Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 47 No. 03
March 2026

Trust-Assisted Blockchain and Machine Learning-Enhanced Energy-Aware Secure Routing for Hierarchical WSNs

Sruthi S[1*], Dr. M. Hemalatha[2]

[1*]Research Scholar, Hindusthan College of Arts & Science, Coimbatore, Tamilnadu, India.

[2]Professor,Department of Information Technology,Hindusthan College of Arts & Science, Coimbatore, Tamilnadu, India

Abstract: As Wireless Sensor Networks (WSNs) advance towards mission-critical applications, routing frameworks must be safe, flexible, and energy-efficient (EE).Conventional clustering-based protocols (CBP) such as LEACH lack resilience against dynamic security threats and offer limited scalability in hostile environments. This paper introduces a novel framework titled Trust-Assisted Blockchain and Fuzzy SVM-Enhanced Energy-Aware Secure Routing (T-BMESR) for hierarchical WSNs. The proposed method combines adaptive trust modelling (ATM), lightweight blockchain (BC) consensus using Proof-of-Authority (PoA) and Directed Acyclic Graph (DAG), and an intelligent anomaly detection mechanism based on Fuzzy based Support Vector Machine (FBSVM). FSVM enhances classification by assigning fuzzy membership values to sensor nodes (SN), improving decision confidence in detecting malicious behavior. Trust values (TV) are dynamically updated using a fusion of direct interactions, indirect recommendations, and FBSVM-based anomaly scores. BC ensures low-overhead validation of data and node identities, securing the routing path. Simulation-based evaluations demonstrate that T-BMESR significantly outperforms baseline protocols in terms of EE, detection accuracy, throughput (T), and trust precision. The integration of FSVM and BC enables robust, scalable, and trustworthy communication across energy-constrained WSN environments.

Keywords: Wireless Sensor Networks (WSNs), Secure Routing, Energy Efficiency, Trust Management, Fuzzy Support Vector Machine (FSVM), Blockchain, Proof-of-Authority (PoA), Directed Acyclic Graph (DAG), Intrusion Detection System (IDS), Cluster Head (CH) Selection

I.INTRODUCTION

Applications ranging from industrial automation and military surveillance to environmental monitoring and healthcare now depend heavily on WSNs. To collect and transmit data to a central base station (BS), these networks are composed of spatially distributed, energy-constrained SN. Ensuring secure, EE, and reliable data transmission has grown more difficult as WSNs get bigger and more complicated.

Multitudinous SN with low-cost, low-power, and small-scale features make up WSN [1]–[3]. Gathering pertinent data in the target region and sending it either single-hop (SH) or multi-hop (MH) to the sink node (BS or control centre) are the roles of these datacentric nodes [4], [5]. Aerospace, industry, homes, the battlefield, and many more areas have used WSN in recent years [6]–[8]. SN are typically placed in unsupervised or hostile surroundings. Their routing protocols (RP) become vulnerable to many types of assaults as a result [9]. Both internal and external attacks fall under this category [10], [36].

Security mechanism (SM) based on identity verification and cryptography are suggested to fend off external attacks on WSNs and allow them to function in a safe and healthy environment. Nevertheless, these defence systems are unable to fend off attacks within the system [11], [12]. This is due to the fact that nodes in a network must be cooperative and completely dependable for these strategies to be realised [13]. They can also have a greater energy overhead because they need a lot of memory and complex computations. Consequently, it has been demonstrated that trust-based SM (TBSM) are viable for addressing internal assaults on WSNs [14], [15]. Based on the node's past behaviour, TBSM forecast its behaviour in the future [16], [17].By creating models, they are able to quantify node behaviour. TV and security will increase with the number of positive behaviours exhibited by a node. The inability to fight against many attack types at once, the slowness of maliciousness detection, and the high (EC) energy consumption are some of the

disadvantages of traditional TBSM. More significantly, trust attacks also known as bad-mouth and on-off attacks are intended to target TBSM, and there is a spear and a shield. Its goal is to stop these defence mechanisms by destroying the trust evaluation mechanism (TEM).As a result, malicious nodes (MN) will also be assessed as normal nodes. Consequently, one of the key topics that many academics investigate is how to defend against both common and trust assaults, as well as how to choose a safe and EE path for the network.

Traditional hierarchical RP like LEACH focus on prolonging network lifetime (NL) by minimizing EC through randomized cluster head (CH) rotation and localized (DA) data aggregation. However, these methods are susceptible to attacks like sinkhole, Sybil, and selective forwarding attacks (SFA) since they lack the tools to evaluate the reliability of nodes. Moreover, their static nature fails to respond dynamically to changing node behavior or evolving security threats.

To resolve these limitations, recent studies have analyzed the incorporation of trust-based models and blockchain technology into WSN routing protocols. Trust management systems enable more secure CH selection and routing decisions based on node behavior. Simultaneously, blockchain provides decentralized authentication and tamper-proof data logging, enhancing overall security. Because of their significant computational and energy overhead, The Proof-of-Work (PoW) or Proof-of-Stake (PoS) are the conventional BC methods, and it is not feasible for WSNs.

Furthermore, Low adaptability and delayed threat responses are caused by traditional intrusion detection systems (IDS), which frequently function independently of RP. A viable way to get around this is by using machine learning (ML)-based anomaly detection to identify MN in real time.In this context, FSVM offer superior classification by assigning fuzzy membership (FM) values to data samples, thus accounting for uncertainty and noise in node behavior.

This paper presents T-BMESR—a Trust-Assisted Blockchain and Fuzzy SVM-Enhanced (EASR)Energy-Aware (EA) Secure Routing framework for hierarchical WSNs. The key contributions of this work are:

- An adaptive trust computation model that integrates direct and indirect observations with anomaly detection feedback from FBSVM.
- A lightweight blockchain structure based on Proof-of-Authority (PoA) and Directed Acyclic Graph (DAG) for secure and scalable validation of routing decisions.
- A real-time anomaly detection system utilizing FSVM to improve classification confidence and robustness in identifying compromised nodes.
- A trust and EACH selection (CHS) mechanism that balances energy consumption with security.

Extensive testoutcomes demonstrate that the suggested T-BMESR framework attainsmaximalEE, better trust accuracy, and improved detection performance compared to conventional routing and trust-enhanced schemes.

II.RELATED WORK

For Internet of Things (IoT) applications, Joshi and Raghuvanshi proposed a new methodology for identifying the CH and the optimal path in a WSN [18]. The CH, a clustering component, is chosen using a Multi-Objective (MO) Rider Optimisation Algorithms (ROA) that takes into account 3 objectives: distance, energy, and delay. The optimal and efficient route for routing is selected using the MO sailfish optimisation algorithm (SFO).runtime, EC, latency, T, PDR, alive nodes in networks, and the rise in dead nodes all show that the suggested model performs better than previous recent studies. The recommended approach minimizes EC by 30-40% and latency by 40-60% when compared to similar MO routing and clustering algorithms, according to experiments conducted on a dense sensor network. It has the highest time complexity (TC) and does not support Attack Detection (AD).

To address the EE problem via CHS in WSN, an EE CHS using Enhanced Sparrow Search Algorithm with Differential Evolutions (EECHS-ISSADE) has been suggested by Kathiroli and Selvadurai [19]. It leverages the High-Level (HL) search efficacy of SSA and the dynamic ability of DE, which prolongs the node lifespan. The performance of this hybrid model is based on T, RE, and the count of nodes that are alive and dead. The ISSADE framework

recommended for choosing the best CH shows gains in RE and T when compared to previous approaches. AD is not taken into account in the RP.

The EECHS-Artificial Rabbits Optimisation (EECHS-ARO) procedure was introduced by Ramalingam et al. [20] in order to reduce the level of EC and raise the NL in a WSN. The EECHS-ARO method balances enhanced exploration and exploitation throughout the search phase to select the best CH.

For WSN, Yang et al. [21] introduced a new cluster RP. For selecting the CH and relay nodes, the multi-policy fusion snake optimisers (MSSO)is utilized by this method. Then, for inter-cluster routing, it utilizes the Minimum Spanning Trees (MST). This willprolong the method's lifetime and conserve network energy. In order to determine the optimal clustering technique, methods that utilizes the adaptive alpha mutations, bi-directional search optimisation, and dynamic parameter updates in MSSO are offered in this study. These proceduresgreatly accelerate system convergence and extend the accessible search space (SS). For WSN, a unique and effective clustering RP is also presented.

For selecting CH and relay nodes, the model generates several Objective Functions (OF) based on factors such as location, energy, BS distance, inter-cluster separation, intra-cluster compactness, and other relevant criteria. When selecting CH, MSSO incorporates the Fuzzy C-Means (FCM) approach to improve the algorithm's optimisation performance. The relay node selects the next hop node based on direction, RE, and distance when planning inter-cluster routing.

For WSN, Hu et al. proposed a new trust-based secure and EE RP (TBSEER) [22]. TBSEER determines the total TV with energy TV, adaptive direct TV, and indirect TV. The TBSEER is not impacted by flood, sink hole, black hole (BH), or SFA. To swiftly identify MN, the adaptive penalty mechanism (APM) and volatilisation factor (VF) are employed.

The nodes are only required to compute the direct TV; the Sink decides the indirect TV in order to reduce the EC caused by repetitive computations. Finally, by identifying the benign MH Route (MHR) based on the entire TV, the CHs actively stop WH attacks. In addition to reducing network EC and accelerating MN detection, the suggested TBSEER is resistant to all common assaults. The results of the simulation showed it. CH has been chosen based on its TV in WSN.

To enhance network communication, the beneficial Enhanced Fuzzy C means and Adaptive time division multiple access Scheduling (ECATS) method was presented by Kavitha and Ananthakumaran [23].CHS is based on energy utilised to regulate the DA across multiple WSN nodes in order to ensure that the Mobile Sink (MS) receives Data Packets (DP) on time. Here, the method named hybridisation of Time Division Multiple Access-based ALO scheduling is introduced for the purpose of selecting an optimal CH and also for EE improvement. The ECATS approach optimises the following WSN performance characteristics: PDR, T, least EC, communication overhead, and E2ED. Not specifying a routing plan between CHs or evaluating how resistant this approach is to various kinds of assaults.

The ACO-based QoS aware energy balancing(EB) secure routing (QEBSR) approach has been suggested by Rathee et al. [24] for WSN. The end-to-end (E2E) transmission delay and the trust factors of the nodes on the routing paths are computed with the support of an improved heuristics. The limitations in the Distributed EB routing and EE routing with node-compromised resistances are resolved by the suggested method. The QEBSR procedureperforms wellin contrast to the other two techniques by performance. Determining weight vectors is either impossible or very difficult in some circumstances, which makes it time-consuming and hard to evaluate how resilient this system is to various attacks.

Using an edge node (EN) with mobility capabilities, Saleh et al. [25] introduced the Trust-Aware Routing Mechanism (TARM) to collect data from faultless nodes. To distinguish abnormal and defective nodes from healthy ones, the EN use a TEM. The clusters are formed from the deployed SN by TARM using a modified variant of Grey Wolf Optimisation (GWO). Determining every cluster’s TV is done after the cluster formation, and the EN begins collectinginformation across the relevant CH only from reliable nodes. The most efficient route between the dependable and mobile EN is followed by the ABC algorithm. It takes a lot of time and doesn't evaluate how resilient this approach is to different types of threats.

Hriez et al. presented a clustering approach with a trust model that identifies untrusted nodes using energy and data trust [25]. Additionally, by using the advantages of stochastic fractal search optimisation, the proposed clustering algorithm expands the NL. The implementation of Fitness Function (FF) may assist in choosing the CH from the trusted nodes. The function is based on the following four variables: 1) the RE of the nodes; 2) their density; 3) the distance between each node and the base station; and 4) the energy dissipated by the network. It falls into the local minimum and disregards QoS constraints.

EASR is presented in [26]. To protect against several threats and increase the speed at which malicious conduct is detected, EASR uses a trust-based routing model. To choose an optimal CH, an enhanced threshold function and energy trust are suggested. EASR incorporates a trust architecture that is resistant to common routing threats and considers EE. The purpose of APM and VF is to build a thorough TV in order to assess trust nodes and speed up MN identification. The outcomes of the simulation demonstrate how well EASR defends against BH and SFA.

III. Proposed Methodology

The proposed T-BMESR framework aims to ensure secure, energy-aware, and intelligent routing in hierarchical WSNs by integrating adaptive trust modeling, BC validation, and Fuzzy Based Support Vector Machine (FBSVM)–based anomaly detection. The framework has5 core phases: cluster formation, CH selection (CHS), trust evaluation, secure blockchain integration, and FSVM-enhanced ID.

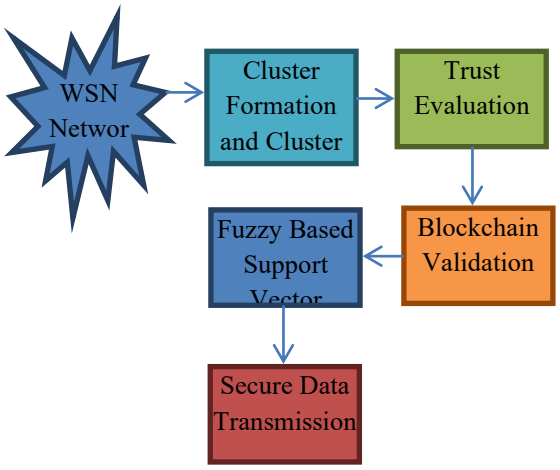


Figure 1: Suggested Flow Diagram

A. Network-model

With distinct ID, n energy-constrained nodes are randomly placed around the m*m network region in T-BMESR. Each cluster contains a CH and several cluster members (CM), and the network is divided into cluster groups as illustrated in Fig. 1. Cluster formation, data collection from CM, DA, and DT to BS via SH or MH transmission are all under the control of CH. Through other CH, the CH can concurrently access BS directly or indirectly. In the cluster group, CH is directly accessible to CM. The following network assumptions are made without sacrificing generality:

- All nodes, including BS, are immobile upon node deployment.
- The initial energy, storage, sensing range, and processing of each node are all the same.
- BS can communicate with any node and has limitless energy and resources.
- To choose reliable nodes for safe communication, the trust model calculates direct, indirect, and comprehensive TV.

B. Energy dissipation model

Recharging node batteries is challenging when nodes are placed in hostile and unsupervised environments. In order to prevent needless energy waste, it is crucial to take the EC of nodes into account when routing. The T-The free space and multipath fading models are used in the BMESR radio energy model. Distance d of transmitting x data bits from the EC of node n_i to node n_j is

$$ET_{(i,j)} = \begin{cases} x * E_{elec} + x * \varepsilon_{fs} * d^2 & d < d_0 \\ x * E_{elec} + x * \varepsilon_{mp} * d^4 & d \geq d_0 \end{cases} \quad (1)$$

To receive x bits of data, EC at node $n_j$is calculated as follows:

$$ER_{(i,j)} = x * E_{elec} \quad (2)$$

Here $d_0 = \sqrt{\frac{\varepsilon_{f_s}}{\varepsilon_{mp}}}$, For modulation and digital coding d_0, the EC of electronic circuit is denoted as E_{elec}. When $d \geq d_0$, $d < d_0$is a threshold. The amplification parameters of transmitter hardware circuit is represented as $\varepsilon_{f_s}$and ε_{mp} .

The following represents the EC for aggregating x data bits:

$$E_{agg} = x * E_{DA} \quad (3)$$

The radio energy per packet is denoted by E_{DA}.

Assume E_{ini} as an initial energy. The following equation expresses the residual energy (RE) of all node,

$$RE = E_{ini} - ET_{(i,j)} - ER_{(i,j)} - E_{agg} \quad (4)$$

The energy TV is expressed as follows:

$$E_{tv} = \frac{RE}{E_{ini}} \quad (5)$$

C. Cluster Formation and CHS

SN are usually deployed in huge numbers in a geographical area and are energy-constrained in WSN. Hierarchical RP is used to control scalability and lower EC. where clusters are formed from SN. The CH in charge of each cluster does DA and sends the compressed data to the BS directly or through similar CH.Efficient cluster formation and intelligent CHS are crucial to enhance network lifetime, ensure load balancing, and defend against security threats. In the T-BMESR (Trust-Assisted Blockchain and FBSVM-Enhanced Secure Routing) framework, the clustering mechanism is designed to group sensor nodes into clusters such that data collection and communication with the BS are optimized.

Network Initialization

- All sensor nodes are stationary, homogeneous (i.e., same hardware capability and initial energy E_{ini}), and uniquely identified.
- Nodes are arranged randomly in a 2D sensing field of size $m \times m$.
- The BS is located either inside or outside the sensing field and has unlimited energy.

Cluster Formation Phase

- Sensor nodes self-organize into clusters based on proximity and signal strength.
- Each node computes a CH threshold using a formula that includes residual energy and trustworthiness (comprehensive trust value derived from trust models and FSVM anomaly detection).
- The node with a high threshold value and not chosen as a CH in recent rounds broadcasts a CH advertisement.
- Neighboring nodes receive advertisements from multiple candidates and select the most trustworthy and EE CH.

Enhanced Cluster Head (CH) Selection using Trust and Energy

CH selection is performed through an intelligent threshold-based mechanism that jointly considers the RE and trustworthiness of nodes. The threshold function dynamically evaluates each node's eligibility by integrating energy levels and comprehensive trust values derived from both direct and indirect interactions, supplemented by FSVM-based anomaly detection scores. Nodes that exceed the calculated threshold and have not recently served as CHs broadcast their candidacy, and neighboring nodes choose the most suitable CH based on trust and proximity. This process ensures that only reliable and energy-efficient nodes are assigned as CHs, thereby mitigating security risks such as selective forwarding or Sybil attacks. Additionally, CH roles are rotated periodically to ensure load balancing and prevent energy exhaustion of individual nodes. This strategy guarantees secure, stable, and energy-optimized communication within the WSN while

maintaining high detection precision and trust accuracy.

To ensure secure and energy-aware routing, a hybrid threshold function drives CHS, defined as:

$$T(n) = \begin{cases} \frac{P}{1-P.(r \bmod \frac{1}{P})}.\left(\propto.\frac{RE_n}{E_{ini}} + \beta.CT_{(n)}\right), & if\ n \in G \\ 0, & otherwise \end{cases} \quad (6)$$

Here:

- P: The optimal % of CHs in each round (e.g., 5%).
- r: Current round number.
- G: Set of nodes that have not been CHs in the past 1/P rounds.
- RE_n: Residual energy of node n.
- $CT_{(n)}$: Comprehensive trust value of node n.
- α, β: Weights (typically $\alpha + \beta = 1$) to balance energy and trust contributions.

This formula ensures only nodes with high RE and high TV are considered for CH roles. It prevents malicious, misbehaving, or low-energy nodes from degrading cluster performance or network security.

Once CHs are elected and broadcast their status, the remaining nodes (CMs) choose the nearest CH with the highest trust value. CMs send Join Requests, and CHs acknowledge these to finalize cluster formation. Data collection, DA, and secure transmission from its CMs to the BS are now the responsibilities of each CH.

To avoid quick depletion of CH energy, CH roles rotate periodically based on threshold re-evaluation. This ensures load balancing and prolongs network lifespan by distributing responsibilities evenly across the network.

D. Trust –evaluation model

Direct trust (DT)

By observing how neighbouring nodes behave, the DT value of a node is calculated. By looking at the neighbor's sending and receiving packet status, the DT function is established. The calculation of DT between node n_i and neighbour $n_j$is

$$DT^n_{(i,j)} = \varphi * HT^n_{(i,j)} + (1-\varphi) * NT^n_{(i,j)} \quad (7)$$

Here, the historical TV of node $n_i$as assessed by node $n_j$in the past is represented by $HT^n_{(i,j)}$.In the current cycle, node n_i evaluates the TV of neighbour n_j, that is denoted as $NT^n_{(i,j)}$.$NT^n_{(i,j)} = r^n_j + s^n_j$.

The factors are measured by φ and $1-\varphi$, thehistorical TV and current TV. These values are set for fairness under particular conditions, $0 < \varphi < 1$. Then, 0.5 is a common value of φ. The ratio of packetsthat are received and send by node n_j to the total number of packets is represented by r^n_j and s^n_j:

$$r^n_j = \frac{\tau * rn_j - Zn_j}{\ln_j} \quad (8)$$

$$s^n_j = \frac{\tau * sn_j - un_j}{\ln_j} \quad (9)$$

Node n_j denied to receive and send data, as indicated by $Zn_j$and un_j. $\ln_j$ is the over-allcount of packets transmitted and received by n_j. Misbehaviour nodes' trust value decreases more quickly due to the adaptive penalty factor τ.

$$\tau = \frac{-p}{1+l^{-q^*(XYn_j+w)}} + 1 \quad (10)$$

$$XY_{n_j} = \frac{MX_{n_j}}{NX_{n_j}} \quad (11)$$

Here, the ratio of misbehaviour MX_{n_j} to normal behaviour NX_{n_j} across the previous five trust computation cycles is denoted by XY_{n_j}. The variable parameters of τ are , q and w. MX_{n_j} rises quickly when a misbehaviour node is caught, which lowers the ratio of $XY_{n_j}$and, in turn, the τ values was reduced. The current assessment can be limited by MN's previous TV, which can be difficult to identify throughout the evaluation cycle. Prior to being recognised as a misbehaviour node, MN was a normal node with a higher TV. In practice, it requires more evaluation cycles to determine whether something is suspicious.The volatilisation factor Δ is included to increase the recognition speed and lessen the impact of historical TV. For the current evaluation cycle, historical TV is calculated using the formula below:

$$HT^n_{(i,j)} = \Delta * (DT^{n-1}_{(i,j)} + HT^{n-1}_{(i,j)}) \quad (12)$$

Indirect trust (IDT)

If there is insufficient information sharing between nodes or if the channel is impacted, IDT can be assessed for the node to progress the precision of the trust evaluation. Through the use of common nodes, IDT offers the TV between the node and the target nodes. The IDT between nodes $n_i$andn_j is computed as follows:

$$IDT^n_{(i,j)} = \sum_{m\in q}\left(\varphi_m * DT^n_{(i,m)} * DT^n_{(j,m)}\right) \quad (13)$$

Here,$n_i$and n_j jointly hold a collection of trusted nodes denoted by q. To filter neighbour nodes and stop third-party node m from launching attacks, common neighbours of $n_i$and $n_j$may have trusted or untrusted nodes. The following expression is provided to improve security and filter false evaluations:

$$dt^n_m = \sqrt{\frac{\sum_{V_X\in V}\left(\bar{D}-DT^n_{mV_X}\right)^2}{L}} \quad (14)$$

Here, node n_i evaluates node V_x. The median is denoted by D. The nodes jointly owned by $n_i$and the third party node m are denoted by V_x, whereas the common neighbours are represented by L. When m is set to a recommendation threshold value of 0.5, the correspondence value suggested by m is dt^n_m. The misbehaviour of m rises by L if $dt^n_m$is > the threshold, and node n_i does not accept the m suggestion value. To increase trust accuracy, node m is given weights, which are stated as follows:

$$\varphi_m = \frac{DT^n_{(i,m)}}{\sum_{m\in q} DT^n_{(i,m)}} \quad (15)$$

Comprehensive trust

Comprehensive trust combines DT and IDT to indicate if a node is trustworthy or not, resulting in strong security and reliable nodes.

$$CT^n_{(i,j)} = \begin{cases} (1-\beta) * DT^n_{(i,j)} + \beta * IDT^n_{(i,j)} & if\ n_j \neq m \\ (1-\beta) * IDT^n_{(i,j)} + \beta * DT^n_{(i,j)} & else\ n_j = m \end{cases} \quad (16)$$

$$\beta = \begin{cases} 0.5 & if\ dt^n_m < \mu \\ DT^n_{(i,j)} - IDT^n_{(i,j)} \middle| DT^n_{(i,j)} & else\ \ dt^n_m \geq \mu \end{cases} \quad (17)$$

The outcomes of the evaluators' assessments are the primary focus of comprehensive trust, the weight coefficient is denoted by β.

E. **Blockchain Scalability and Consensus Optimization:**

In the T-BMESR framework, the integration of a lightweight blockchain layer serves as the security backbone for validating trust scores, Cluster Head (CH) elections, and anomaly detection events. Unlike conventional blockchains (e.g., Bitcoin's Proof of Work) that are computation-heavy and energy-inefficient, T-BMESR uses optimized mechanisms — Proof of Authority (PoA) and Directed Acyclic Graph (DAG) — tailored for resource-constrained WSNs.

To ensure tamper-proof validation and decentralized control of routing operations in WSN, Proof of Authority (PoA) consensus and a Directed Acyclic Graph (DAG) ledger structure are combined in the proposed T-BMESR framework to create a lightweight and energy-efficient BC mechanism. The enormous computational and energy requirements of traditional BC algorithms, such PoW, make them completely inappropriate for WSNs.In contrast, PoA is a reputation-based consensus protocol in which a limited number of trusted nodes — typically Cluster Heads (CHs) with high RE and high TV — are designated as validators. These validators have the exclusive right to approve and sign transactions, including CH elections, trust value updates, and anomaly detection events. When a node is selected as CH after satisfying the threshold function:

This election is not finalized until PoA validators verify the legitimacy of the selection. The verification involves confirming that the RE of the nodeREnRE_nREn and comprehensive TV of CT(n)CT(n)CT(n) meet the criteria. Once verified, the election event is recorded in the blockchain, thus making it tamper-resistant and historically traceable.

To enhance scalability and reduce latency, the blockchain ledger in T-BMESR adopts a Directed Acyclic Graph (DAG) structure instead of a linear chain. In this structure, each event — whether it is a CH election, a trust value update, or an FSVM-based anomaly detection report — is treated as a transaction node (vertex) in the DAG. Each vertex includes the following attributes: timestamp, transaction type (e.g., CH Election, Trust Update),

the node's ID, cryptographic signature, and a hash reference to its parent nodes in the DAG. This parallel structure allows multiple transactions to be recorded concurrently, without requiring strict ordering, thereby improving throughput and responsiveness. The hash chaining between vertices ensures data immutability, while digital signatures maintain authenticity and accountability.

The equation that links a new DAG vertex $v_t$to its predecessors $\{v_1, v_2\}$ can be represented as:

$$H(v_t) = Hash(ID_t \parallel T_t \parallel \sigma_t \parallel H(v_1) \parallel H(v_2)) \quad (18)$$

Where:

- $H(v_t)$: Hash of the current transaction,
- ID_t: Node ID performing the transaction,
- T_t: Type of event (e.g., CH election, anomaly),
- σ_t: Digital signature of the validator node,
- $H(v_1), H(v_2)$: Hashes of the parent nodes (past events).

By storing transactions in this DAG structure, the system enables:

- **Tamper-proof validation**: Any alteration in past records would require breaking the entire hash chain.
- **No centralized control**: CHs collaboratively manage the consensus and storage.
- **Historical accountability**: All past trust evaluations and CH elections are permanently auditable.

Furthermore, when an anomaly is detected by FSVM (e.g., due to high packet drop rate or energy drain), the trust model reduces the node's comprehensive TV, and this trust degradation event is logged as another DAG vertex. This ensures that misbehavior is cryptographically captured and shared across the network, thereby preventing the node from being elected as CH in future rounds. Thus, the blockchain layer serves as a decentralized control system that safeguards the integrity of CH selection and routing, enables trustworthy behavior validation, and promotes network self-healing through auditable and verifiable updates.

F. FSVM-Based Anomaly Detection and Secure Data Transmission

In the proposed **T-BMESR (Trust-Assisted Blockchain and Machine Learning-Enhanced Energy-Aware Secure Routing)** framework, **anomaly detection** and **secure data transmission** are interdependent components that operate in synergy to ensure high data reliability, energy efficiency, and resistance to node-level attacks. These processes are tightly integrated with **trust evaluation**, **cluster head (CH) selection**, and **blockchain validation**, facilitating WSN's intelligent decision-making

Anomaly Detection Using FSVM

To reliably detect compromised or malfunctioning nodes, a **FSVM** is implemented at the trust management layer. Traditional SVMs often fail under real-world WSN conditions due to noise, partial faults, and uncertainty in data. FSVM enhances robustness by assigning **fuzzy membership values**$\mu_i \in [0,1]$ to each training instance x_i, representing its degree of reliability.

The modified FSVM optimization function is:

$$\min_{w,b,\xi} \left(\frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n} \mu_i \xi_i\right) \quad (19)$$

Subject to:

$$y_i(w^T\phi(x_i) + b) \geq 1 - \xi_i, \xi_i > 0 \quad (20)$$

Here:

- w and b: Classifier parameters,
- $\phi(\cdot)$: Kernel function for non-linear mapping,
- ξ_i: Slack variables for soft margin,
- $y_i \in \{-1, +1\}$: Binary classification (anomalous or normal),
- μ_i: Fuzzy membership based on behavioral deviation.

The feature vectorx_i is constructed from key metrics:

$$x_i = [PDR_i, RED_i, Delay_i, Density_i, TC_i] \quad (21)$$

These features correspond to packet drop rate, residual energy deviation, communication delay, neighbor density, and transmission consistency — all of which characterize the operational integrity of each node.

The FSVM model continuously classifies node behavior in real time. When a node is flagged as anomalous($y_i = -1$), its comprehensive trust value (CTV) is immediately reduced. This change is recorded on theblockchain using PoA validators, preventing the node from acting as a CH or participating in routing. This feedback loop ensures that the network continuously learns and adapts to malicious patterns without manual intervention.

Secure and Adaptive Data Transmission

The data transmission phase starts after cluster formation and CHS (based on trust and energy).It consists of:

- **Intra-cluster communication**: SN (CM) send their sensed information to their respective CH.
- **Inter-cluster communication**: CHs forward the DA toward the BS, either directly (SH) or through trusted relay CHs (MH).

Before data forwarding, each CH performs data aggregation to eliminate redundancy and reduce packet size:

$$D_{CH} = f_{agg}(D_{CM_1}, D_{CM_2}, \dots, D_{CM_k}) \quad (22)$$

Where f_{agg} is the aggregation function (e.g., averaging, max/min, filtering), and D_{CM_i} is the data from the i-th CM.

To ensure reliable delivery and minimize energy waste, CHs employ Carrier Sense Multiple Access (CSMA) techniques. Prior to sending, the CH senses the wireless channel. If the channel is busy($C_{busy} = 1$), the CH enters a wait state until a Clear Channel Assessment (CCA) message is received. Otherwise, if $C_{busy} = 0$, the CH transmits the data:

$$T_{send} = \begin{cases} wait, & if\ C_{busy} = 1 \\ Transmit, & if\ C_{busy} = 0 \end{cases} \quad (23)$$

The routing path from CH to BS is determined by evaluating available CHs based on:

- Updated trust values (CTV),
- Residual energy (RE),
- Validation via the blockchain ledger.

Only CHs whose trust scores exceed a dynamic threshold θ_t and are not flagged as anomalous by FSVM are selected:

$$Node\ n_i\ eligible\ for\ routing \iff CT_{n_i} \geq \theta_t\ and\ y_i = +1 \quad (24)$$

This strict condition ensures that data only flows through verified, trustworthy, and high-energy nodes. Furthermore, the FSVM-based anomaly scores are periodically re-evaluated and used to adjust trust scores, which in turn influence routing paths and future CH selections.

Pseudo code for T-BMESR Framework

1. Initialize WSN with n sensor nodes

  For each node:

    Assign initial energy, trust = 1, status = Normal

  Place Base Station (BS)

2. Cluster Formation

  Partition network into k clusters based on proximity and energy

  For each cluster:

    Elect Cluster Head (CH) using:

CH_Score = α * Energy + (1 - α) * Trust

    Highest CH_Score → CH

    Other nodes → Cluster Members (CM)

3. Trust Evaluation Loop

  For each time cycle t:

    For each node i:

      For each neighbor j:

        Compute Direct Trust DT(i,j)^t

        Compute Indirect Trust IDT(i,j)^t

Compute Comprehensive Trust CT(i,j)^t

Update Trust Table T[i]

4. Blockchain Validation (PoA and DAG)

If CH is elected or Trust Table is updated:

Create transaction block B with:

- Node ID, Trust Score, CH ID, Timestamp

Validate B using PoA by existing CH nodes

Append B to DAG ledger

5. Fuzzy SVM-based Anomaly Detection

For each node:

Collect features: energy drop rate, packet drop rate, delay

Feed into FBSVM model → classify as Normal or Malicious

If node is Malicious:

Reduce trust score

Trigger alert and exclude from routing

6. Secure Data Transmission

For each CM in a cluster:

Send sensed data to CH (intra-cluster)

CH aggregates data:

Wait for channel availability (CCA)

Send aggregated data to next CH or BS (inter-cluster)

Use multihop routing based on highest CT and residual energy

7. Energy and Trust Update

For each node:

Update energy based on:

Transmit, Receive, Aggregate operations

Update E_tv = Remaining Energy / Initial Energy

Recompute CH Score

8. Repeat steps 3–7 for all rounds until energy threshold or node death

9. End Simulation

IV.EXPERIMENTAL RESULT AND DISCUSSION

The network simulator NS2 tool is used in this part to simulate and perform T-BMESR performance with an experimental setup. A BS is situated on top of the sensing region, and 100 nodes are arranged at random throughout a 1000 × 1000 m network space as part of the simulation setup. The trust model is used to introduce and identify MN like BH and SFA. Table 1 displays all of the simulation parameters. Every SN has the same energy level and is uniform and static. Performance indicators including network T, packet deliver ratio (PDR), NL, and EC are calculated and the suggested T-BMESR is compared with ETOR [20], MSCR [21], TBSEER [22], and EASR.

Table 1: Simulation parameters

Parameter	**Value**
Systemconfigurationregion	1000 ×1000 mts
SNinstalled in system	100 nodes
Initial energy allocated	2J
DA energy	20 nJ
Transmission energy	30 nJ
Receiver Energy	20 nJ
Packet Size	256
MAC	802.11
TV	(0 to 1)
Rounds Count	50
BS	1

i.Network Throughput

It is the proportion at which valid DP are successfully distributed to the destination (Base Station) over the communication channel. It reveals the data delivery capacity of the routing protocol.

$$Throughput = \frac{\sum_{i=1}^{N} P_i \times S_i}{T_{Sim\ Time}}$$

Where:

- P_i: Number of successfully received packets by node iii
- S_i: Size of each packet (in bits or bytes)
- $T_{Sim\ Time}$: Total simulation time (in seconds)
- Units: kbps or bps

ii.PDR

When compared to the total packet count that are $sent$ by the source nodes, PDR is the proportion of DP that are effectively$received$ by the destination. It assesses the RP's dependability.

$$PDR\ (\%) = \left(\frac{P_{received}}{P_{sent}}\right) \times 100$$

Where:

- $P_{received}$: Over-allcount of DP received by the BS
- P_{sent}: Over-allcount of DP sent by all SN

iii.NL

The amount of time (rounds) until a specific proportion of nodes run out of energy is known as NL. It is a crucial indicator of the protocol's sustainability and EE.

$$Network\ Lifetime = R_{last\ alive}$$

The number of simulation rounds until all nodes are dead or the first threshold is achieved is denoted by $RR_{last\ alive}$.

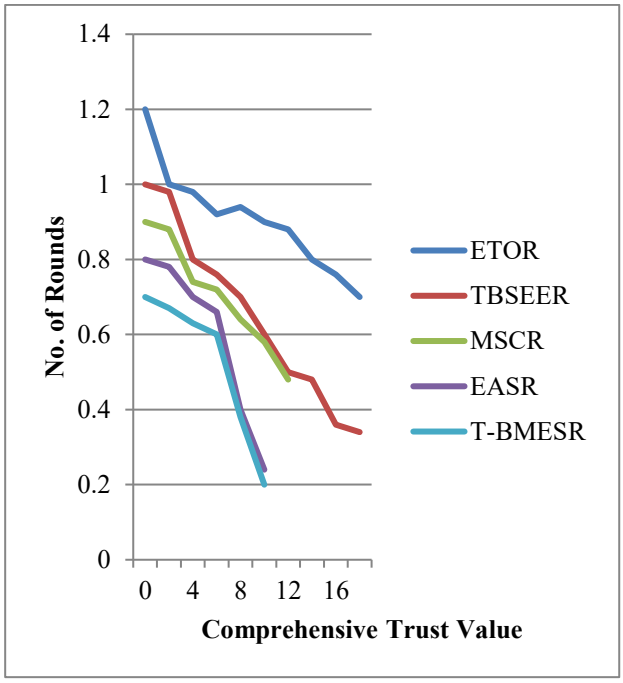
iv.EC

Throughout the entire simulation, the total EC by all nodes. It helps measure the efficiency of the RP in using battery power.

$$Energy\ Consumption = \sum_{i=1}^{N}\left(E_{init}^{i} - E_{rem}^{i}\right)$$

Where:

- E_{init}^{i}: node i's initial energy
- E_{rem}^{i}: Remaining energy of node i at the termination of experiment
- Units: **Joules (J)**



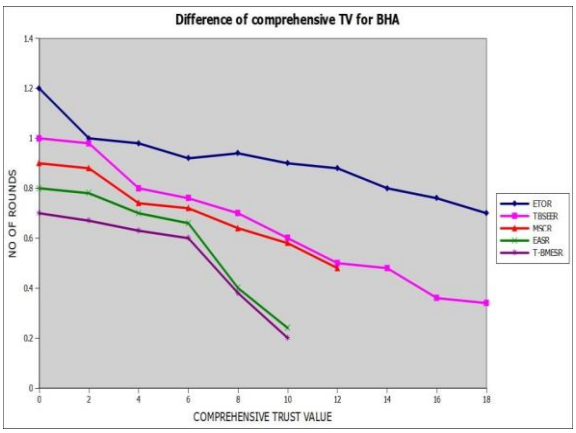


Fig. 2 (a). Difference of comprehensive TV for BHA

This figure 2 (a) illustrates the dynamic behavior of comprehensive trust values for nodes affected by blackhole attacks (BHA). The MN in BHA drops incoming packets after deceptively promoting the best routes.As the attack progresses, the trust evaluation model in T-BMESR detects abnormal behaviors (e.g., abrupt packet drop, irregular energy usage) through the FSVM module. The figure shows a significant decline in the TV of the MN over successive evaluation cycles, indicating successful detection and penalization. The adaptive penalty and volatility factors accelerate the trust degradation, ensuring rapid isolation of the attacker.

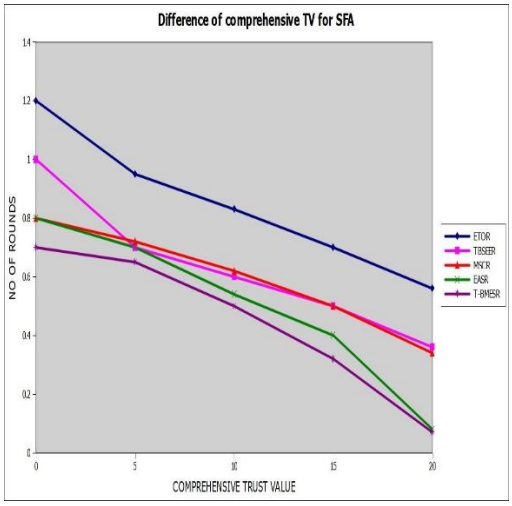


Fig. 2(b). Difference of comprehensive TV for SFA

This graph 2 (b) demonstrates the variation in trust values for nodes performing selective forwarding attacks, where only a subset of packets are maliciously dropped. Unlike blackhole attacks, this behavior is intermittent and harder to detect. The figure shows that T-BMESR still achieves a gradual but steady fall in the comprehensive TV of the attacker node. This is made possible through the integration of direct, indirect, and FSVM-based anomaly detection. The system effectively distinguishes inconsistent behavior patterns and lowers trust values even when the attack is sporadic.

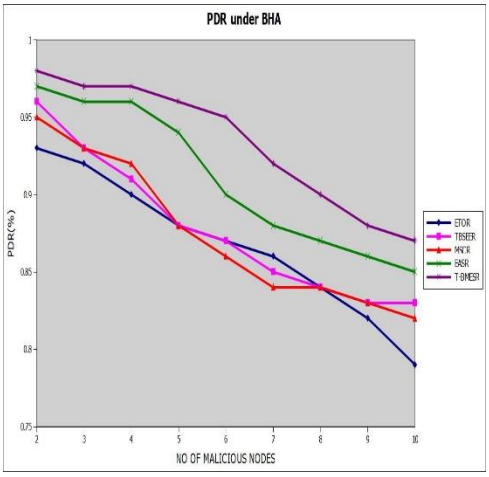


Fig. 3 (a). PDR under BHA

This figure 3(a) compares the Packet Delivery Ratio (PDR) of T-BMESR with baseline protocols under blackhole attack conditions. The PDR of T-BMESR remains significantly higher, indicating that its trust-aware routing mechanism quickly identifies and avoids compromised nodes. In contrast, baseline protocols without trust or anomaly detection show a sharp drop in PDR as blackhole nodes continue to absorb and drop data packets. This demonstrates T-BMESR's robustness in maintaining reliable data delivery despite the presence of aggressive attackers.

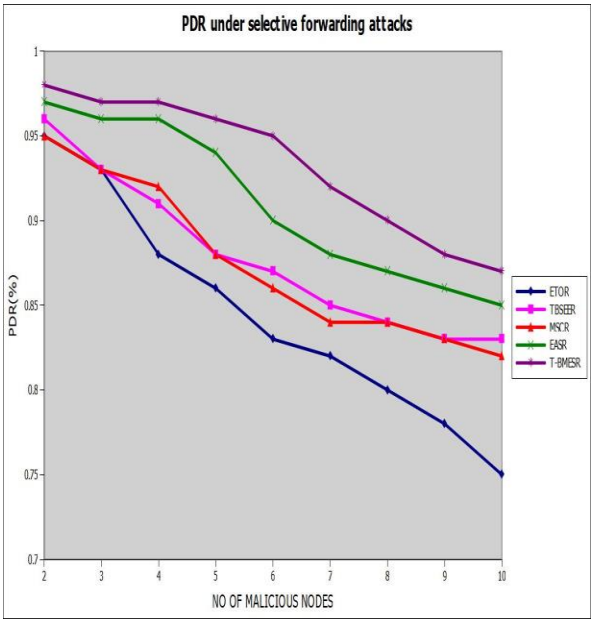


Fig. 3(b). PDR under selective forwarding attacks

The figure 3 (b) presents PDR performance when the network is subjected to selective forwarding attacks. T-BMESR again shows consistently better PDR, outperforming traditional and trust-only models. Even though selective forwarding is subtler than blackhole attacks, the FSVM's fuzzy classification enables real-time identification of partially malicious nodes. The results confirm that T-BMESR successfully maintains packet integrity and avoids untrusted paths during data transmission.

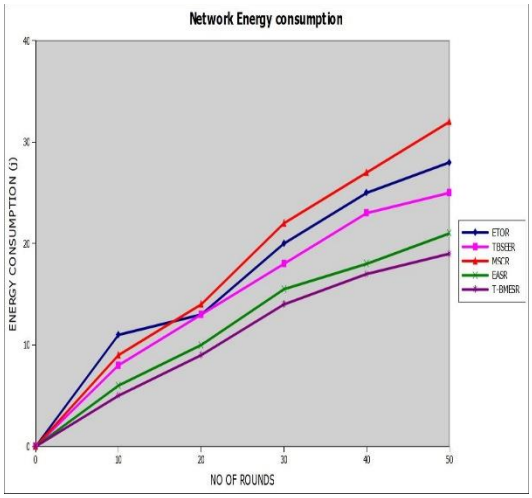


Fig 4. Network Energy consumption

This figure 4 depicts the over-allEC by the network over the simulation period for each evaluated protocol. T-BMESR records the lowest EC, attributed to its intelligent CHS strategy based on both trust and RE. Moreover, early detection and avoidance of malicious nodes prevent unnecessary retransmissions and route discoveries, thereby conserving energy. Baseline protocols such as ETOR and MSCR exhibit higher consumption due to ineffective routing and lack of security mechanisms, which lead to energy wastage from repeated packet loss and re-routing.

V.CONCLUSION

In this paper, an effective methodT-BMESR was suggested for achieving secure, EE, and trustworthy routing in hierarchical WSN.The suggested model combines a strong anomaly detection system based on FSVM, lightweight blockchain consensus utilising PoA and Directed Acyclic Graph (DAG), and adaptive trust modelling.The trust evaluation scheme combines direct and indirect trust metrics with FSVM-based anomaly scores, enabling dynamic detection and isolation of MN such as BHA and SFA. T-BMESR performs better than the current protocols, EASR, TBSEER, ETOR, and MSCR, according to simulation-based studies, in important performance metrics such network T, PDR, NL, and EC. The use of blockchain ensures tamper-resistant trust validation and decentralized control, while FSVM enables real-time classification of node behavior with high accuracy under uncertainty. Overall, a scalable, EASR architecture for mission-critical and hostile WSN situations is effectively accomplished by T-BMESR.

VI.REFERENCES

1. W. Fang, W. Zhang, W. Yang, Z. Li, W. Gao, and Y. Yang, ‘‘Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks,’’ Digit. Commun. Netw., vol. 7, no. 4, pp. 470–478, Nov. 2021, doi: 10.1016/j.dcan.2021.03.005.
2. A. Rachedi and A. Hasnaoui, ‘‘Advanced quality of services with security integration in wireless sensor networks,’’ Wireless Commun. Mobile Comput., vol. 15, no. 6, pp. 1106–1116, Apr. 2015.
3. G. D. Devanagavi, N. Nalini, and R. C. Biradar, ‘‘Secured routing in wireless sensor networks using fault-free and trusted nodes,’’ Int. J. Commun. Syst., vol. 29, no. 1, pp. 170–193, Jan. 2016.
4. K. Thangaramya, K. Kulothungan, S. I. Gandhi, and M. Selvi, ‘‘Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN,’’ Soft Comput., vol. 24, no. 21, pp. 16483–16497, Apr. 2020.
5. L. Zhang, N. Yin, X. Fu, Q. Lin, and R. Wang, ‘‘A multi-attribute pheromone ant secure routing algorithm based on reputation value for sensor networks,’’ Sensors, vol. 17, no. 3, p. 541, Mar. 2017.
6. V. Gomathy, N. Padhy, D. Samanta, M. Sivaram, V. Jain, and I. S. Amiri, ‘‘Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks,’’ J. Ambient Intell. Hum. Comput., vol. 11, no. 11, pp. 4995–5001, Feb. 2020.
7. G. Thahniyath and M. Jayaprasad, ‘‘Secure and load balanced routing model for wireless sensor networks,’’ J. King Saud Univ.-Comput. Inf. Sci.,Oct. 2020, doi: 10.1016/j.jksuci.2020.10.012.
8. K. Hamouid, S. Othmen, and A. Barkat, ‘‘LSTR: Lightweight and secure tree-based routing for wireless sensor networks,’’ Wireless Pers. Commun.,vol. 112, no. 3, pp. 1479–1501, Jan. 2020.
9. M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy, and R. Patan, ‘‘Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks,’’ IEEE Trans. Eng.Manag., vol. 68, no. 1, pp. 170–182, Feb. 2021.
10. M. Mathapati, T. S. Kumaran, A. Muruganandham, and M. Mathivanan, ‘‘Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network,’’ J. Ambient Intell. Humanized Comput., vol. 12, no. 6,pp. 6047–6055, Jun. 2021.
11. W. Fang, W. Zhang, W. Chen, Y. Liu, and C. Tang, ‘‘TMSRS: Trust management-based secure routing scheme in industrial wireless

sensor network with fog computing,'' Wireless Netw., vol. 26, no. 5, pp. 3169–3182,Sep. 2020.

12. L. Wei, Y. Qing, and Y. Nan, ''A trust-based secure routing algorithm for wireless sensor networks,'' in Proc. 34th Chin. Control Conf. (CCC),Jul. 2015, pp. 7726–7729, doi: 10.1109/ChiCC.2015.7260866.
13. A. Ahmed, K. A. Bakar, M. I. Channa, and A. W. Khan, ''A secure routing protocol with trust and energy awareness for wireless sensor network,''Mobile Netw. Appl., vol. 21, no. 2, pp. 272–285, 2016.
14. K. A. Awan, I. Din, A. Almogren, M. Guizani, A. Altameem, and S. U. Jadoon, ''RobustTrust—A pro-privacy robust distributed trust management mechanism for Internet of Things,'' IEEE Access, vol. 7,pp. 62095–62106, 2019.
15. W. Fang, C. Zhu, W. Chen, W. Zhang, and J. J. P. C. Rodrigues, ''BDTMS: Binomial distribution-based trust management scheme for healthcare-oriented wireless sensor network,'' in Proc. 4th Int. Wireless Commun. Mobile Comput. Conf., Jun. 2018, pp. 382–387, doi:10.1109/IWCMC.2018.8450403.
16. R. W. Anwar, A. Zainal, F. Outay, A. Yasar, and S. Iqbal, ''BTEM: Belief based trust evaluation mechanism for wireless sensor networks,'' FutureGener. Comput. Syst., vol. 96, pp. 605–616, Jul. 2019.
17. M. Zhang, ''Trust computation model based on improved Bayesian forwireless sensor networks,'' in Proc. IEEE 17th Int. Conf. Commun. Technol. (ICCT), Oct. 2017, pp. 960–964, doi: 10.1109/ICCT.2017.8359777.
18. P. Joshi, & A. S. Raghuvanshi, "A multi-objective metaheuristic approach based adaptive clustering and path selection in iot enabled wireless sensor networks," International Journal of Computer Networks and Applications, vol. 8, no. 5, pp. 566-584, 2021.
19. P. Kathiroli, & K. Selvadurai, "Energy efficient cluster head selection using improved Sparrow Search Algorithm in Wireless Sensor Networks," Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 10, pp. 8564-8575, 2022
20. R. Ramalingam, S. Basheer, P. Balasubramanian, M. Rashid, & G. Jayaraman, "EECHS-ARO: Energy-efficient cluster head selection mechanism for livestock industry using artificial rabbits' optimization and wireless sensor networks," Electronic Research Archive, vol. 31, no. 6, 2023
21. L. Yang, D. Zhang, L. Li, & Q. He, "Energy efficient cluster-based routing protocol for WSN using multi-strategy fusion snake optimizer and minimum spanning tree," Scientific Reports, vol. 14, no. 1, pp. 16786, 2024.
22. H. Hu, Y. Han, M. Yao, & X. Song, "Trust based secure and energy efficient routing protocol for wireless sensor networks," IEEE access, vol. 10, pp. 10585-10596, 2021.
23. V. Kavidha, & S. Ananthakumaran, "Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink," Peerto-Peer Networking and Applications, vol. 12, pp. 881-892, 2019
24. 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, 2019
25. A. Saleh, P. Joshi, R. S. Rathore, & S. S. Sengar, "Trust-aware routing mechanism through an edge node for IoT-enabled sensor networks," Sensors, vol. 22, no. 20, pp. 7820, 2022.
26. Prasad, V., & Roopashree, H. R. (2024). Energy aware and secure routing for hierarchical cluster through trust evaluation. Measurement: Sensors, 33, 101132.