Trust And Energy-Aware Routing Protocol for Wireless Sensor Networks Based on Secure Routing

Original Scientific Paper

Muneeswari G
School of Computer Science and Engineering,
VIT-AP University, Amaravati,
Andhra Pradesh, India
muneeswari.g@vitap.ac.in

Ahilan A
Department of Electronics and Communication Engineering, PSN College of Engineering and Technology, Tirunelveli, Tamil Nadu, India
listentoahil@gmail.com

Rajeshwari R
Department of Information technology,
Panimalar Engineering College,
Chennai, Tamil Nadu, India
rajeshwariit@gmail.com

Kannan K
Electronics and Communication Engineering,
R.M.K. College Of Engineering And Technology,
Puduvoyal,Chennai Tamil Nadu, India.
Kannan@rmkcet.ac.in

John Clement Singh C
Department of Electronics and Communication Engineering,
Kings Engineering College,
Sriperumbudur, Chennai, Tamil Nadu, India
Johnclement12@gmail.com

Abstract *– Wireless Sensor Network (WSN) is a network area that includes a large number of nodes and the ability of wireless transmission. WSNs are frequently employed for vital applications in which security and dependability are of utmost concern. The main objective of the proposed method is to design a WSN to maximize network longevity while minimizing power usage. In a WSN, trust management is employed to encourage node collaboration, which is crucial for achieving dependable transmission. In this research, a novel Trust and Energy Aware Routing Protocol (TEARP) in wireless sensors networks is proposed, which use blockchain technology to maintain the identity of the Sensor Nodes (SNs) and Aggregator Nodes (ANs). The proposed TEARP technique provides a thorough trust value for nodes based on their direct trust values and the filtering mechanisms generate the indirect trust values. Further, an enhanced threshold technique is employed to identify the most appropriate clustering heads based on dynamic changes in the extensive trust values and residual energy of the networks. Lastly, cluster heads should be routed in a secure manner using a Sand Cat Swarm Optimization Algorithm (SCSOA). The proposed method has been evaluated using specific parameters such as Network Lifetime, Residual Energy, Throughpu,t Packet Delivery Ratio, and Detection Accuracy respectively. The proposed TEARP method improves the network lifetime by 39.64%, 33.05%, and 27.16%, compared with Energy-efficient and Secure Routing (ESR), Multi-Objective nature-inspired algorithm based on Shuffled frog-leaping algorithm and Firefly Algorithm (MOSFA) , and Optimal Support Vector Machine (OSVM).*

Keywords*: Wireless Sensor Network, Routing, Sensor Nodes, Aggregator Nodes, sand cat swarm optimization algorithm*

1. INTRODUCTION

Wireless Sensor Network (WSN) consists of a few cooperative sensor nodes that are spread out geographically. As a result of technological advances in wireless networking techniques and the availability of inexpensive, intelligent, and small-sized sensors, ubiquitous computing has been made possible [1]. The goal of a WSN implementation is to gather data about objects found in the monitoring area, transform that data into electrical signals, and transmit those signals to the base station through wireless multi-channel communication [2]. The sensor nodes join together to create a network in order to gather information from their immediate surroundings and then communicate with one another to carry out specific tasks [3]. During Mobility Wireless Sensor Networks (MWSN), sensors are mobile and can link to a variety of providers, such as robotic systems and intelligent modes of transportation, to detect and collect data that can then be transmitted to the BS via direct or multi-

hop communication models [4]. Unstructured WSNs consist of ad-hoc deployments of dense sensor nodes. The network is called a structured WSN, depending on the other extreme, when all nodes are placed simultaneously [5]. In Sensor nodes' the computing capacity, power, and the battery life are all constrained in WSN. The topology of the network changes when certain network nodes lose power. The network may even become paralyzed and cease to operate correctly if there are too many dead nodes. Due to the inability to detect malicious sites, attacks and energy usage are two issues wireless sensor networks face. They use a particular routing method, they use effort effectively, they choose cluster heads, and the technology they use to create a wireless sensor network are all important considerations.

WSN is one of the most contemporary communication-related technologies. Due to its open architecture and limited resource availability, WSN is challenging to secure and utilize energy effectively. Routing and clustering are just two of the many technologies that have been introduced to secure WSNs. Many reasons, including shortened sensor node usage time, increased power consumption due to larger number of hops, distribution fewer packet distribution, and decreased throughput, may result in improper data transmission from one node to another. This research proposes a novel Trust and Energy Aware Routing Protocol (TEARP) technique, which enhances the security of routes using wireless sensor networks. The major contributions of the proposed TEARP techniques are given as follows.

- Initialization, registration, and authentication are accomplished during the authentication of ANs and SNs on public and private blockchains, respectively.
- The proposed technique provides a thorough trust value for nodes based on their direct trust values while taking volatility and adaptable penalty elements into concern. Filtering mechanisms also generate indirect trust values.
- Further, an enhanced threshold technique is employed to identify the most appropriate clustering heads based on dynamic changes in the extensive trust values and residual energy of the networks.
- Lastly, cluster heads should be routed in a secure manner is determined using a sand cat swarm optimization algorithm.

The remainder of the research is organized as follows. In Section II, a summary of the literature is provided. In Section III, the proposed TEARP methodology is thoroughly explained. The experimental findings are presented in Section IV, and conclusions and future scope is presented in Section V.

1.1. BACKGROUND STUDY

An improved Artificial Bee Colony (iABC) metaheuristic is presented in [6] to maintain a solid balance between mining and exploration abilities while using the least amount of RAM possible. The suggested metadata's abilities to produce ideal cluster heads and increase WSN energy efficiency are inherited by an energy-efficient bee clustering algorithm based on iABC information.

An improved version of the firefly algorithm is presented in [7] which is applied to improve the network lifetimeWhen LEACH, the basic Firefly set of rules, and particle swarm optimization are applied to the same community infrastructure model, the performance of the improved Firefly set of rules is compared to them. In terms of performance and stability, the enhanced Firefly approach is superior than existing algorithms.

A Whale Moth Flame Optimization (WMFO) and Improved African Buffalo Optimization (IABO) is presented in [8] which is applied for effective clustering and routing. The WMFO method can be utilized for effective clustering by employing a fitness function connected to the distance within the cluster, the distance between clusters, the energy, and the equilibrium coefficient. The WMFO algorithm creates a tuning function that contains certain factors like residual energy and distance coefficient in order to choose the best routes in the WSN.

A Particle Distance Updated Sea Lion Optimization (PDU-SLnO) is presented in [9] which is developed to consume less energy consumption and increases the network lifetime. For the WSN, a new hierarchical routing energy-sensitive CH selection architecture is provided using the hybrid optimization technique. When selecting a CH, capacity, distance, latency, and quality of service (QoS) are taken into account. To choose the optimal CH, the Sea Lion Optimization (SLnO) and Particle Swarm Optimization (PSO) algorithm principles are integrated in the new matching method known as the PDU-SLnO algorithm.

2. LITERATURE SURVEY:

The WSN performance, including energy use, network lifetime, etc., has been the subject of many researches. One of the most important characteristics of WSNs is secure routing. Among those, some of the techniques have been reviewed in this section.

In 2019, Haseeb K., et al [10] presenting an energy-efficient and secure routing (ESR) protocol for intrusion defence in IoT based on wireless sensor networks. The proposed solution utilized greedy algorithms to construct routing paths and overlooked intrusions in an infrastructure-less and unattended environment. As a result, there are a great No. of route discovery and re-transmissions, especially when there are attacker networks present and there is a great deal of internet traffic.

In 2020, Barzin et al. [11] Presented a Multi-objective nature-inspired algorithm (MOSFA) is developed from fireflies and shuffling frog-leaping algorithms and is a successful protocol for WSNs. Using this technique, both fireflies and shuffled frog-leaping algorithms are utilized simultaneously. SIF, ERA, FSFLA, and LEACH

have common lifespan development of 68%, 82%, 30%, and 28%, respectively, according to simulation data.

In 2021, Amaran S., et al [12] presented a novel optimal Support Vector Machine (OSVM) based IDS in WSN. The suggested technique's OSVM model has an accuracy of more than 94.09% and a detection rate of 95.02%.In 2021, Reddy D.L. et al [13] Presented a hybrid Ant Colony Optimization (ACO) approach that integrates Glow Worm Swarm Optimization. According to experimental results, the suggested solution keeps more nodes alive and uses less network energy than standard techniques.

From the aforementioned analyses, it's clear that those solutions have several hazards, including the nodes' consumption of electricity and steady routing when transferring data packets to their destinations.To overcome these drawbacks, novel Trust and Energy Aware Routing Protocol (TEARP) techniques are recommended.

3. PROPOSED METHOD

In this paper, a Trust and Energy Aware Routing Protocol (TEARP) in WSN is proposed, which use blockchain technology to maintain the identity of the Sensor Nodes (SNs)and Aggregator Nodes (ANs). Initialization, registration, and authentication are accomplished during the authentication of ANs and SNs on public and private blockchains, respectively. Fig. 1 illustrates the overall structure of the proposed method.

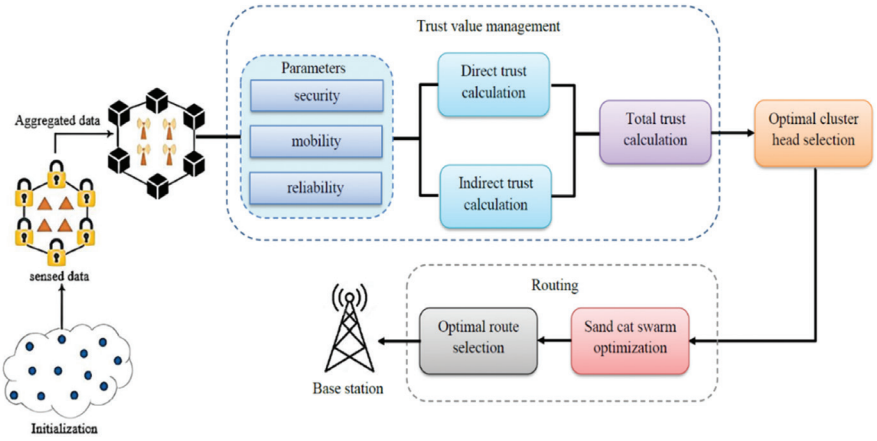


Fig. 1. Overall block diagram for the proposed TEA method

3.1. BLOCKCHAIN TECHNOLOGY

In the proposed blockchain-based routing and reliability evaluation method, BSs transmit encrypted data about routing and trust values to other network nodes. All node-to-node transactions are also verified by the blockchain's. The AN authenticates and authorizes the SN each time they communicate, allowing the SN to send packets to the AN. Additionally, these BSs authenticate the ANs before allowing them to communicate with other ANs or BSs. The blockchain is updated with transactions when the node's identification has been verified. The blockchain cannot be used to delete the transaction data. The transparency and traceability of the blockchain enable the proposed methodology to identify rogue nodes. In this approach, the blockchain offers secure routing and a productive technique for evaluating trust to find malicious nodes.

For SN and AN authentication, blockchains can be either private or public. In this architecture, two different kinds of blockchains are utilized to lessen the stress placed on the NAs. ANs died in the initial rounds of the prior authentication process because they had to register and validate other ANs. However, in our suggested model, the BS, which has powerful computational capabilities, registers and authenticates the AN. The NAs' workload is lightened in this way. Therefore, the coexistence of the two blockchains helps to lower the computational expense of the proposed paradigm. Because the AN is directly connected to the public blockchain, and the identification of every node is uploaded to the blockchain.

3.2. TRUST CALCULATION

Trust value has been calculated for two parameters, such as Direct Trust and Indirect Trust, which are described as follows. The TEARP version contains three inputs, namely security, portability, and dependability, to determine the cost of trust.

3.2.1. Indirect Direct Trust (IDT)

DT displays a node that contains the opinion variable. To use the IDT, which is defined below, a node must have a witness variable, which is not possible without one.

$$\mathbf{MFX}_{\mathbf{m}}^{\mathbf{f}}(\boldsymbol{\tau}) = \frac{1}{\mathbf{s}}\sum_{\mathbf{m}=1}^{\mathbf{s}} \mathbf{FX}_{\mathbf{m}}^{\mathbf{f}}(\mathbf{f}) \quad (1)$$

For the purpose of preventing attacks and enhancing the security of the trust mechanism, formula 5 is used to calculate fraud ratings.

$$d_k^t = \sqrt{\frac{\sum_{B_x \in B}\left(\bar{D} - D_{kB_x}^t\right)^2}{l}} \quad (2)$$

3.2.2. Direct Trust (DT)

A link between the m^{th} source node and the f^{th} endpoint node takes an estimated time to form, which is called the direct trust (DT). Therefore, Direct trust involving the use of the m^{th} source node and f^{th} endpoint has been described as,

$$FX_m^f(\tau) = \frac{1}{3}\left[FX_m^f(\tau-1) - \left(\frac{\tau_{appx}-\tau_{appx}}{\tau_{appx}}\right) + \omega\right] \quad (3)$$

Where τ_{appx} defines the anticipated duration, and τ_{est} specifies the estimated duration. This indicates that it takes time to τ_{appx} acquire and τ_{est} transfer the public key between the destination and the node. ω denotes the nodes' opinion variable.

$$R_f = \frac{\gamma * re_f - rf_f}{me_f} \quad (4)$$

$$S_f = \frac{\gamma * se_f - us_f}{me_f} \quad (5)$$

where re_f and se_f represent number of packets f has transmitted and received, respectively. The amount of information that f has discarded to be received and delivered, respectively, is represented by rf_f and us_f. The total number of packets that node f has received and transmitted is shown in the message. The adaptive penalty coefficient is written as γ.

3.3. CLUSTERING AND OPTIMAL CLUSTER HEAD SELECTION

The SCSO approach maximizes the network's lifespan. If damaged nodes are unable to send data due to damage, collaborate with nearby nodes to replace them. By swapping out the node, the SCSO version of the Cluster Head presented in this study performs better than the prior SCSO. The challenge of keeping them in a small space led to the development of the Sand Cat Swarm Optimization (SCSO) approach. Equation 10 offers an algebraic representation of SCSO.

$$T_m^n = \begin{cases} ET_m + p_1[(VC_m - NC_m)p_2 + NC_m]p_3 \geq 0 \\ ET_m - p_1[(VC_m - NC_m)p_2 + VC_m]p_3 < 0 \end{cases} \quad (6)$$

Where, $T_m{}^n$ is the First cluster head position in m^{th} dimension, ET_m is Food Source's position in m^{th} dimension, VC_{mis} upper bound in m^{th} dimension NC_m is lower bound in m^{th} dimension and p_1, p_2 is random numbers based on the interval [0,1]. The significant coefficient r_1, which is employed in Equation 11 to balance the processes of food acquisition and consumption, is the most crucial factor.

$$p_1 = 2f^{-\left(\frac{4x}{M}\right)^2} \quad (7)$$

The number L denotes the recent round, and M is the extreme number of rounds, where p_1 is a significant coefficient of SCSO.

3.4. ROUTING USING SAND CAT SWARM OPTIMIZATION

The performance of sand cats in nature served as the basis for a metaheuristic algorithm known as sand cat swarm optimization (SCSO). Sand cats, as opposed to domestic cats, survive in stony and sandy deserts. Sand cats have a 2 KHz hearing threshold. They resemble domestic cats and other cat species in regards to appearance. Sand cats only have fur on their hands and soles because of the intense conditions they endure. This protects them from heat and cold at home. This trait makes it challenging to follow a cat's trace. A sand cat's unique physical characteristic is their ability to hear low-frequency disturbancesThe Sand cat swarm optimisation algorithm (SCSO) replicates this characteristic to provide a close to optimal result, enabling them to immediately and accurately determine their targets.

3.4.1. Objective function for Routing

The cluster-based WSN will be able to maximize network lifetime by selecting the optimum path. To achieve this, a four-factor adaptive function is created, accounting for the nodes' remaining energy, their size, their location within the cluster, and their coverage rate. These parameters' definitions and derivatives are as follows:

Node Degree (N_D): It is the quantity of non-CH members that belong to each CH. Thus, it is recommended for CH to have the lowest node degree.

$$N_D = \sum_{x=1}^{p} |C_{m^x}| \quad (8)$$

Here, $|C_{m^x}|$ is the x^{th} cluster head's number of cluster members.

Residual Energy(R_E): It represents the node's present energy level. It is calculated as the difference between the total amount of energy utilised over a period of time and the initial energy level.

$$R_E = \sum_{x=1}^{p} \frac{1}{CH_x} \quad (9)$$

where CH_x is the x^{th} cluster head's remaining energy.

Distance to neighbour (D_N): It specifies the distance between its own CH and its neighbour. The distance between a normal sensor and CH is given by equation (14).

$$D_N = \sum_{x=1}^{p} \left(\sum_{x=1}^{L_y} dis(n_x, CH_y)/L_y\right) \quad (10)$$

Node Centrality (N_C): It is described as the distance between a node's centre location and its neighbours, and it is written in equation (11).

$$N_C = \sum_{x=1}^{p} \frac{\sqrt{(\sum_{y \in n} dis^2(x,y))/n(x)}}{Network\ dimension} \quad (11)$$

where $n(x)$ is the number of nodes that are neighbours to CH_y.

The weighted values are ϑ_1, ϑ_2, ϑ_3,and ϑ_4. The equation (12) displays the single objective function.

$$Fitness = \vartheta_1 N_D + \vartheta_2 R_E + \vartheta_3 D_N + \vartheta_4 N_C, where \sum_{x=1}^{4} v_x = 1, v_x \in (0,1) \quad (12)$$

A metaheuristic algorithm leads the method to satisfy the problem objective, such as minimization or maximization. Every strategy's fitness (cost) for the search

agent determines the subsequent repetition, and so on until optimal outcomes are obtainedThe most effective outcome is typically determined by the hunting mechanism. SCSO search agents look for targets after initiation to identify the most efficient approach. The Sand Cat's capacity to make low-frequency sounds is used to achieve this goal. Every search agent has a predefined sensitive range starting at 2 kHz. In SCSOA, the population size is 500, number of iteration is 1000 and the number of independent runs is 10.

Equation 13 shows the SCSO algorithm $\vec{P}_N$ variable drops gradually from 2 to 0. In this case, the T_D parameter was supposed to be 2. Iteration count is iterc, while iteration maximum is itermax. The sand cat's behaviour becomes sophisticated after half of the repetitions and is swift in the first iteration. Similar to this, the SCSO balances exploration and exploitation processes using T_D variables.

$$\overrightarrow{p_N} = T_D - \left(\frac{T_D \times iter_m}{iter_{Max}}\right) \quad (13)$$

$$\vec{P} = 2 \times \overrightarrow{p_N} \times rand(0,1) - \overrightarrow{p_N} \quad (14)$$

According to Equation 14, phase transformations are balanced. Equation 15 also prevents trapping in the local optimum. A $\vec{p}$ parameter controls evolutionary algorithms' efficiency. SCSO updates each agent's location.

$$\vec{p} = \overrightarrow{p_N} \times rand(0,1) \quad (15)$$

Equation 16 guarantees that the most suitable location of applicants for a search agent ($\overrightarrow{Pos_{im}}$) is updated after each algorithm iteration. Along with the agent's current location ($\overrightarrow{Pos_{im}}$) and sensitivity area ($\vec{p}$), this information is obtained. The SCSO continues with the subsequent step of its procedure, which is the exploiting of the target discovered after looking for it (exploration).

$$\overrightarrow{pos}(s+1) = \vec{p}.\left(\overrightarrow{Pos_{im}}(s) - rand(0,1).\overrightarrow{Pos_m}(s)\right) \quad (16)$$

$$\overrightarrow{pos_{puv}} = \left|rand(0,1).\overrightarrow{Pos_i}(s) - \overrightarrow{Pos_m}(s)\right| \quad (17)$$

$$\overrightarrow{Pos}(s+1) = \overrightarrow{Pos_i}(s) - \vec{p}.\overrightarrow{Pos_{puv}}.\cos(\theta) \quad (18)$$

The direction between the optimum ideal position and the present position of each search agent is determined by Equation 19. The most optimal (balanced) results locations in Equation 22, the ($\overrightarrow{Pos_i}$) and ($\overrightarrow{Pos_{rnd}}$) are as well as the randomly selected locations, appropriately.

$$Y(s+1) = \begin{cases} \overrightarrow{Pos_i} - \vec{p}.\overrightarrow{Pos_{puv}}.\cos(\theta) & |P| \leq; exploitation \\ \vec{p}.\left(\overrightarrow{Pos_{im}}(s) - rand(0,1).\overrightarrow{Pos_m}(s)\right) & |P| >; exploration \end{cases} \quad (19)$$

Pseudocode of SCSOA

Initializing Population

Compute the fitness function dependent upon the main function

Initializing the r, r_G, R

While($t \leq t_{Max}$)

For all the SCs

Obtain an arbitrary angleθ ($0 \leq \theta \leq 360°$)

If($|R| \leq 1$)

Upgrade the searching agent dependent upon the exploitation phase of equation (23); $\overrightarrow{Pos_i}$ - $\vec{p}.\overrightarrow{Pos_{puv}}$ .cos(θ)

Else

Upgrade the searching agent dependent upon the exploration phase of equation (23); $\vec{p}.(\overrightarrow{Pos_{im}}(s)$-$rand(0,1).(\overrightarrow{Pos_m})(s))$

End

End

$t = t+1$

End

4. RESULT

This segment presents the experimental analysis of the suggested approach to Trust and Energy Aware Routing Protocol (TEARP) techniques.

Table 1. Stimulation parameters

Parameters	Units
Frequency	30khz
Queue size	50 packets
Simulation time	50 s
Number of nodes	500 nodes
Packets size	500 bytes
Data rate	2 Mbps
Length of data packet	500 bytes

4.1. COMPARISON ANALYSIS

A comparison is conducted between the proposed Trust and Energy Aware Routing Protocol (TEARP) technique and existing methods ESR [13], MOSFA [16], and OSVM [18] in terms of the No. of nodes, the Packet Delivery Ratio, the Residual Energy, and the Throughput the Network Lifetime.

In Fig. 2, the proposed method strategy shows the Network lifetime. TEARP outperforms other techniques with a lower fraction of nodes, almost doubling the network lifetime in the process.The proposed method achieves a better network lifetime of 61.40 %, 39.64 %, and 52.24 %, than ESR, MOSFA, and OSVM.

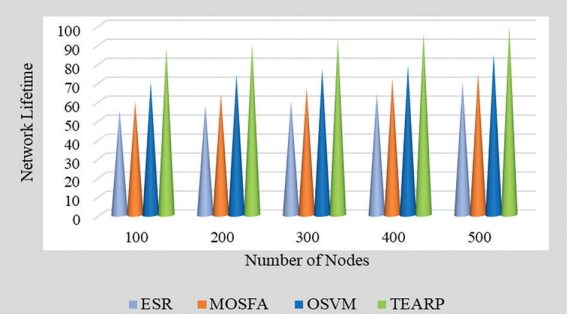


Fig. 2. Comparison of Network Lifetime

Fig. 3 presents the equivalence of the packet delivery ratio of the suggested technique in comparison with existing techniques. TEARP performs better than other existing techniques and the ratio appears to be large. The proposed method achieves a better Packet Delivery Ratio of 45.54 %, 27.16 %, and 38.48 % than ESR, MOSFA, and OSVM.

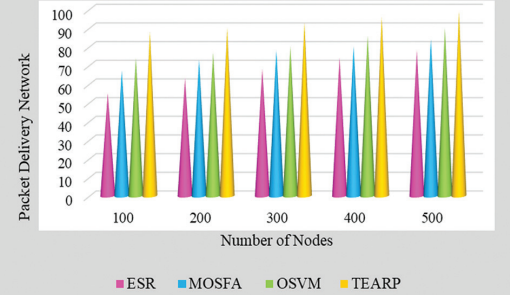
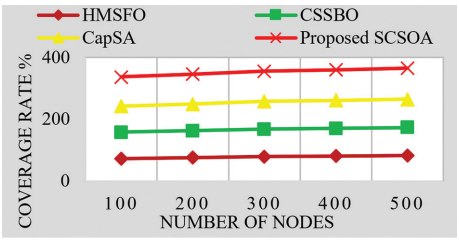
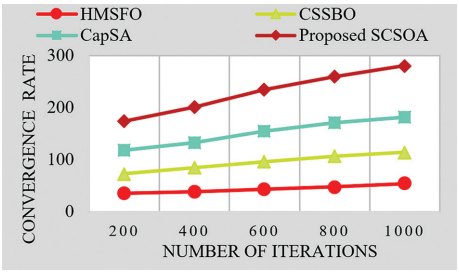


Fig. 3. Comparison of Packet Delivery Network

Fig. 4(a) and (b) examine the four algorithms' rates of coverage, and rates of convergence. The link between coverage and population size when using the SCOA, HMSFO, CSSBO, and CapSA algorithms is depicted in Figure 4(a). Four algorithms will enhance network coverage as the population grows. The HMSFO, CSSBO, and CapSA algorithms cannot compete with the proposed SCSO algorithm. The relationship between convergence rate and iterations for the SCSOA, HMSFO, CSSBO, and CapSA algorithms is depicted in Figure 4(b).



(a)



(b)

Fig. 4. Performance comparison of different algorithms

The SCSO algorithm peaks and converges quickly in terms of growth scope at the number of iterations, whereas the other three algorithms continue to increase quickly after that point. As a result, the SCSO algorithm's convergence speed and time to optimal value are both faster. The SCSO algorithm exhibits a better simulation effect in the algorithm's convergence area. In conclusion, the SCSO method outperforms the other three algorithms in terms of convergence speed and coverage ratio.

Fig. 5 displays a comparison of latency with various options. Due to how long it takes to choose the starting path, current solutions cannot reduce latency. Additionally, a safe and effective path is selected for data transfer. As a result, the delay time will be reduced by the proposed TEA RP approach.

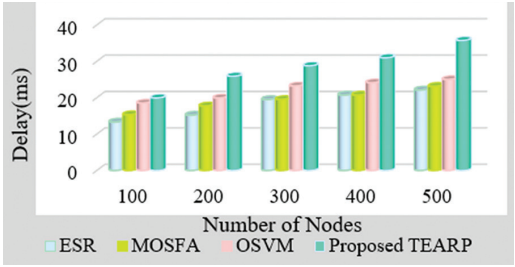


Fig. 5. Comparison of Residual Energy

The proposed technique's throughput equivalent in relation to existing techniques is depicted in Fig. 6. The proposed technique achieves higher throughput than other existing techniques. ESR, MOSFA, and OSVM, and the proposed Trust and Energy Aware Routing Protocol (TEARP) are achieving better than throughput is 50.15 %, 32.45 %, and 29.64 %.

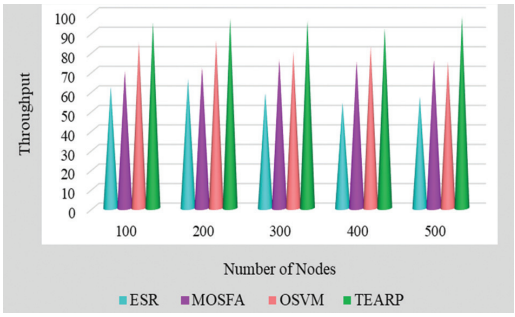


Fig. 6. Comparison of Throughput

4.3. DETECTION ACCURACY

The detection accuracy indicator shows the proportion of correct detections made by the suggested technique with the minimum possible false reports. TEARP detection accuracy is 28.35% and 67.43%, respectively. Detection Accuracy is shown in Fig. 7.

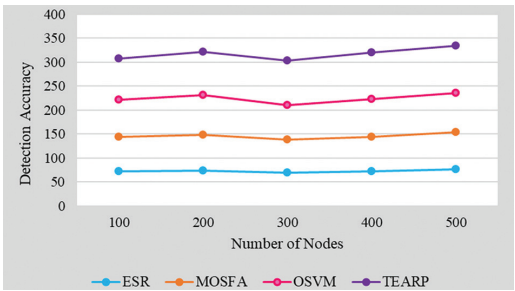


Fig. 7. Detection Accuracy

5. CONCLUSIONS

In this paper, a Trust and Energy Aware Routing Protocol (TEARP) in WSNs is proposed, which use blockchain technology to maintain the identity of the SNs and ANs. The proposed TEARP has been simulated using MATLAB. The simulation outcomes demonstrate that the proposed TEARP framework outperforms more established methods like ESR, MOSFA, and OSVM.The proposed TEARP method improves the network lifetime by 39.64%, 33.05%, 29.64% and 27.16%, respectively, and has better detection accuracy of 28, 35% and 67.43%. compared with ESR, MOSFA and OSVM techniques. The TEARP method is not applicable in large-scale situations. The TEARP technique must be used in a large-scale context in future to overcome such constraints.Additionally the proposed TEARP approach might include algorithmic tests with an extensive network that employs agent-based communication for trust modeling.

Acknowledgment

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

6. REFERENCES:

[1] M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, R. Patan, "Ant colony optimization-based quality of service aware energy balancing secure routing algorithm for wireless sensor networks", IEEE Transactions on Engineering Management, Vol. 68, No. 1, pp. 170-182.

[2] Z. Wang, H. Ding, B. Li, L. Bao, Z. Yang, Q. Liu, "Energy efficient cluster-based routing protocol for WSN using firefly algorithm and ant colony optimization", Wireless Personal Communications, Vol. 125, No. 3, 2022, pp. 2167-2200.

[3] K. Haseeb, N. Islam, A. Almogren, I. U. Din, "Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things", IEEE Access, Vol. 7, 2019, pp. 185496-185505.

[4] Y. Xiong, G. Chen, M. Lu, X. Wan, M. Wu, J. She, "A two-phase lifetime-enhancing method for hybrid energy-harvesting wireless sensor network", IEEE Sensors Journal, Vol. 20, No. 4, 2019, pp. 1934-1946.

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

[6] P. S. Mann, S. Singh, "Improved artificial bee colony metaheuristic for energy-efficient clustering in wireless sensor networks", Artificial Intelligence Review, Vol. 51, 2019, pp. 329-354.

[7] M. Zivkovic, N. Bacanin, E. Tuba, I. Strumberger, T. Bezdan, M. Tuba, "Wireless Sensor Networks Life Time Optimization Based on the Improved Firefly Algorithm", Proceedings of the International Wireless Communications and Mobile Computing, Limassol, Cyprus, 15-19 June 2020, pp. 1176-1181.

[8] S. K. Barnwal, A. Prakash, D. K. Yadav, "Improved African Buffalo Optimization-Based Energy Efficient Clustering Wireless Sensor Networks using Metaheuristic Routing Technique", Wireless Personal Communications, Vol. 130, No. 3, 2023, pp. 1575-1596.

[9] R. K. Yadav, R. P. Mahapatra, "Hybrid metaheuristic algorithm for optimal cluster head selection in wireless sensor network", Pervasive and Mobile Computing, Vol. 79, 2022, p. 101504.

[10] S. Banerjee, R. B. Karennavar, P. Sirigeri, R. Jayashree, "Multimedia Text Summary Generator for Visually Impaired", Proceedings of the 6th International Conference on Communication and Electronics Systems, Coimbatre, India, 8-10 July 2021, pp. 1166-1173.

[11] K. Haseeb, A. Almogren, N. Islam, I. Ud Din, Z. Jan, "An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN", Energies, Vol. 12, No. 21, 2019, p. 4174.

[12] A. Barzin, A. Sadegheih, H. K. Zare, M. Honarvar, "A hybrid swarm intelligence algorithm for clustering-based routing in wireless sensor networks", Journal of Circuits, Systems and Computers, Vol. 29, No. 10, 2020, p. 2050163.

[13] S. Amaran, R. M. Mohan, "Intrusion detection system using optimal support vector machine for wireless sensor networks", Proceedings of the International Conference on Artificial Intelligence and Smart Systems, Coimbatore, India, 25-27 March 2021, pp. 1100-1104.

[14] D. L. Reddy, C. Puttamadappa, H. N. Suresh, "Merged glowworm swarm with ant colony optimization for energy efficient clustering and routing in wireless sensor network", Pervasive and Mobile Computing, Vol. 71, 2021, p. 101338.

[15] G. Manoharan, A. Sumathi, "Efficient routing and performance amelioration using Hybrid Diffusion Clustering Scheme in heterogeneous wireless sensor network", International Journal of Communication Systems, Vol. 35. No. 15, 2022, p. e5281.

[16] M. Rizwanullah, H. K. Alsolai, M. Nour, A. S. A. Aziz, M. I. Eldesouki, A. A. Abdelmageed, "Hybrid Muddy Soil Fish Optimization-Based Energy Aware Routing in IoT-Assisted Wireless Sensor Networks", Sustainability, Vol. 15, No. 10, 2023, p. 8273.

[17] A. Sharma, H. Babbar, S. Rani, D. K. Sah, S. Sehar, G. Gianini, "MHSEER: A Meta-Heuristic Secure and Energy-Efficient Routing Protocol for Wireless Sensor Network-Based Industrial IoT", Energies, Vol. 16, No. 10, 2023, p. 4198.

[18] J. Paruvathavardhini, B. Sargunam, "Stochastic Bat Optimization Model for Secured WSN with Energy-Aware Quantized Indexive Clustering", Journal of Sensors, Vol. 2023, 2023.