare, traffic monitoring, and remote image sensing, wireless sensor networks (WSNs) are unquestionably advantageous. Due to the limits of sensor networks, different levels of security are required for these crucial applications, making it challenging to employ traditional algorithms. Security has arisen as one of the main problems with IoT and smart city applications, and sensor networks are also considered of as the cornerstone of IoTs and smart cities. The WSN handles a number of complex issues, including a routing algorithm, network strength, packet loss, and energy loss. Energy usage, a productive technique for choosing cluster heads, and other complicated challenges are covered by the WSN. Given the distinct attributes and limitations of nodes, delivering dependable and credible data has become increasingly difficult with the latest advancements in WSN infrastructure.**

Keywords— **Trust, Dragonfly, K-means, Lifetime enhancement, Sustainability**

I. INTRODUCTION

The data needed by the network is sent via a wireless sensor network, which is a system of sensor nodes. WSN is utilized for the collection of secure data in a variety of applications, including weather forecasting, the military, underwater research, etc. [1][2][/3]. A transceiver, an external memory, a microcontroller, a power source, and one or more sensors make up a sensor node. The sensor node's battery cannot be replaced once it is deployed. As the energy level drops, so does the node's performance. An overview of the network lifetime resulting from increased energy, consumption[4–5]. Energy conservation is necessary to increase network efficiency and, as a result, increase the network's usable life. Enhancing longevity and energy efficiency can be achieved in a number of ways. The administration of trust in a strategy.

. One could assert that there is a reliable and strong connectivity between the two nodes [7][8]. Trustee, or the person in whom one can have confidence, and Trust, or the person in whom something is trusted, are the two fundamental elements of trust management. To determine if a node is reliable or not, each node in the network must be inspected, and each node must participate in this process. The main objective of a trust management system is to distinguish between trustworthy and trustworthy nodes int he network.

Only the reliable nodes remain in the network after the defective nodes are eliminated. This omission is justified by the probability that malfunctioning nodes will increase network latency, energy consumption, throughput, and longevity.

Delivering network services without any problems is possible if they are built on reliable data. Consequently, before executing additional processing on a data item and transmitting it across a network, a system needs to ascertain its reliability. The source is given a lower reliability rating and untrustworthy material is ignored. As soon as is reasonably possible, the reliability of the data must be evaluated in order to minimize potential harm. This will prevent doubtful information from being processed further. Every node inside the network is obligated to participate in the assessment of reliability and make decisions on credibility. [9]In [10]. From a Wireless Sensor Network (WSN) standpoint, trust is the choice to accept a message after verifying the accuracy of the data and the message's origin.

A trustee is always a notification delivered by one node to another, as the receiving node (the trustor) decides whether the message is valid and trustworthy at the moment of delivery. Every node employs a scale known as the "Trust Scale" in some capacity, and this is the core of the trust management paradigm. The first trust level, the cut-off level, and a complete trust level node that is 100% trustworthy are three typical values that can be taken into account in relation to this scale [11]. The "cut-off level" refers to the degree of confidence below which a node is thought to be untrustworthy. It is mandatory for every node to participate in the trust management procedure and keep accurate records of the reputations of other nodes. The Trust Table is produced as a result of this data structure. Every record in the trust database has a trust value assigned to it based on the trust scale.

II. LITERATURE SURVEY

power consumption, compact size, and light weight are considered in the construction of sensors. However, a major issue that persists is battery depletion, which results in a delay in data transmission and sensing. The expanding influence of WSN in real-world applications has spurred study into different approaches to ensure network stability and minimize energy consumption and end-to-end delay during data transfer. Throughout time, the idea of trust management has also been crucial. The current body of work provides illustrations of the many trust management models and strategies applied in the WSN industry.The concept of trust models was covered by the author. These models can be further divided into three types: "centralized," in which a node's trustworthiness based on data it has gathered on its own or from all other nodes in the network; "hierarchical," in which the network is divided into groups called clusters, and it is the cluster head's job to determine whether a node is trustworthy; and To put it briefly, this study describes the dangers associated with network lifespan and capacity, as well as network limitations, nodes' capabilities, and network restrictions. The goal is to build and apply a trust model that will improve security.

Numerous attacks on these trusted models are covered in addition to the success that WSN has attained with its trust model. These attacks reduce the efficacy of the trust paradigm. attacks like "selective behavior," "bad mouthing," "On-Off," "Sybil," and "newcomer," among others. A collection of best practices is provided along with an explanation of how the trust model for WSN was developed. First- and second-hand information collecting, initial values, granularity, updating and aging, risk and importance, and trust and reputation are among the best practises to be considered. A set of best practices should be taken into account in order to develop a successful trust model for WSN, according to research done on different trust management strategies[13].

The authors looked at the different trust models for clustered and traditional WSNs. Common WSNs can access two different types of trust models: Node trust models and Data trust models [14].The authors published the novel method, called ESRT. It is a brand-new routing system based on trust and energy that offers strong flexibility in the face of malfunctioning nodes and the behaviors they exhibit when forwarding packets.This approach takes uneven trust into account.The simulation demonstrates that ESRT works better than current methods like R-AODV and TLB-AODV when they are presented to varied numbers of problematic nodes and shifting network demand[15].

In [16].According to this study, AF-TNS can improve network security for WSNs with limited resources. The metric-based node evaluation and trust assessment using limited energy are the two stages in which the AF-TNS operates. This guarantees the maintenance of the neighbors' level of trustworthiness. Untrusted node is used by the Random Transition Function to streamline the difficult decision-making process in the AF and trustworthy node is used to guarantee network performance. Based on the simulation results, it can be concluded that AF-TNS extends the life of networks and raises the likelihood of identifying problematic behavior. In terms of network information delivery, the experimental results demonstrate that the AF-TNS technique ensures a minimum of 8.5 seconds of latency, 8.53J of energy, 149 kbps of throughput, and 390 seconds of network lifetime .Additionally, its 1.5% false detection rate is lower[17].

In this study, the novel secure routing algorithm EATSRA is introduced and applied to provide the bestandsafest routing available for WSNs. The decision tree-based routing technique is utilized in this method to choose the least secure option, and trust ratings are employed to more correctly identify attackers in WSNs. Additionally, decisions have been improved by the use of spatial-temporal constraints .It has been demonstrated through simulation-based testing that the recommended EATSRA works better by consuming less energy, improving security, and increasing packet delivery ratio[18].

An efficient BTEM strategy is presented in this study [20] to fend off internal attacks and weak nodes. To further reduce the number of dependable nodes from which to transfer data packets, data correlation is carried out after Bayesian estimation is employed to gather the direct and indirect trust ratings of each sensor node. In addition to the identification and subsequent isolation of problematic nodes, simulation data indicates an increase in the rate of false positive detection. Compared to other algorithms such as AF-TNS [17] and TrustDoc [19], it is more resilient to attacks.

III. Experimental Analysis

To figure out why increasing security and trust might lengthen the network's lifespan, a model can be proposed. The model explains the relationship that exists between the service provider and the customer. A route request requests the service provider for the optimal route that will enable the service user to get their data to their intended destination in a trustworthy manner. If a reliable route is available to transport the data at the designated time, the service provider will send an acknowledgement to the service user instead of failing to serve them. The service provider's location is where a lot of jobs are being done.

The binding of N number of nodes in a Node List into this structure is referred to as the "Service Layer Structure." It gets its name from the fact that all information exchanges take the shape of services, meeting demands that lead to effective communication. The gift Access requests for data are submitted by consumers, and provisioning blocks are part of the architecture of the nodes linked to each other via service orientation. In the suggested technique, each sensor node is deployed in a heterogeneous environment and has a range of sensing and buffer capacities.

They that hold the data that the user has requested are known as the source nodes. Utilizing the assessed QoS metrics, the node's reliability is assessed. As every node starts with a zero trust value and participates in several route forms, it is difficult to apply the trust value at the node level. As used in the suggested study, the swarm intelligence algorithm was developed using the evaluated algorithms from the SI list in the relevant work part. Because it provides resources that are easily accessible for wireless simulations, MATLAB has been used to simulate the entire project.

IV. Conclusion

We can clearly see how each node operates thanks to the trust table and trust management mechanism. According to their location within the network, the unreliable nodes can be eliminated, ensuring the seamless operation of the system [6]. A network's lifetime and energy efficiency are enhanced when its nodes operate correctly. Different types of algorithms are used by conviction management systems. An algorithm's selection may be influenced by the problem specifications. The study article's application of SI allows for the management of trust and reputation.

References

1. J. Yang, T. Qian, F. Zhang and S. U. Khan, "Real-Time Facial Expression Recognition Based on Edge Computing," in IEEE Access, vol. 9, pp. 76178-76190, 2021, doi: 10.1109/ACCESS.2021.3082641.
2. C. Zhang, M. Li and D. Wu, "Federated Multidomain Learning With Graph Ensemble Autoencoder GMM for Emotion Recognition," in IEEE Transactions on Intelligent Transportation Systems, 2022, doi: 10.1109/TITS.2022.3203800.
3. S. K. W. Hwooi, A. Othmani and A. Q. M. Sabri, "Deep Learning-Based Approach for Continuous Affect Prediction From Facial Expression Images in Valence-Arousal Space," in IEEE Access, vol. 10, pp. 96053-96065, 2022, doi: 10.1109/ACCESS.2022.3205018.
4. N. Galea and D. Seychell, "Facial Expression Recognition in the Wild: Dataset Configurations," 2022 IEEE 5th International Conference on Multimedia Information Processing and Retrieval (MIPR), 2022, pp. 216-219, doi: 10.1109/MIPR54900.2022.00045.
5. R. N. B. Priya, M. Hanmandlu and S. Vasikarla, "Emotion Recognition Using Deep Learning," 2021 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), 2021, pp. 1-5, doi: 10.1109/AIPR52630.2021.9762207.
6. T. R. Ganesh Babu, K. Shenbagadevi, V. S. Shoba, S. Shrinidhi, J. Sabitha and U. Saravanakumar, "Image Processing Methods for Face Recognition using Machine Learning Techniques," 2021 International Conference on Computational Performance Evaluation (ComPE), 2021, pp. 519-523, doi: 10.1109/ComPE53109.2021.9752410.
7. L. Li, H. Yan and M. Li, "Disentanglement Learning Generative Adversarial Network for Facial Expression Recognition," 2021 5th Asian Conference on Artificial Intelligence Technology (ACAIT), 2021, pp. 515-521, doi: 10.1109/ACAIT53529.2021.9731242.
8. T. Tiwari, V. Bharti, Srishti and S. K. Vishwakarma, "Facial Expression Recognition Using Keras in Machine Learning," 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2021, pp. 466-471, doi: 10.1109/ICAC3N53548.2021.9725756.
9. X. Fan, R. Qureshi, A. R. Shahid, J. Cao, L. Yang and H. Yan, "Hybrid Separable Convolutional Inception Residual Network for Human Facial Expression Recognition," 2020 International Conference on Machine Learning and Cybernetics (ICMLC), 2020, pp. 21-26, doi: 10.1109/ICMLC51923.2020.9469558.
10. K. V and C. H, "Performance Dependency of Facial Emotion Recognition System on Dropout and Learning Rate," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 71-81, doi: 10.1109/ICISS49785.2020.9316077.