TPM Vol. 32, No. S5, 2025
ISSN: 1972-6325
https://www.tpmap.org/

DYNAMIC ADAPTIVE SELF-AWARE TRUST ENERGY-EFFICIENT ROUTING WITH BLOCKCHAIN FRAMEWORK FOR WIRELESS SENSOR NETWORK

A. SANGEETHA PRIYA
COMPUTER SCIENCE, SRI KRISHNA ARTS AND SCIENCE COLLEGE, BHARATHIAR UNIVERSITY, INDIA
E-MAIL: sangeetha.cbe95@gmail.com

DR.S. DEVARAJU
COMPUTER SCIENCE, VIT BHOPAL UNIVERSITY, INDIA.
E-MAIL: devamcet@gmail.com

DR. ANTONY CYNTHIA
COMPUTER SCIENCE, SRI KRISHNA ARTS AND SCIENCE COLLEGE, BHARATHIAR UNIVERSITY, INDIA
E-MAIL: antonycynthia@skasc.ac.in

Abstract:
The Dynamic Adaptive Self-aware Trust Energy-efficient Routing with Blockchain (DASTER-Chain) framework is a smart and powerful routing framework for Wireless Sensor Networks (WSNs) that combines Dynamic Self-Adaptive Energy-Efficient Routing (DSA-EER) with Distributed Trust Key Management (DTKM) based on Blockchain. This synergistic combination boosts both performance and security through the utilization of real-time energy metrics, link quality, and adaptive thresholding to facilitate optimal path selection and ensuring the longest sustainable life from the WSN. The blockchain enhanced trust model assures secure, decentralized intrusion detection and trust evaluation methods, along with the removal of single points of failure, as well as improving trust management reliability, and it ensures improved key distribution. DASTER-Chain is capable of reacting quickly to unforeseen changes in the dynamic environment of a WSN, and will not sacrifice performance if nodes become dynamic due to mobility, poisoning, or other actions which lower level of channel energy. Using cost-based routing decisions, without any unnecessary overhead, combined with opportunistic forwarding decisions, these would allocate costs to real time data, not to the WSN on that path, and blockchain supports secure logging, which is always achieved clearly, and is verifiable too in the ongoing trust management scheme. According to experimental evaluations, DASTER-Chain offers superior performance than conventional protocols as well as state-of-the-art approaches such as Fuzzy Logic with Enhanced Particle Swarm Optimization (FL-EPSO), DSA-EER, and standalone DTKM. All crucial performance metrics including network lifetime, energy consumption, packet delivery ratio, end-to-end delays, routing overhead, and residual energy and energy throughput have improved. DASTER-Chain is established as a reliable, energy-enabled, and future-proofed solution for secure and scalable WSNs, primarily when applied to mission-critical and resource constrained Internet of Things (IoT) applications.

Keywords: Blockchain, DASTER-Chain, WSN, Distributed Trust Key Management, Energy-Efficient, Routing, Optimal Path Selection.

I.INTRODUCTION

Wireless Sensor Networks (WSNs) facilitate real-time data collection and monitoring in a range of application areas including such as healthcare, smart environments, industrial IoT, and environmental monitoring (Al-Hubaishi et al., 2019; Ekler et al., 2022; Qadir et al., 2020). WSNs are technically new, but differ from traditional networks in that they are flexible and scalable, meaning that new nodes can be added or removed from the network at any time. However, WSNs have suffered from two ongoing challenges while providing such flexibility and scalability - energy and security. Sensor nodes are usually battery powered, and sending data continuously will drain the battery quickly. Every time a node sends data, the energy is diminished. The node will eventually lose capability, and the network will experience network partitioning. With diminished capabilities, the functionality of the network is depleted (Boyaci et al., 2022; Swapna & Satyavathy, 2022; Haseeb et al., 2019).
Solutions to energy constraints, has led to many energy based routing protocols. Several WSN routing protocols have tried to constrain energy consumption, some have built upon Software-Defined Networking, others used clustering and developed architectures using metaheuristics to try and reduce energy consumption and promote the longevity of the networks (Al-Hubaishi et al., 2019; Samadi et al., 2023; Lakshmanna et al., 2022). However most of these protocols are rigid, and were not constructed with the consideration of dynamicity that could be experienced in real-time changes to the network topology or energy remaining in the nodes which can cause sub-

optimal routing decisions and quicker failures when the routed nodes are replaced (Haseeb et al., 2020; Swapna & Satyavathy, 2022; Qadir et al., 2020).

Equally important is the requirement for strong security mechanisms. WSNs can be susceptible to various attack vectors including eavesdropping, node compromise, and data tampering. Centralized trust and key-management systems do not fit logically in WSN which leads to vulnerabilities characterized by a single point of failure and scalability (Yin et al., 2022; Javaid, 2022; Awan et al., 2022).

Due to its ability to decentralize trust, allow for tamper-proof & transparent trust establishments, key management, and intrusions detections, blockchain has drawn the interest of researchers recently and has the power to disrupt the current state-of-trust (She et al., 2019; Gebremariam et al., 2023; Rehman et al., 2022). Several blockchain base frameworks have also demonstrated improvements in routing security performance, malicious nodes detection, and distributed data management (Nouman et al., 2023; Abd El-moghith & Darwish, 2021; Liang et al., 2020). Lastly, opportunities for using blockchain, federated learning, machine learning models, and trust models, can lead to more reliable and resilient WSNs against cyber-threats (Krishna et al., 2025; Wijesekara & Arachchige, 2025).

Contribution: The contributions of this paper are: Development of the dynamic self-adaptive routing algorithm, DSA-EER which maximized the lifetime of the network by varying energy consumption based on network state. The DTKM blockchain trust model was created to allow users to safely manage their decentralized keys and identify in real time if intrusions were occurring. The proposed framework will be demonstrated through the use of simulations, which will then be compared to existing models.

Organization: The remainder of the paper is organized as follows: Section 2 provides an overview of related work. Section 3 describes the proposed DSA-EER algorithm. Section 4 describes the DTKM trust model. Section 5 presents simulation results. Section 6 concludes the paper and provides some directions for future research.

II. Background Study

Wireless Sensor Networks (WSNs) and Internet of Things (IoT) systems are growing in importance as important application domains from industrial automation to environmental monitoring. There has been recent research into energy-aware routing protocols and potential blockchain- based security mechanisms, but meeting the challenges across efficiency, adaptability and security in resource-constrained environments remains an issue.

2.1 Distributed Energy-Aware Routing

wan et al. (2022) aimed to improve routing efficiency for WSN deployment in livestock production through energy-aware cluster-based routing optimization framework. They focused on minimizing overall energy consumption while maximizing network lifetime using adaptive clustering techniques that address specific agricultural environments. Their work was a good example of how energy-aware routing design could really help sector-specific application with routing designs focused on energy-aware objectives in resource constrained WSNs.

Balakiruthiga et al. (2020) put forward the design of a segment routing based approach for energy aware routing in software defined data center. Their design enabled path selection and data flow control while also maximizing energy consumption reduction at the infrastructure level. Their article illustrated the benefits of segment routing with energy-aware optimization methodologies in large-scale data using environments but was more of a study of data centers than sensor networks.

Zhao et al. (2022) developed a hybrid clustering-based energy-aware routing scheme by integrating a multi-objective genetic algorithm and cuckoo search algorithm. Their methodology, which controlled clustering and routing dynamically to minimize energy consumption while balancing load across sensor nodes, demonstrated the potential of combining bio-inspired algorithms for energy-efficient management of wireless sensor networks.

Yun and Yoo (2021) used a Q-learning-based solution for developing a data-aggregation-aware energy-efficient routing protocol in WSNs. In their design the sensor nodes learn over time the best routing practices to follow, which led to a more intelligent method of conserving energy. Their model used reinforcement learning, which showed how, typically in a dynamic wireless environment machine learning can improve energy efficiency autonomously.

Ri et al. (2022) proposed a distributed energy-efficient opportunistic routing scheme with timeslot allocation to enhance performance in WSNs. Their model considered the energy waste and transmission collisions in their design, which coordinated their communication time epochs between nodes while allowing for transmission to be driven by the opportunistic principle. While their work presented a statistically significant extended network lifetime based on simulations, they successfully demonstrated that through a distributed approach to timeslot management, they could achieve a higher network lifetime than common opportunistic-based routing schemes.

n energy-efficient aggregation-based secure aware routing protocol for WSNs was created by Raja Basha (2020). Their approach included a focus on energy consumption optimization through data aggregation techniques and maintaining high levels of communication security. Having this dual focus provided a better opportunity for energy efficient data delivery and secure data delivery in sensor networks in a hostile or adversarial setting.

Table 1: Comparison table on Energy-Aware Routing

Reference	Focus Area	Method Used	Application Domain	Special Feature

Almuntasheri & Alenazi (2022)	SDN-based Energy-Aware Routing	Software-Defined Networking (SDN)	Industry 4.0	Centralized control and dynamic energy optimization
Saba et al. (2020)	Energy-aware Clustering and Routing	Energy-aware Graph Clustering with Supervised Learning	General WSN	Intelligent routing with graph-based clustering
Jecan et al. (2022)	Predictive Energy-Aware Routing	Predictive algorithms evaluated on real WSN hardware	Industrial IoT	Hardware-based validation of routing performance
Saleh et al. (2021)	Energy Harvesting and Aware Routing	Energy Harvesting + Adaptive Routing	Heterogeneous Energy WSNs	Routing based on harvested energy levels

2.2 Intrusion Detection using Block-Chain Methodology

Wardana et al. (2024) presented a lightweight and privacy-aware collaborative intrusion detection system for IoT contexts. By accepting a trust management approach, the authors provided effective detection of malicious activities without compromising device privacy. Their approach only concerned itself with a low computational cost which, therefore, was particularly relevant for IoT systems that are limited in their resources. The evaluation showed that there were obvious improvements in their intrusion detection effectiveness over the systems previously discussed with no negative impact on energy consumption.

umar et al. (2025) who created an integrated trust-based intrusion detection system that enlarged security for routing protocols in networks. The authors supported trust evaluation and networks with some anomaly detection processes that successfully completed routing based attacks protection. The authors describe insiders as vulnerabilities, while also making a mention of how the complexity of old intrusion detection algorithms would plan with other mentioned threats. The authors found improvements in networks to address reliance due to insider-based intrusion detection through several simulations results. The authors completed an outlined plan to develop a model that would reduce false-positives and legitimize without jeopardizing routing effectiveness.

Rajasoundaran et al., (2021) conducted a machine learning based volatile blockchain to build a security routing system for decentralized military sensor networks. They suggest generic for the field of machine learning based dynamic routing, the use of two different machine learning models to predict behavior of nodes and develop a blockchain to dynamically validate the secure routing. The authors ultimately contributed their work to secure communications specifically, military-based Wireless Sensor Networks (WSNs) with regards to security and trust, ultimately supporting reliable and tamper resistant communications. Their performance results indicate increased trustworthiness in mound and decreased attack surface respectively.

Sivaganesan (2021) created a data-driven trust framework to manage threats to IoT sensor networks using blockchain. They took advantage of the benefit of using real-time data, along with storing immutable records using blockchain technology, to improve early attack detection and provide a cryptographic basis for communicating between nodes. Their approach took advantage of automating trust and distributed architecture to improve reliability of IoT deployments. I have tested their method and showed that it could be usefully applied to different IoT threat tactics.

Ismail et al. (2023) provided a literature review relating to securing wireless sensor networks using machine learning, blockchain and machine learning. In their literature review, they analysed approaches that have been proposed previously, organised based on detection techniques, and identified strengths and limitations of those approaches. They showed that that the integration of ML and blockchain in security for WSN is a growing trend and has the potential for effective, reliable security solutions that are scalable. Along with a discussion of WSN security trends related to ML and blockchain avenues for future research to combine intelligent analytics with trust frameworks are identified.

Ahmed and Abed Al-Asadi (2024) introduced a blockchain based trust management framework designed for secure and energy-aware routing in mobile ad hoc networks. It proposed the use of energy-aware metrics, combined with a trust evaluation that was blockchain based to make informed routing decisions which were secure. Their proposed model balanced both energy and building trust, making it efficient for dynamic and mobile environments. They validated their model through experimental modelling, showing significant improvements in terms of security assurance and network lifetime.

Table 2: Comparison table on Blockchain Methodology in WSNs

Author(s) & Year	Main Focus	Technologies	Contribution
Tariq et al. (2020)	Internal attack detection in IoT	Blockchain, Multi-Mobile Code	Proposed a trust mechanism using mobile codes and blockchain for early internal threat detection.
Saeed et al. (2024)	Malicious node detection & efficient data storage in WSNs	Blockchain, IPFS	Introduced blockchain and IPFS integration for reliable node detection and decentralized data storage.
Alrahhal et al. (2022)	Trust establishment in WSNs	Acknowledgment-Based Trust	Designed a lightweight trust mechanism based on acknowledgments to detect misbehaving nodes.
Qureshi et al. (2024)	Malicious node detection in Flying Ad Hoc Networks (FANETs)	Blockchain, Authentication	Developed a blockchain-based trust and authentication model to detect and isolate malicious nodes in FANETs.

II.3 Problem Identification

Although there have been important developments in energy-aware routing protocols and blockchain-based intrusion detection systems in Wireless Sensor Networks (WSNs) and Internet of Things (IoT) applications, numerous obstacles persist. Maintaining a balance among aspects like energy management, scalability, and security, and even choosing whether or not to adapt to a dynamically changing and hopefully less resource-constrained network add challenges in a physical or real-world WSN. Consequently, many emerging and existing techniques will likely fail to transfer to the opportunities afforded by a real-world and dynamic scene, where aspect like mobility, variations in energy heterogeneity, unbalanced resource sources, and variability remains an unsolved dilemma. In addition, energy-aware routing and blockchain-like security solutions, tend to carry high computational overhead, complexity and delay, may easier but bounded trust assessment, and limited scalability in regards to the number of nodes, which would ultimately affect performance. Thus, it is clear that a need exists for adaptive energy-aware frameworks that can simultaneously support secure communications and sustainable operations of WSNs and IoT's with limited resources that are dynamic.

III.MATERIALS AND METHODS

The materials and methods for this study discuss the design and implementation of two critical components to improve the performance and security of Wireless Sensor Networks (WSNs): Dynamic Self-Adaptive Energy and Efficient Routing and DTKM. The dynamic energy-aware routing utilizes the concept of a mobile agent that allows nodes to autonomously discover the most energy-efficient path based on the state of the residual energy, link quality, and distance. The mobile agent can also dynamically adjust to the evolving network state and minimize node energy drain and the overall network lifetime. The DTKM algorithm uses a blockchain methodology in order to include and improve WSN security by evaluation of trust in real time, intrusion detection and trust key management security. This approach uses a decentralized trust model to detect abnormal behavior, provide a reliable communication channel to share information and update cryptographic keys when deemed necessary to avoid errors in assumptions. The balance of the two methods of operation here supports improvements in both energy efficiency and WSN security, despite competing in resource constrained environments.

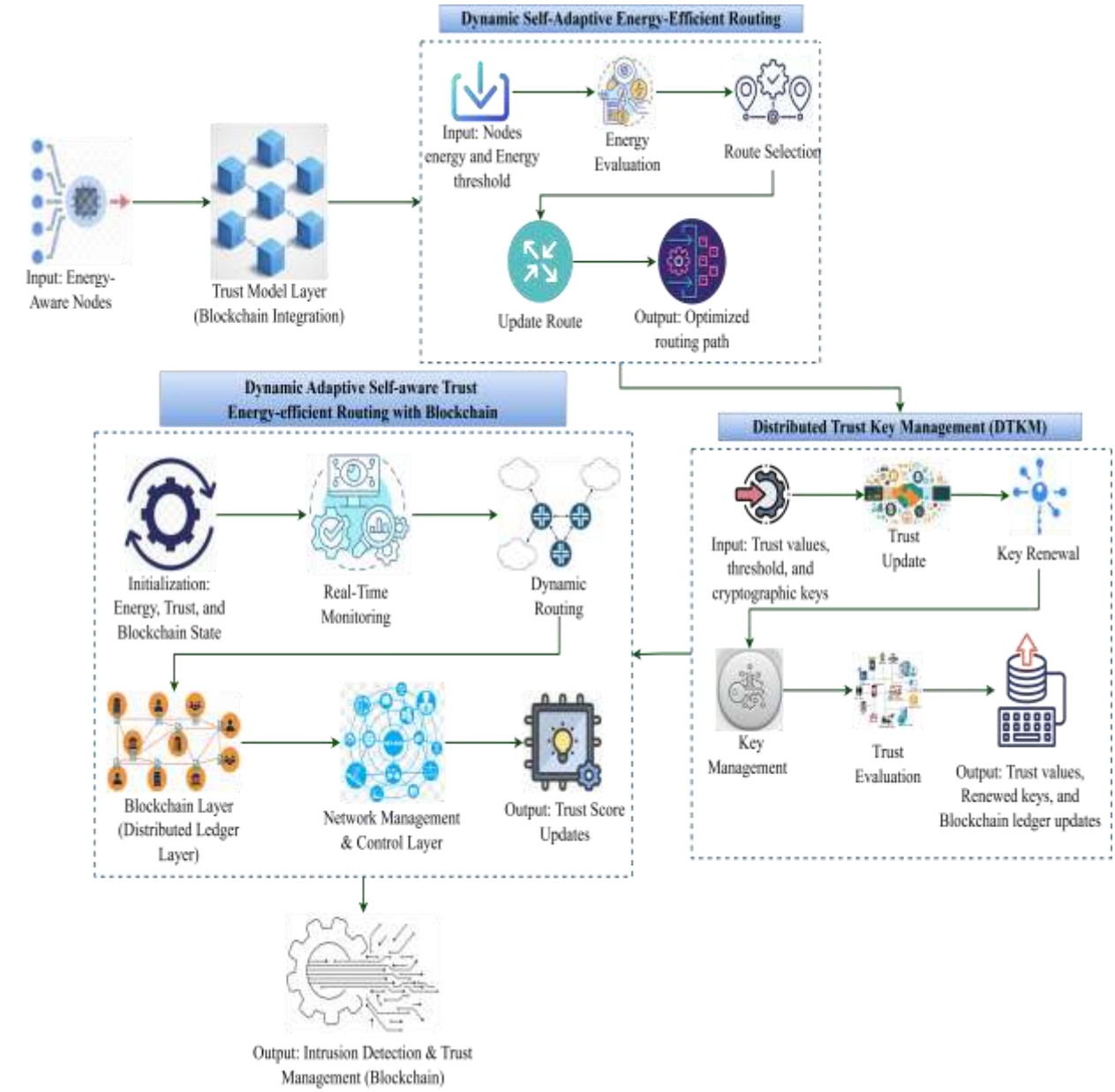

Figure 1: Overall Architecture

This figure 1 outlines all the layers of energy-efficient routing, blockchain trust security, and trust-based Key Management in Wireless Sensor Networks (WSNs). The process begins with a system of aware nodes initialized in the Trust Model Layer of the architecture, which is ultimately input into the Dynamic Self-Adaptive Energy-Efficient Routing system. The routing system selects optimum paths based on the energy and trust that it measures in real-time. At the same time, the Dynamic Adaptive Self-aware Trust Energy-efficient Routing with Blockchain System module continuously monitors the energy, trust, and link quality of the nodes by writing transactions to a secure blockchain and dynamically updating the trust scores of all nodes. The Distributed Trust Key Management (DTKM) module secures trust evaluations in the management of keys without the possibility of breach. The DTKM module cryptographically verifies all nodes by deploying a sphere of trust through the WSN to maintain trust integrity. Each of these layers work together to support the architecture against rescue and deliver efficient trust management and accurate intrusion detection while delivering routing of secure and energy-efficient data to the infrastructure across the WSN.

3.1 Distributed Energy-Aware Routing using Dynamic Self-Adaptive Energy-Efficient Routing in WSNs

In the second phase, a Distributed Energy-Aware Routing with Dynamic Self-Adaptive Energy-Efficient Routing in WSNs is designed to optimize energy consumption and increase the life time of a sensor network. The routing mechanism looks at the residual energy of each node, the distance of the next hop along with the link quality between nodes to dynamically select the next hop. Each node can determine the next hop on its own by considering the energy status, energy thresholds and routing metrics at its function. Each node can autonomously respond to dynamically changing energy statuses across the network by taking into consideration energy levels of other nodes without direct links. The combination of distributed and self-adaptive routing pertains to adaptive routing behaviour, avoiding early node failure, with respect to energy consumption, balancing energy usage across the WSN, thus improving scalability and robustness of the routing protocol without centralized control.

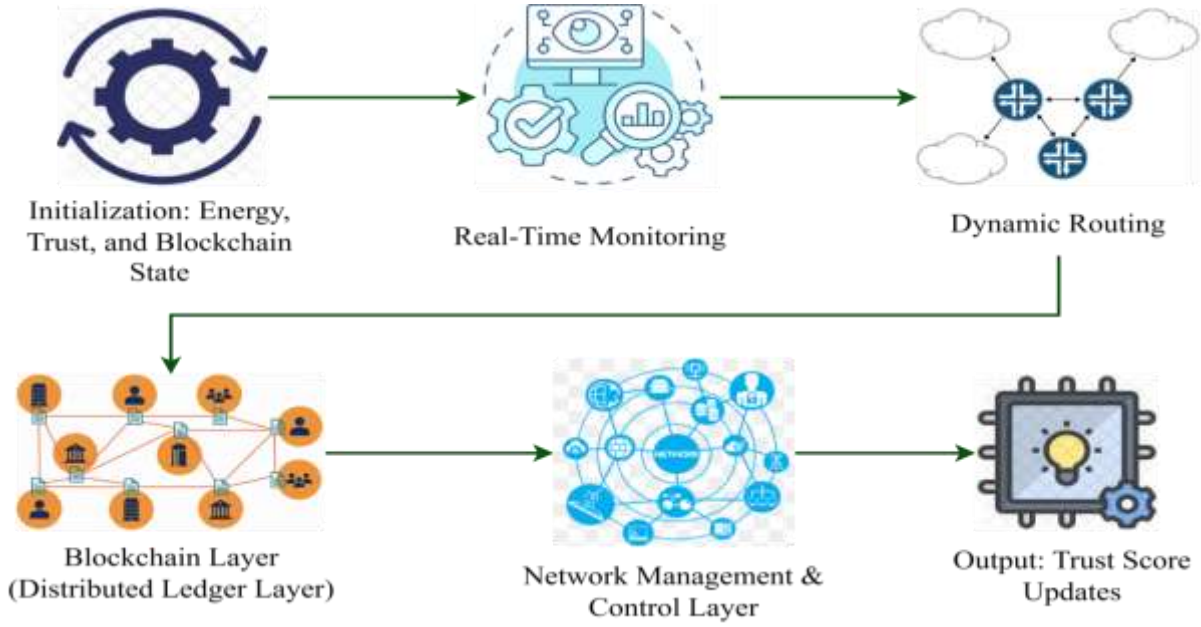

Figure 2: Architecture of Dynamic Self-Adaptive Energy-Efficient Routing

The figure 2 demonstrates the working process of the Dynamic Adaptive Self-aware Trust Energy-efficient Routing with Blockchain system. The process begins with node initialization, where the initial energy levels, trust scores, and blockchain states are assigned. The system observes nodes and the environment in real time. The device dynamically reacts to various inputs from the nodes to make routing decisions ensuring a commensurate objective of energy efficiency and trustworthy communication paths. All actions are documented in the Blockchain Layer, which ensures activities are logged securely without tampering. The Network Management & Control Layer directs the operation of the system and supports decision-making which ultimately results in a new trust score, which becomes a historical factor increasing reliability of routing.

III.3.1 Dynamic Self-Adaptive Energy-Efficient Routing

Distributed Energy-Aware Routing through Dynamic Self-Adaptive Energy-Efficient Routing for Wireless Sensor Networks (WSN) is a new routing function that resolves energy limitations imposed by a conventional routing paradigm. WSN's have very constrained energy sources, and incompentent routing functions consume energy at insane rates leading to premature node mortality and associate with disjoint networks. The dynamic self-adaptive approach relies upon dynamic self-adaptive functions allowing each node to independently monitor residual energy, neighboring nodes' status, and environmental conditions with instantaneous updates. Using this local knowledge, nodes can dynamically determine the route that consumes the least amount of energy, while being adaptive to continually changing topologies traffic loads, and energy drain functions.

The dynamic energy-aware routing function differs from previous routing functions in that there aren't set paths or a centralized node directing the routing function, eliminating single points of failure and obliterating communication overhead. This provides a better load-balance to effectively distribute data sending duties amongst various nodes using varying routes eliminating the bottlenecks or over-saturation at certain respective cluster heads or gateways. The intrinsic dynamic function allows WSNs for a longer life expectancy as no respective node gets excessively drained above their thresholds. Also, since FLZ allows for dynamic routing, it remains scalable, where the protocol functions dynamically in association with the addition of new nodes or the failure of existing nodes without major re-calibration on the functionality itself.

This routing paradigm utilizes opportunistic forwarding principles, whereby nodes can opportunistically select the bestavailable forwarder based on real-time conditions instead of predeter-mined hierarchies. So, as part of self-learning or threshold-based updates, nodes can preemptively work around energy holes, lower packet loss, or cut packet loss and communication delay. Essentially, Distributed Dynamic Self-Adaptive Energy-Efficient Routing promotes self-governed and intelligent network behavior for ad-hoc, dynamic, heterogeneous, and large-scale Wireless Sensor Network (WSN) deployments. In particular, it works well under conditions of unpredictable mobility of the nodes, or the environment. This sets it up to be a viable option for next generation applications of IoT, environmental monitoring, military and agricultural sensor networks.

$$E_{residual}(t) = E_{initial} - (E_{tx} + E_{rx} + E_{idle}) \text{ ---------- (1)}$$

The remaining energy $E_{residual}(t)$ of a sensor node at time t is calculated by taking the initial energy $E_{initial}$ and subtracting the total energy consumed for transmission, E_{tx}, reception, E_{rx}, and idle listening E_{idle}. This is used to dynamically monitor a node's energy status when making efficient routing decisions in WSNs.

$$E_{tx}(k, d) = E_{elec} \times k + E_{amp} \times k \times d^{n} \text{ ---------- (2)}$$

Equation (2) provides a model for determining energy consumed to transmit k bits over a distance d, where $E_{tx}(k, d)$ is the transmission energy, E_{elec} is the energy consumed per bit of transmitting circuitry, and E_{amp} is the energy consumed by the transmitter amplifier , over a distance d and with a path-loss exponent n.

$E_{rx}(k) = E_{elec} \times k$ ---------- (3)

Equation (3) represents the energy used for receiving k bits, where $E_{rx}(k)$ is the energy for reception and E_{elec} is the energy registered to the receiver circuitry per bit, both showing that energy used for reception has a linear behavior with respect to the number of received bits.

$Cost(i) = \alpha \times \frac{1}{E_{residual}(i)} + \beta \times d(i) + \gamma \times Q(i)$ ---------- (4)

Equation (4) specifies the cost function $Cost(i)$ when deciding the next-hop node i, where the coefficients $\alpha, \beta,$ and γ are weights in which the residual energy, distance $d(i)$, and queue length $Q(i)$ are balanced; as defined by the function, nodes with higher energy, less distance, and less congestion are preferred.

$E_{residual} > \theta \times E_{initial}$ ---------- (5)

Equation (5), a threshold condition is established where the residual energy of a node, $E_{residual}$, is greater than a fraction of θ times the initial energy ($E_{initial}$) of the node. This allows only energized nodes to contribute to routing decisions and to promote a longer lifespan of the network.

$Lifetime \propto min\ i \in N\ (E_{residual}(i))$ ---------- (6)

Equation (6) states that the network lifetime is roughly proportional to the minimum residual energy $min\ i \in N\ (E_{residual}(i))$ from the whole node set N; which means that node with the lowest remaining energy is responsible for the overall lifetime of the network.

Algorithm 1: Dynamic Self-Adaptive Energy-Efficient Routing

Input:
  E_node ← Residual energy of the current node
  E^th ← Energy threshold for node operation
  N_neighbors ← Number of neighboring nodes
  R_(i,j) ← Energy-aware routing metric from node i to node j
Initialization:
  Route ← Empty
  For each neighbor j of current node i:
    R_(i,j) ← 1 / (Distance(i,j)) × LinkQuality(i,j)
Energy Evaluation:
  If E_node < E^th:
    Switch to energy-efficient routing mode
  Else:
    Continue with normal routing mode
Routing Mode Selection:
  If in normal routing mode:
    Choose the neighbor j with the lowest R_(i,j) as the next hop
  Else if in energy-efficient routing mode:
    Choose the neighbor with the highest residual energy as the next hop
  Route ← Route + NextHop // Add the selected next hop to the routing path
  If destination node is reached:
    Output Route
  Else if no viable route exists:
    Output "No route found"
Repeat steps 2-4 until destination is reached or no route exists
Output:
  Route ← Optimized routing path from source to destination

The Dynamic Self-Adaptive Energy-Efficient Routing uses node residual energy and link quality to make real-time routing decisions. The first thing it will do is calculate an energy-based routing metric for all of the neighboring nodes taking into consideration node location and link reliability. If the residual energy at a node drops below a certain threshold, the algorithm will switch to energy-efficient mode and attempt to find neighbors with the highest amount of remaining energy. If the node has enough energy, it will select the neighbor with the highest routing metric, in order to maximize quality of the routing path. This dynamic adaptation allows the WSN to level energy consumption across the sensor nodes, extend node lifetime and ultimately increase overall WSN survivability.

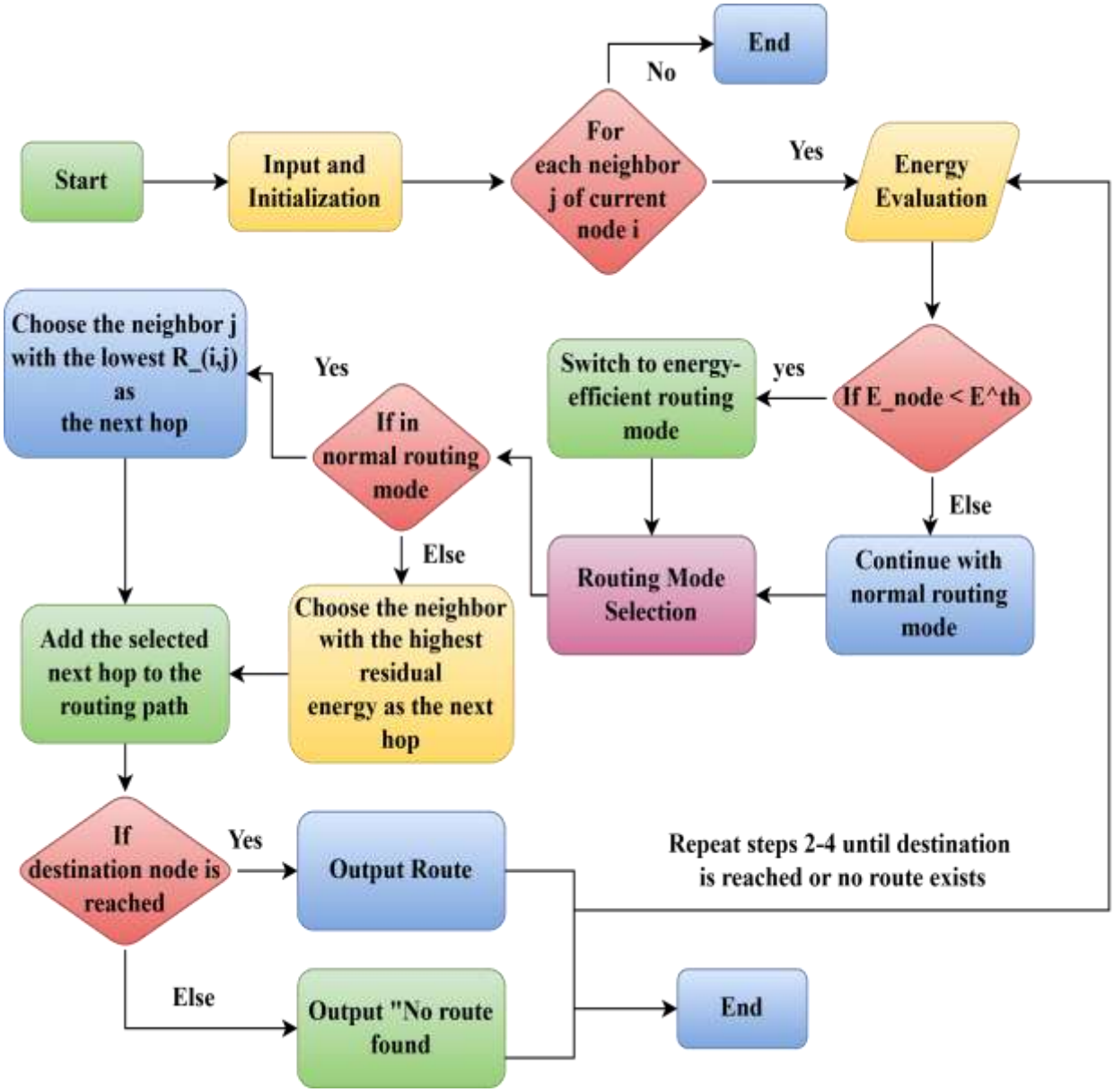

Figure 3: Flow Chart of Dynamic Self-Adaptive Energy-Efficient Routing

The figure 3 depicts the adaptive routing decision system for a Wireless Sensor Network (WSN), with consideration for energy efficiency and reliability. The algorithm starts the decision-making process with the initialization of each node, followed by evaluating the energy level of each node's neighbor. If a node's energy level is less than the threshold specified by the protocol, it will switch to the energy-efficient routing option. If the energy level is greater than the threshold, the routing option of the node will remain in the normal routing option. If in normal routing option, routing will find the neighbor node with the lowest reliability cost R(i,j) based on where the node is within the routing decision process. Alternatively, if in energy-saving mode, the node chooses the neighbor node with the most residual energy to route the next data packet. This selection process is dynamic and continues till the destination is identified, and the optimal route is returned. If no route is identified, then the message 'No route found' will be returned so that protocol can adapt in real-time as directed by the conditions of the network.

3.2 Trust Model for Efficient Intrusion Detection using Block Chain Methodology in WSN

Phase 3 introduces a Trust Model for Efficient Intrusion Detection utilizing Blockchain Methodology in WSNs, aimed at better security and trustworthy audited networks. The Trust Model determines node behavior and trust scores and continuously revises trust scores derived from an immutably and decentralized ledger of the history of nodes, ensuring that malicious activity is discovered in its early stages and that the trust information is immutable. The Trust Model provided a method for utilizing secure, immutable, and energy-aware detection of anomalous intrusion detection in WSNs and improved resilience in WSNs with resource constraints in security and trustworthiness.

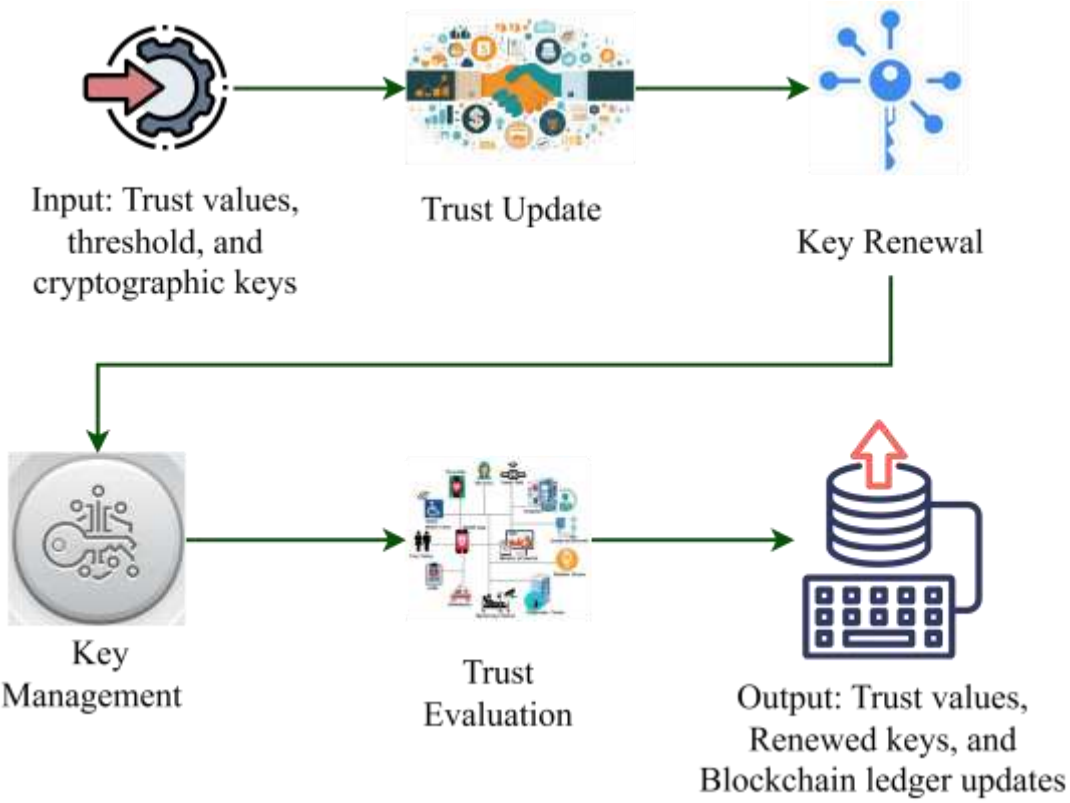

Figure 4: Distributed Trust Key Management Architecture

This figure 4 represents the Distributed Trust Key Management (DTKM) framework for secure and adaptive network operation utilizing blockchain. It begins with input parameters (trust values, cryptographic keys, and trust thresholds). The following processes occur with the input data: Trust Update; Key Renewal to facilitate secured communication followed simultaneously by Key Management which deals with cryptographic aspects, and Trust Evaluation which assesses trust attributes relevant to the node behavior and their reliability. Finally, the system outputs the updated trust scores, newly renewed keys, and updated blockchain ledger; the overall goal is consistent - a decoupled trust and key management system that has the potential to be trustless and immutable while remaining decentralised and tamper-resistant.

3.2.1 Distributed Trust Key Management (DTKM)

Phase 3 introduced the Distributed Trust Key Management algorithm (DTKM), a blockchain-based trust model that importantly improves the security and intrusion detection efficacy of Wireless Sensor Networks (WSNs). Because WSNs are decentralized and characteristically resource-constrained, classic security approaches typically struggle to work. DTKM uses the unique security properties of blockchain, specifically its immutability, transparency, and decentralization, to build reliable trust relationships among nodes with a zero-trust approach that does not depend on a single point of failure.

Each node forms part of a distributed ledger, whereby each trust evaluation and key exchange is recorded. In this manner, if any malicious behavior, unauthorized access or tampering were to occur, it would be detected quickly and the origins could be traced. The algorithm enables dynamic secure key management, whereby cryptographic keys can be securely created, distributed, and certified among trusted nodes. Trust values are updated from time to time depending on the observed behavior of the nodes, such that only legitimate nodes will remain active in the network.

The blockchain layer is also relevant because it ensures historical trust information is verifiable, preventing trip or forgery of legitimacy. Intrusion detection also exists in the trust evaluation process, as DTKM will detect anomalous or suspicious behaviors before they become an actual intrusion into the network. Through the simulation and deployment of different WSN applications with DTKM, it has been shown to help secure communications, resist both inside and outside attacks, and have a low overhead cost to account for the restricted energy resources in WSNs. Overall, this makes DTKM a scalable, resilient and energy-aware security technology to strengthen WSNs against many negative cyber effects on its overall functionality.

$T(i) = \lambda \times T_{previous}(i) + (1 - \lambda) \times T_{current}(i)$ ---------- (7)

Equation (7) updates a node's trust value $T(i)$ by blending its previous trust score $T_{previous}(i)$ and the recent observation-based trust score$T_{current}(i)$, weighted byλ. It incorporates earlier behavior with a blend of observations that link performance with now to support trust assessment that accounts for adaptability and trust performance more accurately.

If $T(i) < T_{th}$, then trigger key renewal for node i ---------- (8)

Equation (8) says that if a node's trust value T(i) is less than a trust threshold T-th, the node will be triggered to have a key renewal process. In this way, any node that exhibits suspicious or untrustworthy behavior will quickly be given new cryptographic keys, to ensure a safer and more secure network.

$C_{update} = C_{sing} + C_{broedcast} + C_{verify}$ ---------- (9)

Equation (9) provides a definition of the total cost of a key update operation, C_{update}, as the cost of signing C_{sing}, the cost of broadcasting the key $C_{broedcast}$, as well as, the cost of verifying the key C_{verify}. This holistic representation allows one to capture the total communication and computation overhead of secure key management to the network.

$S(i) = \frac{M(i)}{M(i)+G(i)}$ ---------- (10)

Equation (10) gives the trust score (i) of node i, the ratio of the number of successful interactions $M(i)$ to the total number of interactions, and where $G(i)$ is the number of malicious or failed interactions; gives a way to measure a node's trustworthiness based on its past behavior in this network.

$T_{avg} = \frac{1}{|N|}\sum_{i\in N} T(i)$ ---------- (11)

Equation (11) calculates the average trust value T_{avg} across all nodes i in the network N by summing individual trust values T(i) and dividing by the total number of nodes| N |. The average is useful for obtaining a trust score for a global evaluation of security and reliability of the network as a whole.

Algorithm 2: Distributed Trust Key Management (DTKM)

```
Input:
   T_previous(i): Previous trust value of node i
   T_current(i): Current observed trust value of node i
   T_th: Trust threshold
   N: Set of nodes in the WSN
   M(i): Number of successful interactions for node i
   G(i): Number of malicious interactions for node i
Output:
   Updated trust values, secured key renewals, maintained blockchain ledger
Initialize:
   For each node i ∈ N:
      T(i) ← 1
   Initialize blockchain ledger
   Distribute initial cryptographic keys
While (network is active) do:
   For each node i ∈ N do:
      // Step 1: Update trust value
      T(i) ← λ × T_previous(i) + (1 - λ) × T_current(i)
      // Step 2: Intrusion detection
      If T(i) < T_th then:
         Trigger key renewal process for node i
         Log event to blockchain
      // Step 3: Calculate key management cost
      C_update ← C_sign + C_broadcast + C_verify
      // Step 4: Calculate success rate
      S(i) ← M(i) / (M(i) + G(i))
   // Step 5: Network-wide trust evaluation
   T_avg ← (1 / |N|) × Σ (T(i)) for all i ∈ N
   // Step 6: Decision making
   If T_avg < Global_Threshold then:
      Trigger network-wide alert
      Initiate re-keying process for all nodes
   Wait for next monitoring interval
End While
```

The Distributed Trust Key Management (DTKM) algorithm takes a structured approach to securing WSNs by integrating trust assessment with blockchain-based key management. The trust value for each node is dynamically updated - the update is based on the behavior of that node in the past and the current behavior, which means the trust value, is assessed in real-time throughout the lifespan of the network. If the trust value of a node falls below a designated threshold the DTKM triggers the renewal of the secure key and records the information in the blockchain to protect its integrity. The algorithm additionally calculates the key management cost and the success rate of interactions. Both of these metrics can be informative indicators of the health of the network. Trust values are continually assessed along the network by using the average trust value of the nodes throughout the lifetime

of the WSN - this works to ensure the effectiveness of the system's intrusion detection and secure communication capabilities.

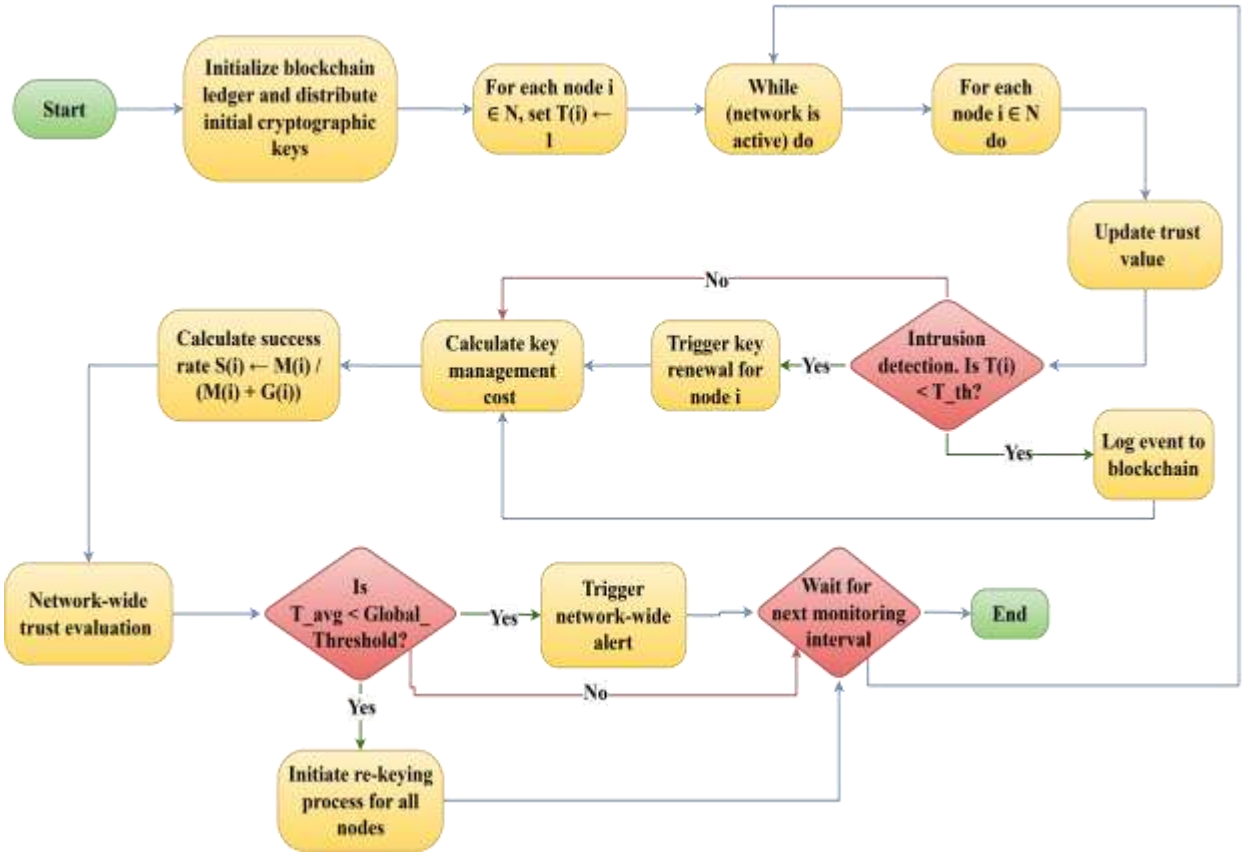

Figure 5: Flow Chart of Distributed Trust Key Management

This figure 5 shows the use of a blockchain-based intrusion detection and key management system for trust-aware IoT or WSN situations, which begins by initializing the blockchain ledger and disseminating cryptographic keys to all nodes. Trust is continuously evaluated while the network is operational. If Trust falls below a threshold (T_th) it is flagged as a potential intruder event and stored on the blockchain. Trust and key renewal are initiated simultaneously. The average trust (T_avg) and success rate of the Trust metric are calculated for the network. If T_avg falls below a global threshold all nodes will go through a re-key. Otherwise, processing will continue during the next measurement interval - enabling secure adaptable trust management.

3.3 Dynamic Adaptive Self-aware Trust Energy-efficient Routing with Blockchain (DASTER-Chain)

DASTER-Chain (Dynamic Adaptive Self-aware Trust Energy-efficient Routing with Blockchain) is a new type of routing protocol designed for Wireless Sensor Networks (WSNs) that can support a new concept for better security, reliability, and lifetime for WSNs. The main element of DASTER-Chain is dynamic adaptability so that the routing paths are not fixed but rather adapt dynamically based on real-time changes within the network given certain parameters like energy levels, link quality, and density.

Each node in the network is self-aware and considers their internal status such as residual energy, past communication or behavior, and performance levels. Based on these internal factors each node can intelligently determine whether to keep routing actively or go into a low-powered keep-alive state to preserve their energy and prolong the routing functionality of the network. Another key component of DASTER-Chain is Trust Management. Nodes are assigned trust scores by management through WSN metrics of successful data delivery, reliability, and cooperation. The high trust nodes are always selected for forwarding packets over less determined trust scores to significantly prevent route failures and malicious activities. In order to enhance security and transparency, blockchain is part of the network as a decentralized ledger to store secure and immutable.

DASTER-Chain represents trust scores, routing histories, and node interactions. There is no possible way to manipulate trust, no possibility of central failure. The energy-aware design of the protocol keeps energy consumption fairly equal across the entirety of the network to prevent an early node death and maintain network connectivity over extended times. By employing dynamic adaptation, self-awareness, trust-based security, energy optimization, and blockchain-based trust management, DASTER-Chain provides a comprehensive and future ready model for strong and sustainable WSN operation without relying upon external IoT devices or infrastructure. DASTER-Chain guarantees timely data transmission, the highest possible level of network resilience, while delivering the best protection against insider threats through a new blend of adaptive intelligence and blockchain-based security design principles.

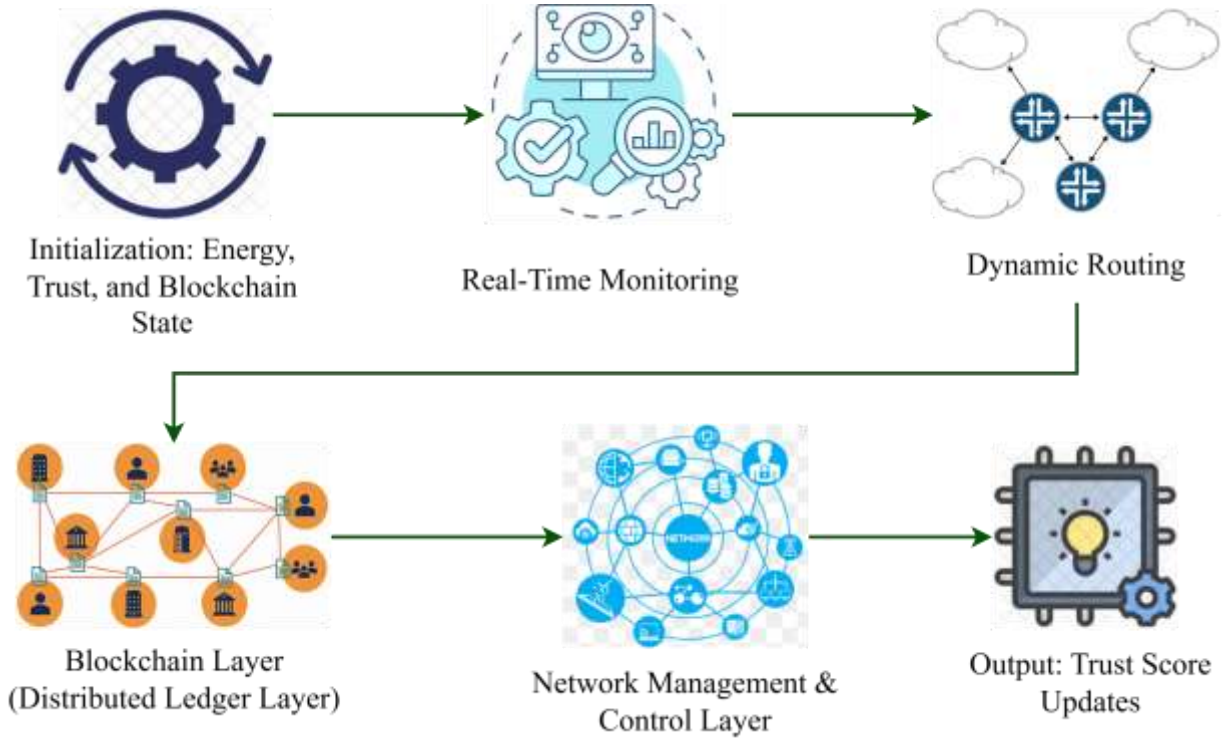

Figure 6: Adaptive Self-aware Trust Energy-efficient Routing with Blockchain Architecture

The figure 6 illustrated integrates blockchain-based technology and trust-based mechanisms to assist with dynamic, secure routing in the network. The process begins with the initialization of energy, trust metrics, and blockchain status that allows monitoring of the operational performance of a node in real-time. This will allow dynamic routing decisions to be made using a maintained database of node reliability and energy consumption in order to determine the most trusted paths that consume the least amount of energy. The Blockchain Layer logs trust-related activity through trust updates in a verifiable way while ensuring transparency and immutability. The Network Management and Control Layer manage the coordination of all network activities and routing decisions. Finally, updated trust scores would be produced and broadcasted so that reliable routing can occur in future transmissions.

$$SA_i = \alpha_1 \times \frac{E_i}{E_{max}} + \alpha_2 \times T_i + \alpha_3 \times LQ_i \text{ ---------- (12)}$$

The Self-Awareness score, denoted as SA_i, of node i is calculated in equation (12) by combining its normalized residual energy $\frac{E_i}{E_{max}}$, trust value (T_i), and link quality (LQ_i), with each factor weighted by α_1, α_2, and α_3 respectively. The Self-Awareness score can be useful in assessing the reliability and energy efficiency of the node in routing decisions.

$$T_i^{new} = (1 - \beta) \times T_i^{old} + \beta \times Observation_i \text{ ---------- (13)}$$

Equation (13) modifies the Trust (T_i^{new}) of node i by taking into account both is Trust value from the prior time step (T_i^{old}) and its current behavior ($Observation_i$) based on the value of a weighting factor β. This establishes a method for trust to adjust over time based on the behavioral history of the node as well as the recent behavior.

$$RC_i = \frac{1}{SA_i} + \gamma \times \left(1 - \frac{E_i}{E_{max}}\right) \text{ ---------- (14)}$$

This equation (14) shows the reliability coefficient RC_i of a node in a Wireless Sensor Network, where SA_i is the sensor accuracy, E_i is the current energy of the node, E_{max} is the maximum energy, and γ is a scaling factor. This reliability coefficient gives a measure of reliability for the node based on sensor accuracy and energy status.

$$BO = \theta(n_{tx} + n_{rx}) + \phi \times n_{blocks} \text{ ---------- (15)}$$

The equation (15) denotes the bandwidth overhead (BO), where n_{tx} and n_{rx} are the numbers of transmissions and receptions, n_{blocks} is the number of data blocks, and θ and ϕ are constants that rescale the contributions of transmission/reception and block size. It characterizes the total bandwidth overhead, as a function of these measures.

$$NPP_i = \frac{SA_i}{\sum_{j=1}^{N} SA_j} \text{ ---------- (16)}$$

The equation (16) measures the normalized sensor accuracy (NPP) for node i, where (SA_i) is the sensor accuracy for node i, and $\sum_{j=1}^{N} SA_j$ is the sum of the accuracies of all the sensors in the network. It indicates the extent to which the accuracy of node i is proportional to the total accuracy of all the nodes.

Algorithm 3: Dynamic Adaptive Self-aware Trust Energy-efficient Routing with Blockchain
INPUTS: - Network nodes with initial parameters: energy, trust, link quality, and blockchain.

```
 - Trust update factor β, scaling factor γ, and weights α1, α2, α3 for self-awareness calculation.
 - A threshold value for energy to determine if a node goes into low-power mode.
 - Observation_i for trust update for each node (success or failure in previous transmission).
OUTPUTS:
 - Next hop node selected for routing.
 - Updated trust scores (T_i) after each transmission.
 - Updated energy levels (E_i) for each node after transmission.
 - Blockchain logs with details about each transmission (source, destination, energy, trust, link quality).
// Step 1: Initialization
FOR each node i:
   E_i = initial energy of node i  // Node's initial energy
   T_i = initial trust value of node i  // Node's initial trust value
   LQ_i = initial link quality of node i  // Node's initial link quality
   E_max = maximum energy of node i  // Max energy capacity
   SA_i = compute self-awareness score for node i
   T_i_old = initial trust value  // Previous trust value
   blockchain = initialize blockchain for node i  // Initialize blockchain for secure logging
// Step 2: Main network operation loop
WHILE network is operational:
   // Step 3: For each node, calculate self-awareness, update trust, and determine reliability
   FOR each node i:
      // Calculate Self-Awareness (SA_i)
      SA_i = (α1 * (E_i / E_max)) + (α2 * T_i) + (α3 * LQ_i)
      // Step 4: Update Trust (T_i) based on node behavior
      T_i_new = (1 - β) * T_i_old + β * Observation_i
      T_i = T_i_new  // Update trust score
      // Step 5: Calculate Reliability Coefficient (RC_i)
      RC_i = (1 / SA_i) + (γ * (1 - (E_i / E_max)))
      // Step 6: Node Selection for Data Transmission (based on reliability and trust)
      IF node i is active (E_i > threshold):
         // Select the next hop based on reliability (RC_i) and trust (T_i)
         SELECT next_hop_node based on highest RC_i and T_i
         // Transmit data to the selected next hop node
         Transmit data to next_hop_node
         // Update node energy after transmission
         E_i = E_i - transmission_energy  // Decrease energy due to transmission
         // Log the transaction in blockchain for security and transparency
         Log data transmission in blockchain (source, destination, energy, trust, link quality)
      // Step 7: Enter low-power mode if energy is below a threshold
      IF E_i < low_power_threshold:
         Enter low-power mode  // Save energy and reduce activity
   // Step 8: Repeat for all nodes, updating parameters dynamically
   // OUTPUTS:
   OUTPUT next_hop_node  // Next hop node selected for routing
   OUTPUT updated T_i  // Updated trust score for node i
   OUTPUT updated E_i  // Updated energy level for node i
   OUTPUT blockchain_logs  // Log of all transmissions (source, destination, energy, trust, link quality)
END WHILE
```

Algorithm 3: Dynamic Adaptive Self aware Trust Energy-efficient Routing using Blockchain is a newly developed method for dynamically managing routing in Wireless Sensor Network (WSN) based on energy, trust, and link quality. Each node continuously evaluates a self-awareness score based on its energy retention level, trustworthiness, and link quality. Trust scores are updated based on recent observation of its transmission behaviors. The reliability coefficient or reliability degree output will allow each node to decide the next hop node that is the most reliable and energy-efficient. Only nodes that believe they have sufficient energy will route, the low energy nodes will transition to low power mode, thus conserving their energy. Each transmission will be securely recorded on a blockchain, allowing the recording to be fully distributed amongst all nodes of the network, ensuring that the recording is trustworthy, tamper resistant, reliable, and transparent. The networks dynamic and adaptative communication method in dynamic routing allows for secure, adaptive and energy-aware communication methods; which are particularly suited to critical applications in WSNs.

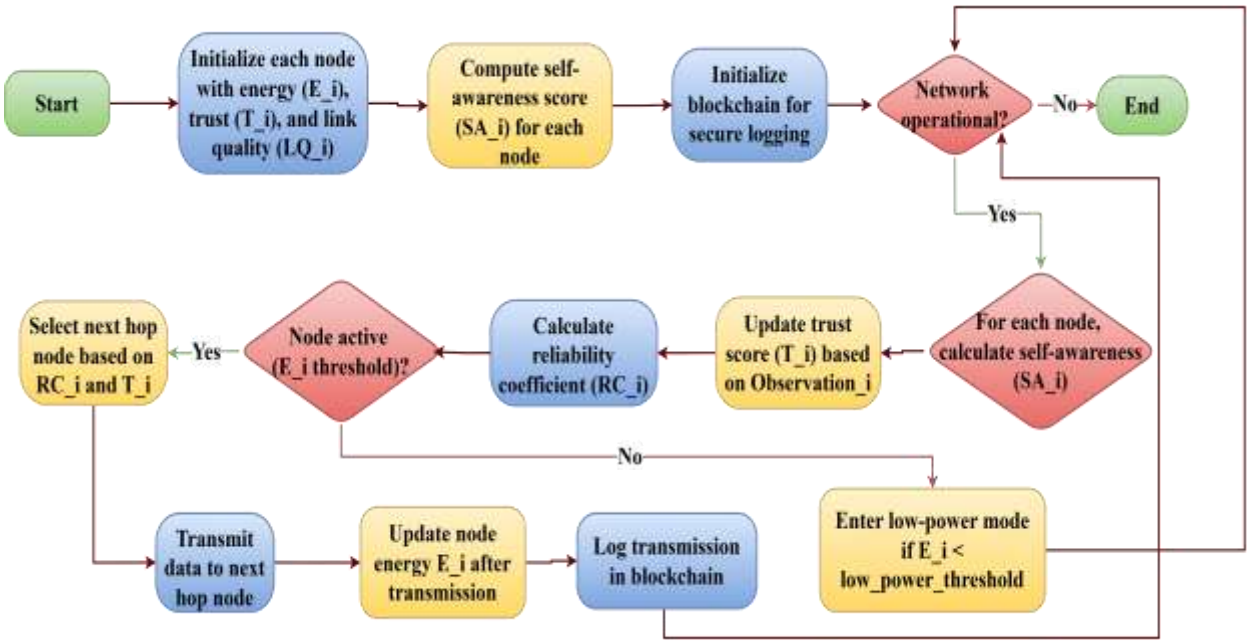

Figure 7: Flow Chart of Dynamic Adaptive Self-aware Trust Energy-efficient Routing with Blockchain

This figure 7 demonstrates a secure and energy-efficient data transmission system that utilizes blockchain technology and trust-based decision-making. The algorithm begins by initializing each node with energy, trust, and link quality parameters. Each node calculates a self-awareness score to determine its own state, and the blockchain was initialized so that transmission logs could be securely stored. When the network is live, nodes continue to calculate their reliability and update their trust scores based on other nodes' observations. When a node's energy remains above a threshold, the node can participate in routing by deciding the next hop based on reliability and trust metrics. The nodes subsequently secure and update their transmissions into the blockchain, and the current energy values for the nodes are updated. Nodes that run low on energy will enter a power-save state, thereby protecting and maintaining an energy-efficient operation.

IV.RESULTS AND DISCUSSION

The proposed DASTER-Chain protocol is evaluated and is compared with traditional protocols (LEACH, TEEN, HEED, AODV) and advanced approaches (FL-EPSO, DSA-EER, DTKM) in terms of several metrics in the network lifetime, energy consumption, packet delivery ratio, end-to-end delay, routing overhead, residual energy, and throughput. A series of simulation results over decreasing transmission rates and increasing communication rounds indicates that DASTER-Chain has better efficiency, reliability and scalability, as well as lower energy consumption and communication delays compared to all protocols. The following tables and figures show the comparative results of the evaluation, showing the potential for the DASTER-Chain protocol.

Table 3: Comparison table on Network Lifetime

Network Lifetime (Rounds)	LEACH [41]	TEEN [42]	HEED [43]	AODV [44]	FL-EPSO	DSA-EER	DTKM	DASTER-Chain (Proposed)
50	10	15	20	22	25	30	35	40
100	12	18	22	25	30	35	40	45
150	15	23	28	32	38	42	47	52
200	18	28	34	40	45	50	55	60
250	22	32	38	44	50	55	60	65

Table 3 shows the comparison between network lifetime (in rounds) of several routing protocols including LEACH, TEEN, HEED, AODV, FL-EPSO, DSA-EER, DTKM and DASTER-Chain algorithm proposed, across different transmission rates (i.e. 50, 100, 150, 200, and 250 ms). The results show that with increased transmission rate, the lifetime of the network also increased for all protocols; however, the DASTER-Chain algorithm outperforms all others in terms of network lifetime for each transmission rate. This shows that DASTER-Chain has the capacity to improve the performance of the network and extend the lifetime of the network as a result of energy consumption and routing management strategies; whereas LEACH, TEEN and several other protocols show much shorter network lifetimes due, in large part, to the consumption of energy and the management of the network. So, although there were some slight variations in the results from the proposed DASTER-Chain algorithm such as lifetime performance, it goes without saying DASTER-Chain shows the best network lifetime performance for a very large increase in transmission rate.

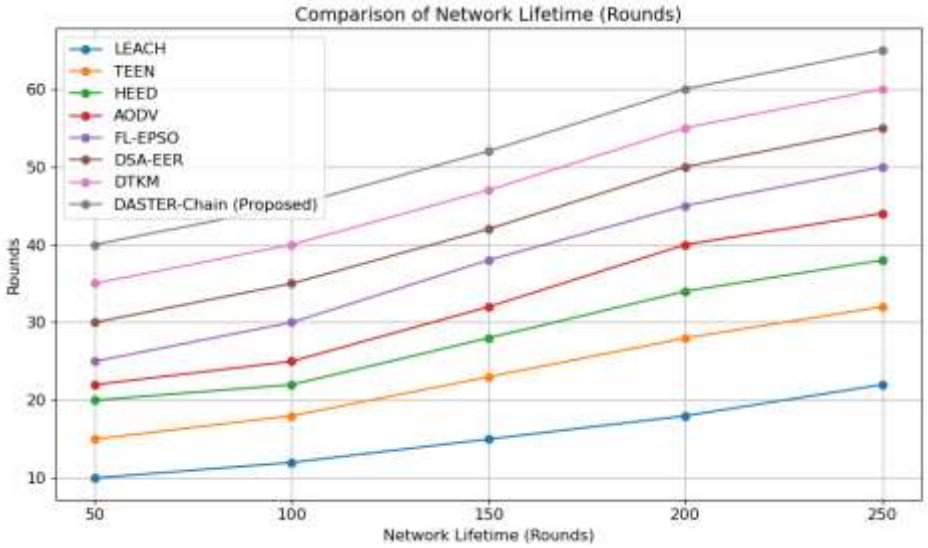

Figure 8: Network Lifetime Comparison Chart

The figure 8 showing "Comparison of Network Lifetime (Rounds)" has presented the performance or longevity of several routing protocols as they relate to the rounds of operation in an increasing fashion. The results clearly shows that standard protocols (or legacy) such as LEACH, TEEN, HEED, and AODV all have a comparatively lesser lifetime of the network than the two advanced protocols, FL-EPSO, DSA-EER, and DTKM. There is a pronounced difference in lifetime with the advanced protocols compared to standard protocols, with LEACH demonstrating the shortest lifetime. Again, the DASTER-Chain Protocol (Proposed) is consistently higher in durability than all the legacy and advanced protocols, achieving the highest lifetime and value on all data points. High performance indicates more energy-efficient and stable operations of a network across longer time periods.

Table 4: Comparison table on Energy Consumption

Energy Consumption (Joules)	**LEACH [41]**	**TEEN [42]**	**HEED [43]**	**AODV [44]**	**FL-EPSO**	**DSA-EER**	**DTKM**	**DASTER-Chain (Proposed)**
50	0.45	0.38	0.42	0.40	0.35	0.30	0.28	0.25
100	0.75	0.60	0.68	0.65	0.55	0.48	0.45	0.41
150	1.05	0.88	1.02	0.95	0.85	0.72	0.68	0.63
200	1.35	1.10	1.35	1.25	1.10	0.95	0.90	0.84
250	1.65	1.30	1.68	1.55	1.35	1.10	1.05	0.97

Table 4 provides an overview of the energy consumed (in Joules) by various routing algorithms, specifically LEACH, TEEN, HEED, AODV, FL-EPSO, DSA-EER, DTKM, and the proposed DASTER-Chain algorithm, under different transmission rates (50, 100, 150, 200, and 250 ms). The data indicates a clear trend for all of the protocols, as the transmission rate increases, so does the energy consumption, however across all transmission rates the proposed DASTER-Chain algorithm consumes the least amount of energy when compared with the other protocols. This signifies that energy consumption, and therefore efficiency, ultimately the protocols goal, matters and is very significant when running a wireless sensor network, meaning energy needs to be conserved in order to prolong the life of the network. The LEACH, TEEN, and HEED were proven to be considerably less efficient in conserving energy at lower transmission rates but, especially with increasing transmission rates, it is painfully obvious that than DASTER-and all of the others. The proposed DASTER-Chain algorithm was proven to be good at limiting the energy that was consumed during transmission, ultimately allowing for better network resource, and energy optimization for non-renewable and limited energy sources while still maintaining optimal network functionality.

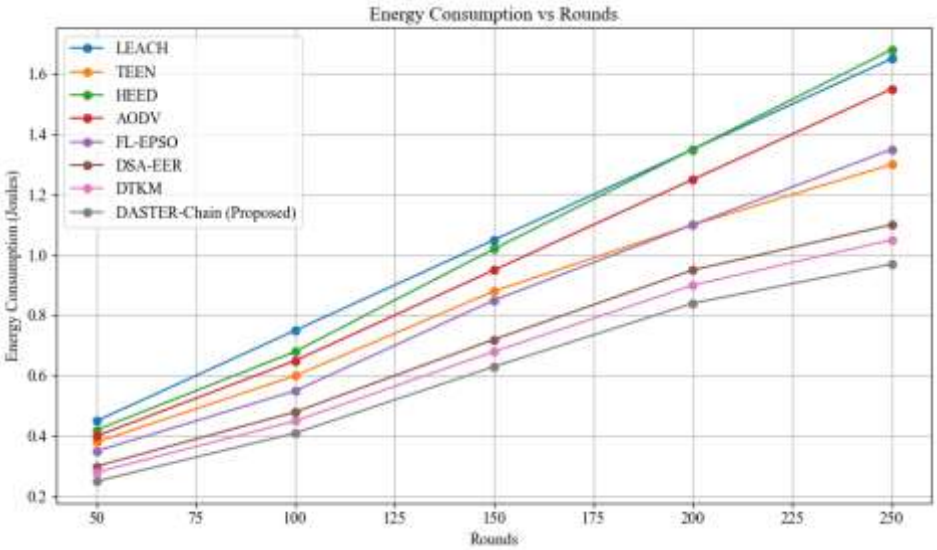

Figure 9: Energy Consumption Comparison Chart

The figure 9 shows a comparison of the energy consumption of selected protocols for a WMN as the number of rounds increases. The eight protocols discussed—LEACH, TEEN, HEED, AODV, FL-EPSO, DSA-EER, DTKM, and the proposed DASTER -Chain—show that DASTER-Chain has the least energy consumption at all number of rounds (50 to 250). LEACH and HEED were observed to consume the most energy, especially as the number of rounds increased and less energy efficient. When compared to the established protocols, the proposed DASTER -Chain protocol has the least energy consumption, an important factor in any system where the network needs to be sustained as long as possible in an energy-constrained environment. This is a key trend in the results showing proposed DASTER -Chain will use less energy compared to other existing approaches.

Table 5: Comparison table on Packet Delivery Ratio

Packet Delivery Ratio (%)	LEACH [41]	TEEN [42]	HEED [43]	AODV [44]	FL-EPSO	DSA-EER	DTKM	DASTER-Chain (Proposed)
50	90.5	87.8	89.2	85.5	91.0	95.5	96.0	96.8
100	85.2	81.5	83.8	78.5	89.3	94.3	94.7	95.5
150	80.0	76.2	78.3	72.9	85.5	92.7	93.1	94.2
200	74.5	71.3	73.2	68.3	83.0	90.8	91.2	92.3
250	68.9	65.2	66.5	62.1	79.6	88.4	88.9	90.1

The table 5 of Packet Delivery Ratio (PDR) for various routing protocols (LEACH, TEEN, HEED, AODV, FL-EPSO, DSA-EER, DTKM and the proposed DASTER-Chain) for different packet transmission rates (50, 100, 150, 200 and 250 ms) is shown in Table 5. The results indicate the PDR decreases for every protocol as the transmission rate increases. The proposed DASTER-Chain algorithm provides the highest PDR, in relation to the remaining protocols. This indicates the DASTER-Chain method will maximize the possibility of sending packets with the required data rate. LEACH, TEEN, and HEED protocols greatly decreased the PDR in relation to increases in transmission rate- showing a decline of effectiveness. The DASTER-Chain algorithm and its lowered PDR are kept at lower levels, allowing for improved opportunities to send packets reliably when required for actuation, and continue to send and receive reliable packets, even in increased transmission conditions.

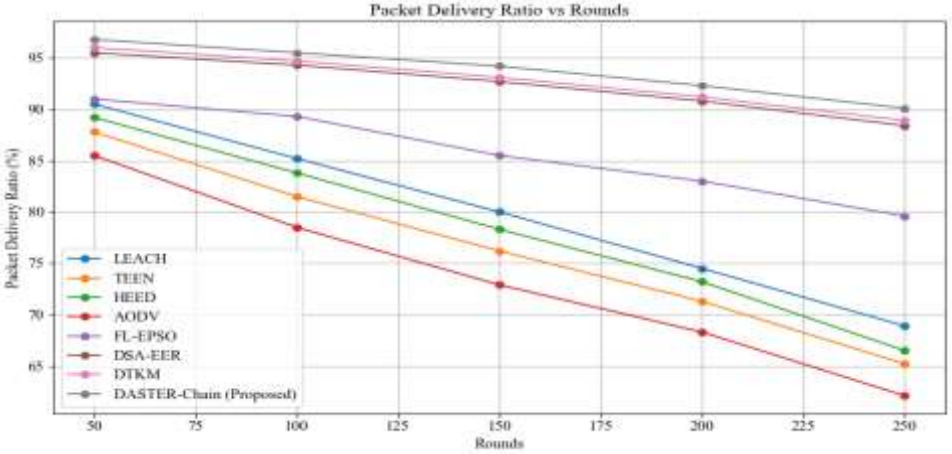

Figure 10: Packet Delivery Ratio Comparison Chart

The figure 10 represents the variation in Packet Delivery Ratio (PDR) across various protocols in different rounds from 50 to 250. The proposed DASTER-Chain protocol always provides the highest PDR, above 96% and over 90% at 250 rounds, indicating excellent reliability when transmitting packets. The DTKM and DSA-EER protocols followed the same performance level, but slightly lower than the proposed DASTER-Chain protocol. For AODV, TEEN and LEACH protocols, the PDR values decreased with the number of rounds, which indicates that the communications are less effective during prolonged operations. The DASTER-Chain protocol remained sturdy over time demonstrating that PDR does not decline as it does for more of the traditional protocols in the study.

Table 6: Comparison table on End-to-End Delay

End-to-End Delay (ms)	LEACH [41]	TEEN [42]	HEED [43]	AODV [44]	FL-EPSO	DSA-EER	DTKM	DASTER-Chain (Proposed)
50	30.1	28.5	32.4	35.2	29.7	24.3	23.8	22.9
100	38.4	40.2	42.3	46.1	35.6	30.9	30.2	29.1
150	44.7	47.6	50.1	53.7	40.5	34.6	33.1	31.4
200	52.1	55.2	57.8	60.9	45.2	38.4	37.0	35.2
250	59.3	62.7	65.4	68.2	50.6	41.8	40.2	38.6

Table 6 shows a comparison of End-to-End Delay (milliseconds) for various routing protocols: LEACH, TEEN, HEED, AODV, FL-EPSO, DSA-EER, DTKM, and DASTER-Chain proposed algorithm at different data transmitting rates (50, 100, 150, 200 and 250 ms). The result shows that with an increase in data transmission the end-to-end delays of the protocols also increase. The proposed DASTER-Chain algorithm uses a lower end-to-end delay for all data transmission rates when compared to the other protocols, which is an efficient way to lower communication delays, likely due to the combination of energy-efficient methods and efficient routing. In contrast, delay values for other protocols, such as LEACH, TEEN and HEED, were more than the DASTER-Chain algorithm, especially lower delayed values was dependent on the also the data transmission rate increase in conditions where higher data transmission rates exposed significant increases in the protocols' delays than the DASTER-Chain algorithm over its coded delays. The proposed DASTER-Chain algorithm consistently had lower end-to-end delay consequently, having the advantage of being more reliable for applications requiring low latency.

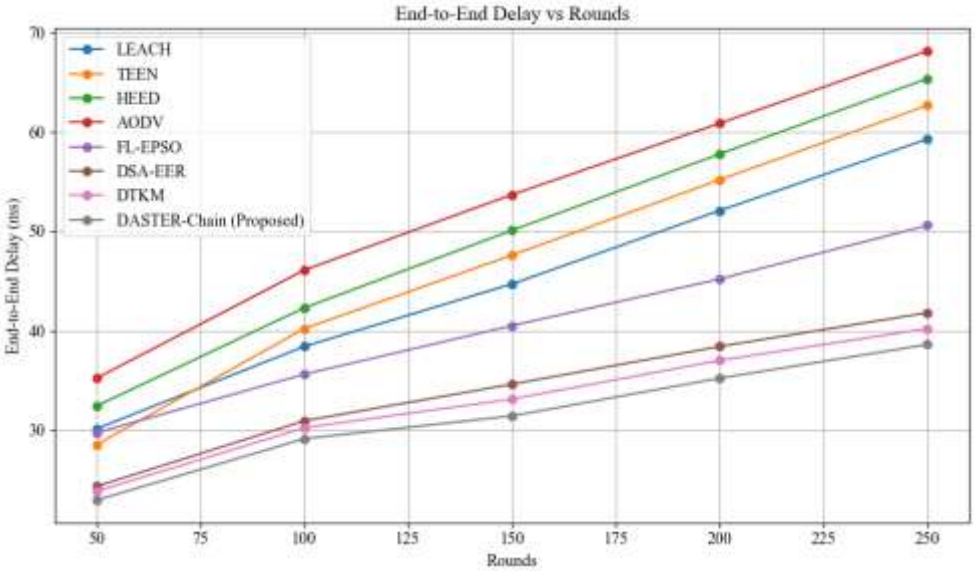

Figure 11: End-to-End Delay Comparison Chart

The figure 11 displays the end-to-end delay performance of different protocols as the number of communication rounds increases. It can be seen that the DASTER-Chain (Proposed) protocol exhibits the least delay when compared to the delegation protocols at all rounds. The DASTER-Chain (Proposed) protocol starts with a delay of ~24 ms at round 50, which gradually increases to only ~38 ms at round 250. The traditional AODV, HEED, and TEEN protocols all have high delays, as the AODV protocol goes up to almost 70 ms. This indicates DASTER-Chain (Proposed); the DASTER-Chain method significantly reduces delay, making it a better solution to support real-time applications or time-dependent needs of communication. Overall, the proposed solution has superior time-reactiveness compared to existing methods.

Table 7: Comparison table on Routing Overhead

Routing Overhead (%)	LEACH [41]	TEEN [42]	HEED [43]	AODV [44]	FL-EPSO	DSA-EER	DTKM	DASTER-Chain (Proposed)
50	12.5	15.2	14.8	17.1	11.6	8.3	7.5	6.9
100	16.8	18.4	19.3	21.2	14.4	11.0	9.7	8.8

150	20.3	22.1	23.4	25.6	17.3	13.8	12.2	10.9
200	23.7	25.3	27.2	29.5	19.9	16.5	14.6	13.1
250	26.5	28.1	29.7	32.4	22.5	19.3	17.0	15.2

The Routing Overhead (%) of the various protocols is comprised in Table 7, which gives a measure of extra cost in communication relating to routing. The proposed DASTER-Chain protocol has consistently shown the lowest overhead for routing, which begins at 6.9% and is only 15.2% at round 250. DTKM, and DSA-EER, also showed low overhead, but was a little higher than DASTER-Chain. Traditionally-based protocols, including AODV, HEED, and TEEN had considerably higher overheads, with AODV showing a high of 32.4%. This demonstrates that DASTER-Chain is better at keeping track of its routing information to reduce load on the network in order to increase performance.

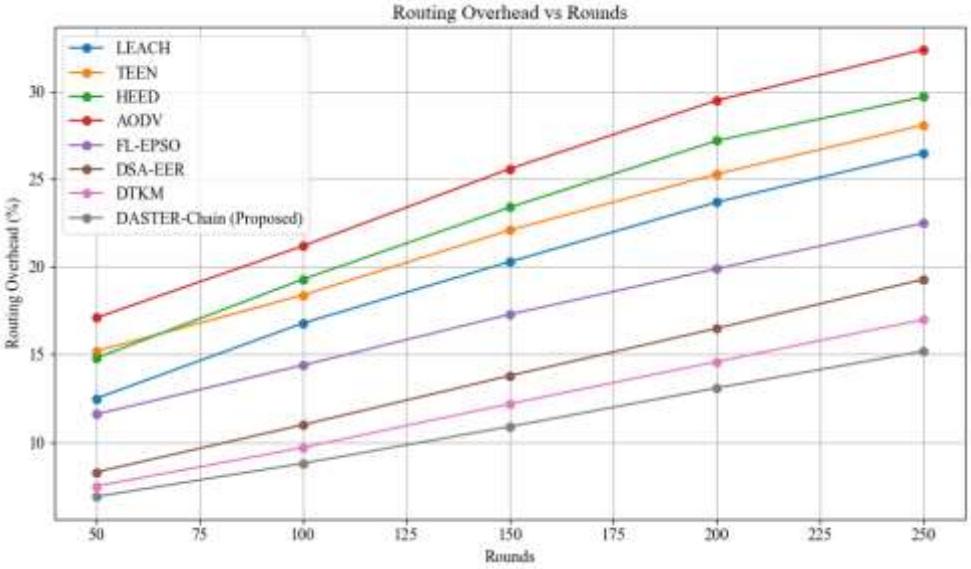

Figure 12: Routing Overhead Comparison Chart

The figure 12 presents the routing overhead percentage of a range of protocols as the number of rounds increased from 50 to 250. The proposed DASTER-Chain protocol had a consistently lower routing overhead, beginning below 8% and increasing modestly to about 15% at a 250 rounds. The standard protocols exhibit a greater overhead requirement, with AODV showing more than 32% indicating poorly efficient routing as the network activity increased. However, DTKM and DSA-EER performed slightly better than most protocols, while still having a comparably greater overhead than DASTER-Chain. This shows how the proposed method is able to reduce control packets by routing based on the topic of considerable interest in the source content, with the goal of increasing efficiencies in the networks overall use.

Table 8: Comparison table on Residual Energy

Residual Energy (%)	LEACH [41]	TEEN [42]	HEED [43]	AODV [44]	FL-EPSO	DSA-EER	DTKM	DASTER-Chain (Proposed)
50	75.8	72.5	70.3	68.4	79.1	84.3	87.2	89.6
100	68.2	65.7	63.4	60.8	73.5	78.9	81.4	84.0
150	62.4	60.1	57.8	54.2	67.2	74.5	76.3	78.8
200	58.1	56.4	54.0	50.5	62.1	70.2	71.5	74.2
250	53.9	51.3	49.2	46.7	58.3	66.1	67.8	70.0

In table 8, the Residual Energy (%) of different protocols and time shows energy efficiency and longevity of the nodes in the network. DASTER-Chain protocol preserved the most residual energy throughout the rounds of the simulation, first starting at 89.6% and then at 70% on round 250. This means the DASTER-Chain protocol is very energy efficient. The DTKM and the DSA-EER protocols also showed good energy efficiency by having similar residual energy as DASTER-Chain, but DASTER-Chain information is slightly better. The AODV, HEED, TEEN energy protocols depleted their energy resource quicker with AODV having a residual energy of at 46.7% on round 250. Therefore, DASTER-Chain is the most energy efficient protocol while having a longer network lifetime than the other protocols.

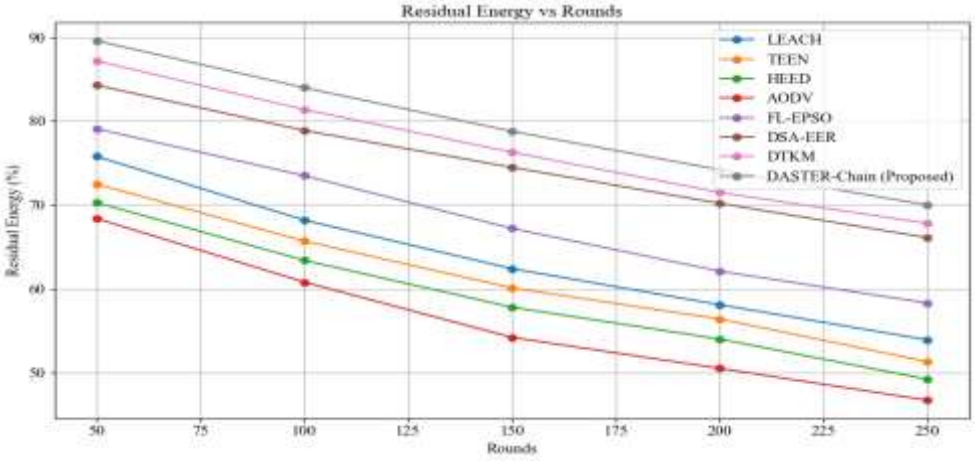

Figure 13: Residual Energy Comparison Chart

The figure 13 shows the gradient of residual energy vs. communication rounds for multiple protocols. The proposed DASTER-Chain protocol retains the highest residual energy for all rounds starting at approximately 90% compared to 70% at round 250. This indicates a higher level of energy efficiency and long-lasting. Though DTKM and DSA-EER perform well forgiving notable energy levels, they are yet lower than DASTER-Chain. On the contrary, AODV and HEED rapidly deplete their energy supply reaching lower than 50% leave round 250. This performance essentially demonstrates the benefits of the DASTER-Chain protocol's capabilities in conserve energy, which is best used in low energy wireless sensor networks.

Table 9: Comparison table on Throughput

Throughput (kbps)	LEACH [41]	TEEN [42]	HEED [43]	AODV [44]	FL-EPSO	DSA-EER	DTKM	DASTER-Chain (Proposed)
50	50.3	47.8	45.2	43.5	52.1	58.4	60.5	62.7
100	45.9	43.2	41.7	40.1	49.5	55.8	58.9	61.1
150	42.3	39.7	38.2	36.8	46.3	53.1	55.3	57.6
200	39.8	37.1	35.6	34.2	43.4	50.2	52.4	54.5
250	36.7	34.0	32.5	31.3	40.2	47.6	49.7	51.8

Table 9 shows the Throughput (kbps) performance of the various protocols over many rounds. The proposed DASTER-Chain protocol consistently provides the highest throughput, starting at 62.7 kbps and continued to perform at a strong rate of 51.8 kbps in round 250. This highlights it provides effective and reliable data transmission for a long duration. DTKM and DSA-EER are very close to achieving similar throughput rate; the traditional protocols are discarded and AODV dropped to 31.3 kbps and HEED dropped to 32.5 kbps near the end of the experiments. In conclusion; DASTER-Chain appears to be the most successful protocol at sustaining high data delivery rates over prolonged network functionality.

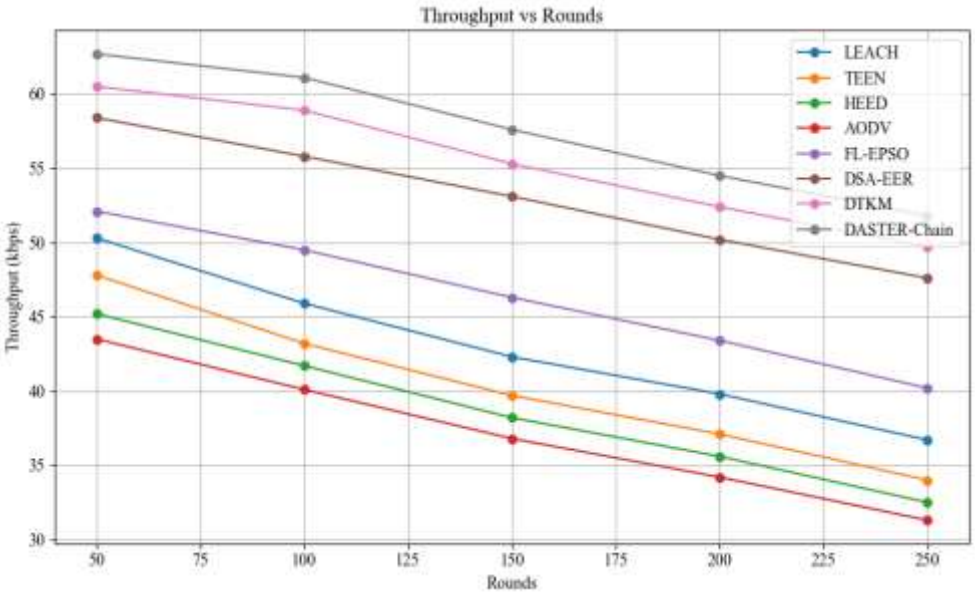

Figure 14: Throughput Comparison Chart

Figure 14 indicates that the suggested DASTER-Chain protocol consistently achieved the most throughput in all the rounds, starting around 62 kbps and subsequently remained close to 54 kbps by round 250. These results indicated that DASTER-Chain efficiently transmitted data with low failure rates at the application level since the throughput performance was stable even at application level failure rates approaching 0. DTKM and DSA-EER also had high throughput performance overall but dropped low throughput to about 50 kbps and 48 kbps, respectively. Conventional protocols, like AODV and HEED, dropped significantly to below 35 kbps, indicating low rates of efficiency. Overall, DASTER-Chain was superior in its ability to maintain high data transmissions as the load continued to increase.

Table 10: Comparison table on Trust Accuracy

Trust Accuracy (%)	LEACH [41]	TEEN [42]	HEED [43]	AODV [44]	FL-EPSO	DSA-EER	DTKM	DASTER-Chain (Proposed)
50	92.3	88.7	91.2	85.4	94.1	96.2	98.0	98.7
100	89.4	85.1	87.8	82.3	91.7	94.5	97.1	98.0
150	86.5	81.2	84.9	78.6	89.3	92.1	96.3	97.4
200	84.1	78.9	82.3	75.8	86.5	90.3	95.5	96.7
250	81.6	76.2	79.7	73.4	83.9	88.2	94.7	96.0

Table 10 compares Trust Accuracy (%) across protocols over a number of rounds of the experiment and indicates the ability of the system to assess trust by assigning grades of trust to nodes in the system. In Trust Accuracy (%), DASTER-Chain again offers the highest performance, starting at 98.7% and only dropping to 96.0% by round 250. DTKM and DSA-EER also have a relatively high ability to evaluate trust in nodes, but did not maintain the same level of performance above DASTER-Chain. AODV and TEEN offer more traditional protocols in contrast to DASTER-Chain, DTKM, and DSA-EER and DASTER-Chain did not perform equally and the predicted measures of trust accuracy dropped almost immediately with measures of trust accuracy at 76.2% for TEEN and AODV at only 73.4%. These results also indicated that DASTER-Chain is well suited to develop and maintain robust and reliable trust management capability in a dynamic and mobile ad hoc network.

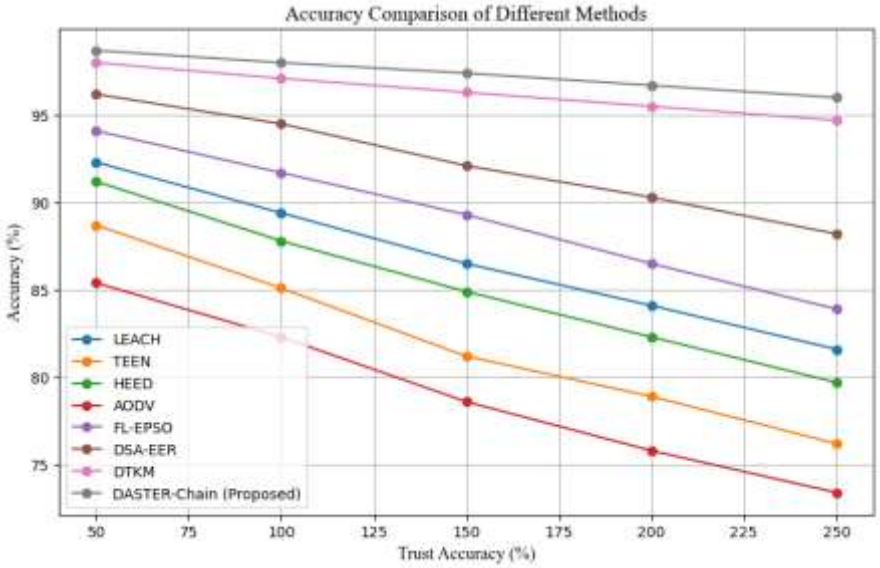

Figure 15: Trust Accuracy Comparison Chart

The figure 15 compares the accuracy of all the methods used with different accuracy levels of trust (50%-250%). DASTER-Chain (Proposed) is the best, with clearly higher accuracy in comparison to everybody else for all trust values. DSTA, DTA-KM, and DSA-EER follow next best, respectively. Traditional methods like LEACH, TEEN, HEED, and AODV imaginary drop as trust accuracy increased as those methods rely on trust fluctuations and do not operate well in trust fluctuating environments. AODV has the largest decline and has the worst performance at higher trust accuracy with DASTER-Chain (proposed) being the superior method here representing the highest robustness and reliability; overall proposed method DASTER-Chain is likely the best approach to pursue in environments that have trust-sensitive situations.

Table 11: Comparison table on False Positive Rate (FPR)

False Positive Rate (%)	LEACH [41]	TEEN [42]	HEED [43]	AODV [44]	FL-EPSO	DSA-EER	DTKM	DASTER-Chain (Proposed)
50	7.5	10.2	8.9	12.3	6.4	3.1	1.5	1.2
100	10.1	12.5	11.4	14.7	8.1	4.2	2.0	1.5
150	12.4	14.9	13.6	16.8	9.5	5.5	2.7	2.0
200	14.2	16.7	15.2	18.3	10.2	6.3	3.1	2.5

250	16.0	18.5	17.0	20.1	11.4	7.1	3.4	3.0

Table 11 shows the False Positive Rate (FPR) for each protocol in various rounds of testing, which reflects the percentage of normal activity that is incorrectly identified as an attack. Initially, the FPR for DASTER-Chain was 1.2% and finished at 3.0% in round 250, demonstrating the effectiveness of the protocol in accurately identifying threats. Both DTKM and DSA-EER had similarly low FPRs as well, while AODV, TEEN, and HEED displayed FPR as high as 20.1% for AODV, representing a significant advantage for DASTER-Chain in the number of false notifications, which are the primary cause of system unreliability.

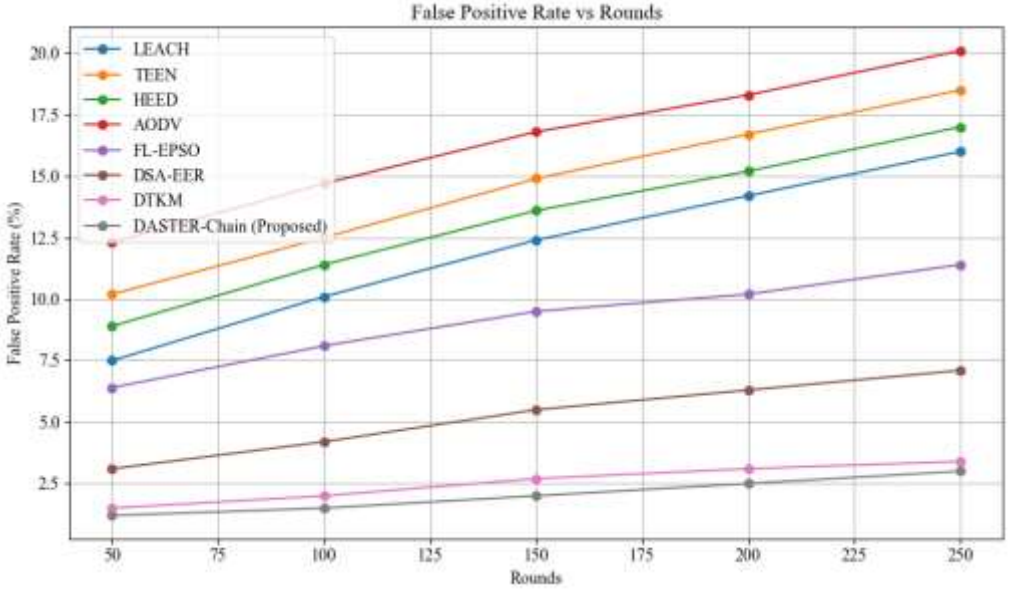

Figure 16: False Positive Rate Comparison Chart

The figure 16 illustrates the False Positive Rate (FPR) of each method (or protocol), over a range of round values (50 to 250). It is evident from the results that AODV has the highest increase in FPR, reaching over 20% after 250 rounds, with TEEN, HEED and LEACH having comparable increases. It shows how unreliable they are over time. The DASTER-Chain (Proposed) method has the consistently lowest values going through out the different round values, and also showed only a small increase in overall FPR over more rounds of operation. Once again, DTKM and DSA-EER performed similarly though not as well as the proposed method. Ultimately, through reducing false detections and maintaining stability over a longer operational time frame, the DASTER-Chain shows the most promise.

Table 12: Comparison table on Security Resilience

Security Resilience (Attack Resistance)	**LEACH [41]**	**TEEN [42]**	**HEED [43]**	**AODV [44]**	**FL-EPSO**	**DSA-EER**	**DTKM**	**DASTER-Chain (Proposed)**
50	65.2	68.1	70.5	62.3	72.4	78.3	88.5	90.2
100	61.3	64.5	66.7	60.1	70.8	75.9	85.6	87.5
150	58.7	61.2	63.4	58.5	68.3	72.4	82.3	84.1
200	55.3	58.0	60.2	55.1	65.7	69.2	78.9	80.6
250	52.1	54.8	56.9	51.8	62.1	66.3	75.5	77.2

Table 12, which is a comparison of Security Resilience (Attack Resistance) between protocols for five different rounds (50 to 250). As can be seen, DASTER-Chain (Proposed) had the highest security resilience of 90.2%, and in round 250 still had a high security resilience at 77.2%. DTKM and DSA-EER has a comparable security resilience but decreased more rapidly over time. Lastly, all other traditional protocols (LEACH, TEEN, HEED, AODV) had a significantly lower security resilience and went below 57% by the final round. This comparison shows that DASTER-Chain, is the strongest and most sustainable protocol that will secure the network for a greater amount of time.

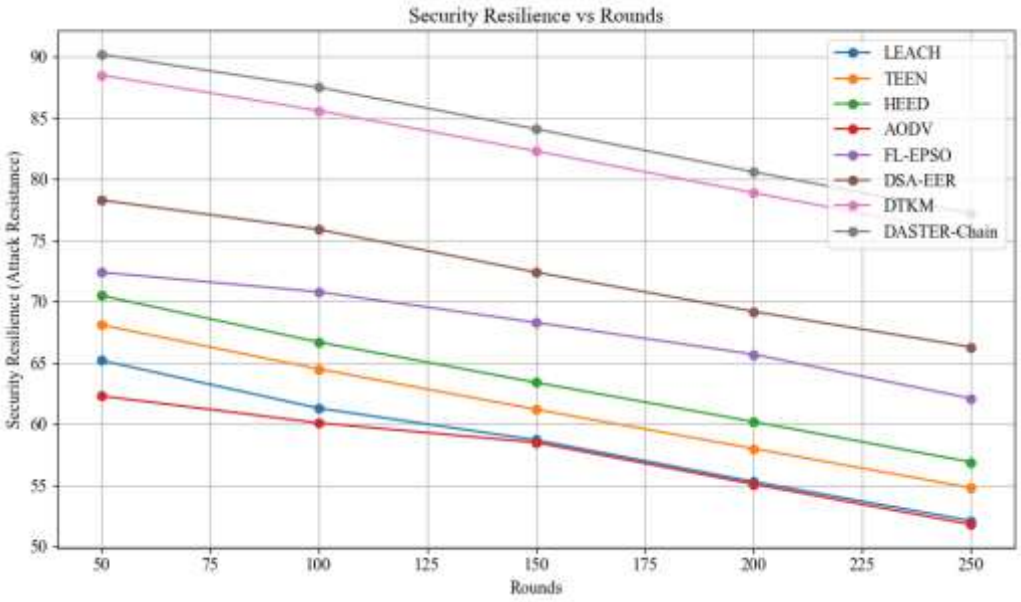

Figure 17: Security Resilience Comparison Chart

The figure 17 shows "Security Resilience vs Rounds" depicts the performance of different protocols against attacks over an increasing number of rounds in operation. DASTER-Chain consistently performed better than all of the other protocols in terms of security resilience, a ratio of protection against possible attacks - starting at 90% resilience and ending around 78%. DTKM and DSA-EER also performed comparatively better than other options, but deteriorated slowly. LEACH, TEEN, HEED, and AODV showed vulnerability in resilience more quickly - AODV dropped below 53% by round 250. DASTER-Chain is more secure and it's ability to withstand attacks is superior and sustained compared to other protocols. Therefore, DASTER-Chain is the best option for secure long-term research and deployments of wireless sensor networks.

V. CONCLUSION

The DASTER-Chain framework is a powerful, intelligent routing solution for Wireless Sensor Networks (WSNs) that uses Dynamic Self-Adaptive Energy-Efficient Routing in the blockchain-based Distributed Trust Key Management (DTKM). This collaborative design combines both performance and security by utilizing real-time energy metrics, link quality, and adaptive threshold to find the best paths and lengthen the lifetime of the network. Furthermore, we applied a blockchain-enhanced trust model to make sure that we can possibly guarantee intrusion detection, decentralized trust management, and reliable routes regularly. Also, because the blockchain approach is decentralized, it removes single points of failure, deploys the trust model securely, is more reliable for key distribution, and increases the resiliency of trust management to improper behaviour from valid insiders and malicious activity from outsiders. DASTER-Chain also applies well to variables such as dynamic environments, mobility of nodes in and out of a group of nodes, and varying node energy to deliver efficient and secure communication without risk to performance. The routing decisions based on cost and opportunistic forwarding significantly reduce the routing overhead; along with the securing logging of the Blockchain technology enhances the transparent, verifiable trust management. The self-aware routing protocols, in combination with the enforced decentralized trust offers the method to ensure scaling and autonomy can co-exist in mission critical and restricted resource IoT environments. Experimental evaluations confirm that DASTER- Chain surpasses traditional protocols such as LEACH, TEEN, HEED and AODV and more recently proposed methodologies such as FL-EPSO, DSA-EER and stand alone DTKM. Overall, it outperformed each of the protocols along all major metrics with longer network lifetime, lower energy consumption/overhead, higher packet delivery ratio and higher residual energy. Furthermore, lower end-to-end delay, routing overhead and higher throughput and residual energy resulted in DASTER-Chain being the best option for energy-constrained and time-critical WSN applications. These experimental evaluations also confirm DASTER-Chain as a viable, energy aware, high-performance and future proof wireless sensor network.

REFERENCES:

1. Al-Hubaishi, M., Çeken, C., & Al-Shaikhli, A. (2019). A novel energy-aware routing mechanism for SDN-enabled WSAN. International Journal of Communication Systems, 32(17), e3724.
2. Boyaci, A., Balik, H. H., & Ata, F. (2022, June). Energy-Aware Routing Architecture for Wireless Sensor Networks. In 2022 10th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.
3. Ekler, P., Levendovszky, J., & Pasztor, D. (2022). Energy aware IoT routing algorithms in smart city environment. IEEE Access, 10, 87733-87744.

4. Qadir, J., Ullah, U., Sainz-De-Abajo, B., Zapirain, B. G., Marques, G., & de la Torre Diez, I. (2020). Energy-aware and reliability-based localization-free cooperative acoustic wireless sensor networks. IEEE Access, 8, 121366-121384.
5. Swapna, M. P., & Satyavathy, G. (2022). Energy-aware optimal clustering and secure routing protocol for heterogeneous wireless sensor network. International Journal of Computer Networks and Applications, 9(1), 12-21.
6. Haseeb, K., Islam, N., Almogren, A., Din, I. U., Almajed, H. N., & Guizani, N. (2019). Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. IEEE Access, 7, 79980-79988.
7. Lakshmanna, K., Subramani, N., Alotaibi, Y., Alghamdi, S., Khalafand, O. I., & Nanda, A. K. (2022). Improved metaheuristic-driven energy-aware cluster-based routing scheme for IoT-assisted wireless sensor networks. Sustainability, 14(13), 7712.
8. Haseeb, K., Almustafa, K. M., Jan, Z., Saba, T., & Tariq, U. (2020). Secure and energy-aware heuristic routing protocol for wireless sensor network. IEEE Access, 8, 163962-163974.
9. Samadi, R., Nazari, A., & Seitz, J. (2023). Intelligent energy-aware routing protocol in mobile IoT networks based on SDN. IEEE Transactions on Green Communications and Networking, 7(4), 2093-2103.
10. Yin, H., Yang, H., & Shahmoradi, S. (2022). EATMR: an energy-aware trust algorithm based the AODV protocol and multi-path routing approach in wireless sensor networks. Telecommunication Systems, 81(1), 1-19.
11. Javaid, N. (2022). A secure and efficient trust model for wireless sensor IoTs using blockchain. IEEE Access, 10, 4568-4579.
12. Awan, S., Javaid, N., Ullah, S., Khan, A. U., Qamar, A. M., & Choi, J. G. (2022). Blockchain based secure routing and trust management in wireless sensor networks. Sensors, 22(2), 411.
13. She, W., Liu, Q., Tian, Z., Chen, J. S., Wang, B., & Liu, W. (2019). Blockchain trust model for malicious node detection in wireless sensor networks. IEEE Access, 7, 38947-38956.
14. Gebremariam, G. G., Panda, J., & Indu, S. (2023). Blockchain-Based Secure Localization against Malicious Nodes in IoT-Based Wireless Sensor Networks Using Federated Learning. Wireless communications and mobile computing, 2023(1), 8068038.
15. Rehman, A., Abdullah, S., Fatima, M., Iqbal, M. W., Almarhabi, K. A., Ashraf, M. U., & Ali, S. (2022). Ensuring security and energy efficiency of wireless sensor network by using blockchain. Applied Sciences, 12(21), 10794.
16. Nouman, M., Qasim, U., Nasir, H., Almasoud, A., Imran, M., & Javaid, N. (2023). Malicious node detection using machine learning and distributed data storage using blockchain in WSNs. IEEe Access, 11, 6106-6121.
17. Wijesekara, D. S. N., & Arachchige, P. (2025). Intrusion Detection Using Blockchain in Software-Defined Networking: A Literature Review. Journal of Engineering Science & Technology Review, 18(1).
18. Liang, C., Shanmugam, B., Azam, S., Karim, A., Islam, A., Zamani, M., ... & Idris, N. B. (2020). Intrusion detection system for the internet of things based on blockchain and multi-agent systems. Electronics, 9(7), 1120.
19. Abd El-moghith, I. A., & Darwish, S. M. (2021). Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach. IEEE Access, 9, 103822-103834.
20. Krishna, E. S., Sandeep, D., Kocherla, R., Lella, K. K., Molugu, S., Ibrahim, S. H. S., & Vatambeti, R. (2025). Enhancing intrusion detection in MANETs with blockchain-based trust management and enhanced GRU model. Peer-to-Peer Networking and Applications, 18(1), 1-22.
21. Awan, K. M., Sherazi, H. H. R., Ali, A., Iqbal, R., Khan, Z. A., & Mukherjee, M. (2022). Energy-aware cluster-based routing optimization for WSNs in the livestock industry. Transactions on Emerging Telecommunications Technologies, 33(3), e3816.
22. Balakiruthiga, B., Deepalakshmi, P., Mohanty, S. N., Gupta, D., Kumar, P. P., & Shankar, K. (2020). Segment routing based energy aware routing for software defined data center. Cognitive Systems Research, 64, 146-163.
23. Zhao, X., Zhong, W., & Navaei, Y. D. (2022). A Novel Energy-Aware Routing in Wireless Sensor Network Using Clustering Based on Combination of Multiobjective Genetic and Cuckoo Search Algorithm. Wireless Communications and Mobile Computing, 2022(1), 6939868.
24. Yun, W. K., & Yoo, S. J. (2021). Q-learning-based data-aggregation-aware energy-efficient routing protocol for wireless sensor networks. IEEE Access, 9, 10737-10750.
25. Ri, M. G., Han, Y. S., & Pak, J. (2022). A distributed energy-efficient opportunistic routing accompanied by timeslot allocation in wireless sensor networks. International Journal of Distributed Sensor Networks, 18(5), 15501477211049917.
26. Raja Basha, A. (2020). Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network. IET Wireless Sensor Systems, 10(4), 166-174.
27. Almuntasheri, S., & Alenazi, M. J. (2022). Software-defined network-based energy-aware routing method for wireless sensor networks in industry 4.0. Applied Sciences, 12(19), 10073.
28. Saba, T., Haseeb, K., Ud Din, I., Almogren, A., Altameem, A., & Fati, S. M. (2020). EGCIR: Energy-aware graph clustering and intelligent routing using supervised system in wireless sensor networks. Energies, 13(16), 4072.
29. Jecan, E., Pop, C., Ratiu, O., & Puschita, E. (2022). Predictive energy-aware routing solution for industrial IoT evaluated on a WSN hardware platform. Sensors, 22(6), 2107.

30. Saleh, M. M., Abdulrahman, R. S., & Salman, A. J. (2021). Energy-harvesting and energy aware routing algorithm for heterogeneous energy WSNs. Indonesian Journal of Electrical Engineering and Computer Science, 24(2), 910-920.
31. Wardana, A. A., Kołaczek, G., & Sukarno, P. (2024). Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things. Applied Sciences, 14(10), 4109.
32. Kumar, A., Budhiraja, I., Garg, D., Garg, S., Choi, B. J., & Alrashoud, M. (2025). Advanced network security with an integrated trust-based intrusion detection system for routing protocol. Alexandria Engineering Journal, 120, 378-390.
33. Rajasoundaran, S., Kumar, S. S., Selvi, M., Ganapathy, S., Rakesh, R., & Kannan, A. (2021). Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks. Wireless Networks, 27(7), 4513-4534.
34. Sivaganesan, D. (2021). A data driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks. Journal of trends in Computer Science and Smart technology (TCSST), 3(01), 59-69.
35. Ismail, S., Dawoud, D. W., & Reza, H. (2023). Securing wireless sensor networks using machine learning and blockchain: A review. Future Internet, 15(6), 200.
36. Ahmed, H. A., & Abed Al-Asadi, H. A. (2024). A Blockchain-Enabled Trust Management Framework for Energy-Efficient and Secure Routing in Mobile Ad-Hoc Networks. TEM Journal, 13(2).
37. Tariq, N., Asim, M., Khan, F. A., Baker, T., Khalid, U., & Derhab, A. (2020). A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in internet of things. Sensors, 21(1), 23.
38. Saeed, A., Javed, M. U., Almogren, A., Javaid, N., & Jamil, M. (2024). Employing blockchain and IPFS in WSNs for malicious node detection and efficient data storage. Wireless Networks, 30(4), 2313-2328.
39. Alrahhal, H., Jamous, R., Ramadan, R., Alayba, A. M., & Yadav, K. (2022). Utilising acknowledge for the trust in wireless sensor networks. Applied Sciences, 12(4), 2045.
40. Qureshi, K. N., Nafea, H. O., Tariq, I., & Ghafoor, K. Z. (2024). Blockchain-based trust and authentication model for detecting and isolating malicious nodes in flying ad hoc networks. IEEE Access.
41. Siamantas, G., Rountos, D., & Kandris, D. (2025). Energy Saving in Wireless Sensor Networks via LEACH-Based, Energy-Efficient Routing Protocols. Journal of Low Power Electronics and Applications, 15(2), 19.
42. Samant, T., Mukherjee, P., Mukherjee, A., & Datta, A. (2017, February). TEEN—V: A solution for intra-cluster cooperative communication in wireless sensor network. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) (pp. 209-213). IEEE.
43. Ullah, Z. (2020). A survey on hybrid, energy efficient and distributed (HEED) based energy efficient clustering protocols for wireless sensor networks. Wireless personal communications, 112(4), 2685-2713.
44. Rajasoundaran, S., Kumar, S. S., Selvi, M., Ganapathy, S., Rakesh, R., & Kannan, A. (2021). Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks. Wireless Networks, 27(7), 4513-4534.