Journal of Rare Cardiovascular Diseases
ISSN: 2299-3711 (Print) | e-ISSN: 2300-5505 (Online)
www.jrcd.eu
RESEARCH ARTICLE

# Trust-Aware Secure Optimization for QOS in Healthcare Wireless Sensor Networks

**Prema K[1] and Dr. N. Thenmozhi[2]**
[1]Research Scholar PG AND Research, Department Of Information Technology, Government Arts College Coimbatore
[2]Associate Professor PG And Research, Department Of Information Technology, Government Arts College Coimbatore

*Corresponding Author
Prema K
**(kprema.25.k@gmail.com)**

Article History
**Received: 21.09.2025**
**Revised: 30.09.2025**
**Accepted: 22.10.2025**
**Published: 14.11.2025**

Abstract: This research proposes a Secure Optimization paradigm to Quality of Service (QoS) in healthcare oriented Wireless Sensor Networks (WSNs), using Modular Aging Optimization (MAO) and Energy Conversion Optimization (ECO). The MAO protocol guarantees security and energy-efficient multi-hop communications by adequately taking into consideration the Node trust, energies, and aging, whereas the ECO protocol takes into account energy-aware sensing and secure data transmission. The cluster head (CH) selection based on trust tries to maximize communication reliability, which is fundamental for healthcare IoT applications. Also, the ECO protocol can optimize energy usage in addition to providing reliable data transmission via energy harvesting techniques and adaptive routing protocols to enable sensor nodes to operate sustainably within previously resource-limited environments. This enhances the health and performance of healthcare-based IoT and data protection. The study performed concentrated on testing the impact of MAO with ECO compared to five other protocols in terms of throughput, packet delivery ratio, false positive rate, end-to-end delay, and security overhead, and trust convergence time. The results indicate that MAO with ECO performed better than the baseline protocols throughout the parameters and presented better data delivery, reduced latency, and lower overhead in general. Therefore, MAO with ECO emerged as a practical and reliable method for healthcare IoT applications in large-scale and energy-limited networks.

Keywords: Healthcare IoT, Wireless Sensor Networks, Quality of Service, The trust-based Cluster Head, Modular Aging Optimization and Energy Conversion Optimization.

## INTRODUCTION

The convergence of Wireless Sensor Networks (WSNs) and Internet of Things (IoT) technologies has brought modern healthcare monitoring systems enormous developments in capabilities by enabling real-time monitoring of key parameters and managing patient data distributed over multiple nodes [1, 2]. The smart healthcare systems of today depend on system integration between IoT-enabled medical devices and sensor nodes/users within WSNs, sustaining real-time data transmission essential for life-saving healthcare services [3, 4]. However, these technological deployments continue to face ongoing challenges in the area of Quality of Service (QoS) in all areas of interest including latency, throughput, security, and energy restrictions in resource restricted or large-scale deployments [5, 6, and 7].

Although WSNs have tremendous potential for real-time continuous monitoring of health data, it is essential to consider how reliable the transmission will be, along with the trustworthiness and integrity of that data. Operationally, WSNs are vulnerable to many security threats, especially intrusion attacks, node impersonation, and data tampering [8, 9]. For trust-based communications and secure routing protocol utilization, WSNs must promote trust across the entire network. Scholarly work on security in IoT medical systems has accelerated by researching encryption, trust models, and access control systems [10, 11]. However, many of those systems are not flexible enough to adapt dynamically as nodes age and their energy levels diminish, and this has a direct relationship with routing performance and data quality. Although energy-awareness of data transmission in healthcare environments could help maximize the lifespan of sensor nodes and therefore maintain an overall performance level, other factors may adversely affect their longevity.

Recent methodologies have begun to utilize artificial intelligence-based and adaptive optimization schemes to address the dual issues of security/energy efficiency as they pertain to IoT-enabled WSNs [14, 15]. However, these methodologies typically do not offer integrated frameworks which address trust evaluation, routing and energy optimization at a single time, particularly in health-related or health care implementation's where a node impacting these issues could have dire consequences, especially from node failure, or communication delay.

In addressing these shortfalls, this paper presents a secure, trust-aware, energy optimized routing framework which includes both a Modular Aging Optimization Algorithm for adaptable route selection in pursuit of trust metrics (direct, indirect, and recent trust), and an Energy Conversion Optimization Algorithm for optimizing mobilization of energy utilized in moving information from healthcare IoT devices. The proposed framework evaluates nodes and anticipates availability of energy resources based on behaviors and metrics at run time making it scalable in terms of dynamic input, while

affording resilient multi-hop communication and detecting compromised nodes or impeding intrusions by assessing the data from the networked nodes fully aware of defined or pre-defined trust levels.

**Contribution:** A trust based Cluster Head (CH) selection algorithm with time and trust decay factors for secure route discovery. A Modular Aging Optimization method that determines acceptable routing paths based on latency, throughput and reliability of the connection. An Energy Conversion Optimization framework that reduces energy usage and prolongs the life of the network without compromising data quality, An applied illustration of the use case for the proposed framework, compared against other existing methods, as they improve on QoS metrics such as data deliverability, average end-to-end latency and energy efficiency in health-care IoT applications.

**Organization:** To identify the outline of this paper, the succeeding sections are as follows: Section 2 presents the existing works pertaining to QoS optimizations and trust-based routing in WSNs. Section 3 details the proposed optimizations framework. Section 4 explains the experimental design and performance evaluations. Section 5 compares from evaluation criteria. Section 6 provides the overall conclusion and future research context.

**Background Study**

Said et al. [16] presented a light-weight and secure data aggregation technique for IoT-enabled WSNs, with a focus on enabling data sharing with privacy. Their method enhances the performance of data aggregation while ensuring that overhead is maintained to a minimum, through the application of elliptic curve cryptography and hash -based message authentication codes. The method attempts to balance security with performance, ensuring that it is applicable in healthcare settings where sensor nodes have limited energy and processing capabilities. The secure data aggregation essentially ensures that data collected from medical sensors can still be sent while appending integrity and confidentiality.

Rathee et al. [17] dealt with the security and privacy issues specific to electronic healthcare records in an IoT-enabled environment. Their research reflects the meaning of secure communication protocols, and implies that integrating user-comprehensible devices like touch-enabled handhelds will bridge the gap of heterogeneity that exist in healthcare ecosystems. A distinct gap in the research remains multi-layered security architecture that prevents associated threats from compromised devices, communication mediums, and data compromise. This remains relevant to core concepts of security measures, as research into trust-based optimization frameworks need theory to secure healthcare data from unauthorized access and manipulation.

Qadri et al. (2018) [18] presented an extensive survey of IoT technologies emerging in healthcare, including edge computing, fog networks, and blockchain technologies. They examined the important challenges in real-time healthcare IoT systems where latency, data loss, and energy consumption can impose significant constraints on real-time processing. They noted that more effort is needed to develop intelligent and energy-aware routing protocols and intrusion detection systems for WSNs, and that the information presented will support the motivation for developing a modular approach based on Modular Aging strategies, and Energy Conversion Optimization to address real-time limitations found in critical healthcare applications.

Albahri et al. (2019) [19] propose a conceptual framework for mHealth systems that can sustain patient healthcare services in the event of network disruptions. They presented a framework that will leverage both smart paradigms of IoT architectures, and enable the system to be engaged while experiencing connectivity disruptions. The aim of their study was to highlight mHealth service continuity to patients for real-time monitoring, while integrating local-leveled data caching and smart decision making components to enact alternations or keep patient care consistent and reliable. The present work does support the notion of trust-based, multi-hop routing, as well as energy aware optimization to provide visual diagnostic tools for healthcare service continuity amidst poor monitoring, environmental or otherwise.

This patient behavioral analytics research by Tiwari et al. [20] was examining the behavior of patients in smart healthcare systems utilizing IoT based models to collect and understand patient data. Most effective was the research that highlighted the benefits of continuous tracking of patient behavior and its effect on decision making in healthcare. Smart sensors and data analytics is providing more comprehensive knowledge about patient conditions, but also needs to develop effective models for delivering that data. This models can ensure QoS (considering latency, reliability), which the proposed secure WSN framework would address utilizing energy efficient and trustaware routing models.

**Table 1: Comparison table on Healthcare IoT Devices**

| Authors & Year | Focus Area | Techniques Used | Application in Healthcare IoT | Contribution |
|---|---|---|---|---|
| Ali et al. (2022) [21] | Secure Searchable Encryption | Blockchain, Neural Network | Secure data search and | Developed a blockchain-enabled searchable encryption approach using AI |

| | | | | |
|---|---|---|---|---|
| | | | retrieval in healthcare | for secure and efficient access to encrypted medical data. |
| Elhoseny et al. (2021) [22] | Security & Privacy in MIoT | Overview & Survey | General Medical IoT Systems | Provided a comprehensive analysis of existing threats, countermeasures, and future challenges in medical IoT environments. |
| Aldahiri et al. (2021) [23] | Health Prediction Systems | IoT, Machine Learning | Predictive healthcare analytics | Reviewed recent trends combining IoT and ML for real-time patient health prediction systems. |
| Devi & Muthuselvi (2016) [24] | Data Security | Cryptographic Algorithms | IoT healthcare data confidentiality | Proposed a secret sharing mechanism using symmetric cryptography to ensure privacy in IoT-based medical data sharing. |
| Peng et al. (2017) [25] | Fault Tolerance | Network Coding | WBAN for patient monitoring | Introduced an efficient, network coding-based fault-tolerant model to enhance data reliability in smart healthcare systems. |

Dang et al. (2023) [26] these authors investigates the impact new technologies such as Artificial Intelligence (AI), Blockchain and Internet of Things (IoT) will have on intelligent healthcare systems, which utilize new technologies to advance data-driven diagnostics, remote patient monitoring, and decision making. The authors present a framework of an IoT system that is essentially a link between physical medical systems and computational intelligence. While the intent of the framework is to enhance the quality of life and responsiveness of healthcare services for patients, it is representative of the transformation of healthcare services as part of using emergent and disruptive technologies.

Ali et al. (2022) [27] these authors offer a thorough comparison of the approaches to data collection from IoT systems, Wireless Sensor Networks (WSNs) and Sensor Clouds (SC). The authors demonstrated that, while the architectures are fundamentally the same, they are different in their latency, scalability and energy efficiency. They argue that, while WSNs are energy-constrained, sensor clouds would represent better integration for large-scale healthcare monitoring, and even propose hybrid models that allow for more optimized data management in IoT-enabled medical systems.

Gowda et al. (2022) [28] these authors presents an IoT fog-computing-based approach to enhance the quality and efficiency of industrial healthcare services. The proposed system minimizes the loading on cloud servers and allows computation to occur at the location of the data source, improving response time and reliability for critical healthcare applications. The paper focuses on health service delivery that uses real-time data acquisition and processing for clinical decision support in the development of low latency, location-aware healthcare services.

Wu et al. (2023) [29] propose a lightweight authentication and key agreement protocol developed specifically for smart medical services in the Internet of Health Things (IoHT) environment. The proposed protocol allows encrypted and low-complexity communication between medical devices and backend servers. The protocol integrates the distinction between authentication and limited permission in the IoT environment to combat threats, such as impersonation and replay attacks, that are common to IoT devices and appropriate for restricted medical sensor environments.

Kumar et al (2023) [30] these authors provides a detailed summary of Healthcare IoT (H-IoT) which includes a description of current uses, future developments, and main challenges. Key areas discussed by the authors include: real-time health monitoring; emergency response systems; and wearable technologies. The authors provided a right reflexive discussion of privacy and security concerns, identifying the urgency for further lightweight cryptographic options and AI-type threat detection strategies to protect sensitive health information, as it relates to smart environments.

### 1.1 Problem Identification

Despite notable developments in IoT-based healthcare systems, there remain serious challenges in methods that accomplish secure, reliable, and energy-efficient communication in constrained environments and among resource constrained devices. Many solutions exist addressing lightweight encryption, fault tolerance, data integrity, authentication, and fog computing, but these solutions often do not consider some holistic optimization framework based on needs, use-cases, or circumstances. The aspects of integrity, latency, and QoS are inadequately addressed in a real-time environment for multi-hop WSN-based systems. Trust-aware routing and resilience to losses of nodes and services (if at all) and scalable data aggregation never used to be an issue, and better avenues and processes exist, however, this remains challenging to implement - especially in high-stakes medical IoT use cases, where patient lives may be at stake in the event any aspect suffers compromise. For these reasons, we advocate for a meaningful and rigorous needs analysis that reflects a comprehensive, modular, and flexible framework for efficiently (while also securely and adaptively) transmitting medical data in patient IoT ecosystems based on sufficiency.

# MATERIALS AND METHODS

In this study on Secure Optimization for QoS for Modular Aging and Energy Conversion Optimization for WSNs is focused on optimizing the Quality of Service (QoS) of the application on healthcare through Internet of Things (IoT) devices. The IoT health monitoring devices capture and transmit vital health-related data on a person in an accurate and timely manner, and the communication mechanism must be energy-efficient, secure, and reliable. The Modular Aging Optimization balances the energy consumption of the WSN by changing the behaviour of the WSN in terms of performance over time, whereas, Energy Conversion Optimization improves the efficiency of energy utilization in the WSN, which helps to minimize power consumption to operate for extended times. Modulation Aging Optimization integrates secure multi-hop routing and trust-bases cluster head selection method to ensure the QoS process is met to obtain timely and accurate healthcare data capture and transmission. Therefore, the entire system is suitable for real-time health monitoring and diagnosis using IoT technologies.

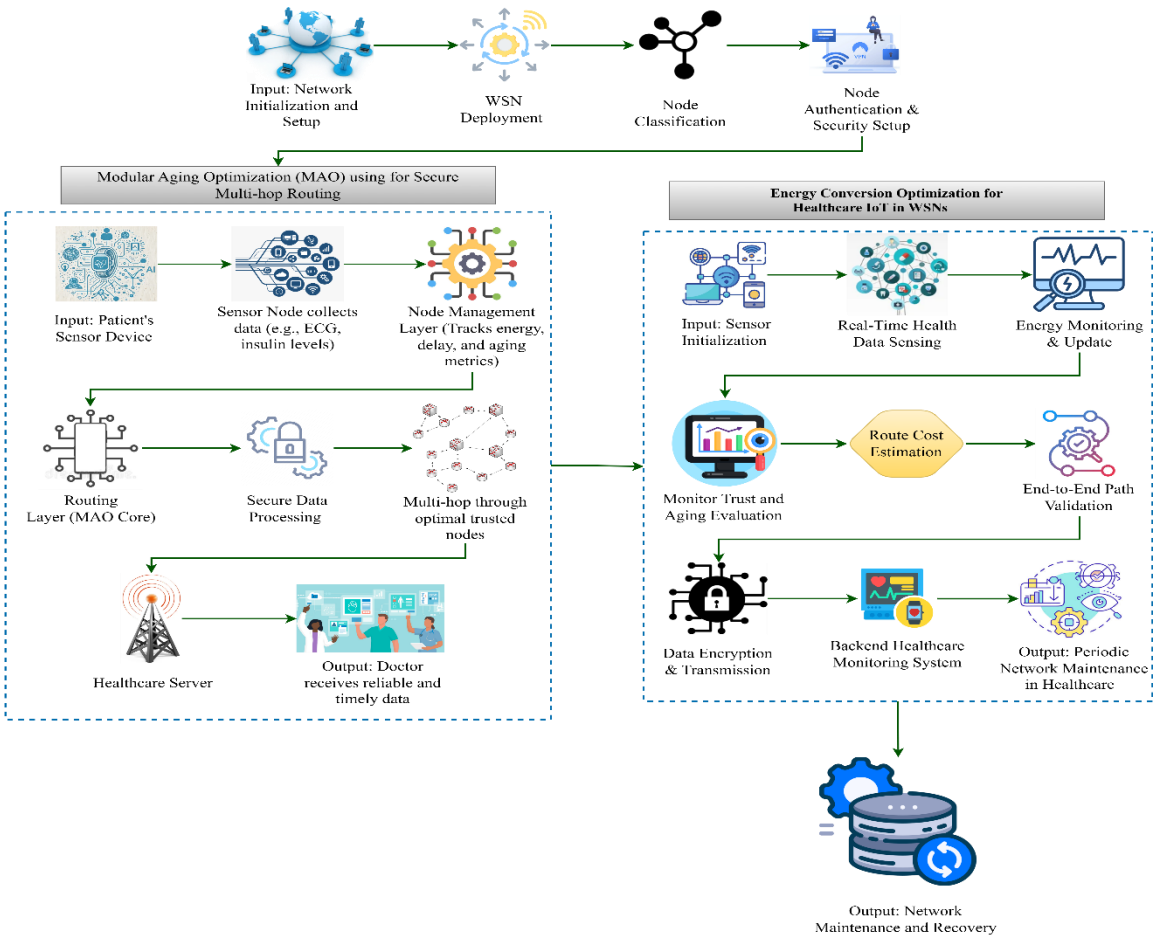


**Figure 1: Overall Architecture**

The figure 1, as depicted in the figure above, demonstrates a secure and energy-efficient operational framework for Healthcare IoT based on Wireless Sensor Networks (WSNs). The left side of the diagram, Modular Aging Optimization (MAO), performs trusted multi-hop routing by using secure sensor nodes, collects the physiological data, and assigns nodes a trust and aging parameter. The MAO ensures that data is routed through an optimized path using the MAO core engine and to the healthcare server. The right side of the diagram, Energy Conversion Optimization (ECO), includes energy aware sensing, dynamic energy updates, and evaluation of the route cost based on trust and aging score. It then ensures that the information is secured, encrypted, and sent to the backend cloud for real-time monitoring and emergency services. The last step is network maintenance, which ensures WSNs are functional, reliable, and consistently performing optimally as it relates to health-critical applications.

### 1.2 Secure Cluster Head Selection and Trust Management in WSNs

The research of security must be taken seriously when choosing Cluster Heads (CHs) and trust in Wireless Sensor Networks (WSN) as this issue is especially pertinent to healthcare applications where the data is sensitive and time critical. In a clustered WSN architecture, communication can be reduced as data is aggregated at each CH before being sent to the base

station which in most healthcare applications where monitoring is continuous saves energy for many WSN nodes. Securing CHs to ensure they have a high trust score, good energy levels, and can therefore be trusted to provide secure communication channels in deploying healthcare WSNs. Additionally, faulty CHs could corrupt or discard critical patient data if they lose energy or are otherwise malfunctioning leading to a catastrophic event. Trust management frameworks can be used to assess node behavior based on their data integrity, packet forwarding rates, and energy usage to decide if the CH is thriving or a malfunctioning node if not malicious. In time-critical healthcare applications, this process would identify CHs committed to ensuring reliable real-time patient vital sign data and even real-time monitoring of patients under controlled care. In the case of a faulty CH and persistent monitoring, the trust evaluation framework would determine if the CH was appropriate to continue using or was malicious and needed lockdown in the case of a faulty pediatric patient monitoring CH. Using lightweight cryptographic techniques and a trust scoring methodology would insulate a healthcare WSN service's monitoring activity from potential cyber threats. In conclusion, selecting a secure CH and trust framework allows for reliable and low-latency healthcare IoT solutions.

### 1.3 Modular Aging Optimization for Secure Multi-hop Routing

Modular Aging Optimization (MAO) is a new protocol that better accounts for secure multi-hop routing in Wireless Sensor Networks (WSNs) for health uses where timely information transfer is assumed to include reliability, latency, and safety. For WSNs in a health environment, data generated from a wearable or implantable device can need to hop through multiple sensor nodes before relaying back to a base station or server. As noted, previous routing protocols generally do not regard both security and dynamic aging (like processing overload or battery depletion) to avoid delays or collisions of uninvited users that may render validity concerns with data animated from the sensor node or the data message itself. MAO attempts to accommodate for security and dynamic aging through an aging model that continually tracks node health like residual energy, signal strength, trust, and processing delay across the modularized semantic fields.

In the MAO model, each node in the network is given a modular aging attribute that dynamically alters according to its operating characteristics and behavior within the network. This attribute additionally provides better informed path options that either do not traverse used or abused nodes, or preferably avoided sections of the network. The MAO model also includes trust evaluation models to help handle malicious or misbehaving nodes that can drop packets, re-order packets, and inject false medical readings. The model will allow routing processes to be distributed, avoiding depleting any node, while possibly extending the lifetime of the entire network and simultaneous QoS. Quality of Service is critical to healthcare applications and includes criteria such as low latencies and good throughput with a high packet delivery ratio.

As an added benefit, this method provides a defense mechanism for data aggregation and encryption at all of the selected nodes while taking advantage of a load distribution perspective. This is especially helpful in sensitive areas such as cardiac monitoring, ordering of insulin, or a patient motion detection system; where a delay or loss of packets would be punitive. MAO also allows for flexibility in dynamic environments, such as patient (node) movement or node failure, supported by the framework also allowing for route recalibration of the nodes. In addition, MAO supports the appraised routing path in a proportional aging manner along with trusted routing.

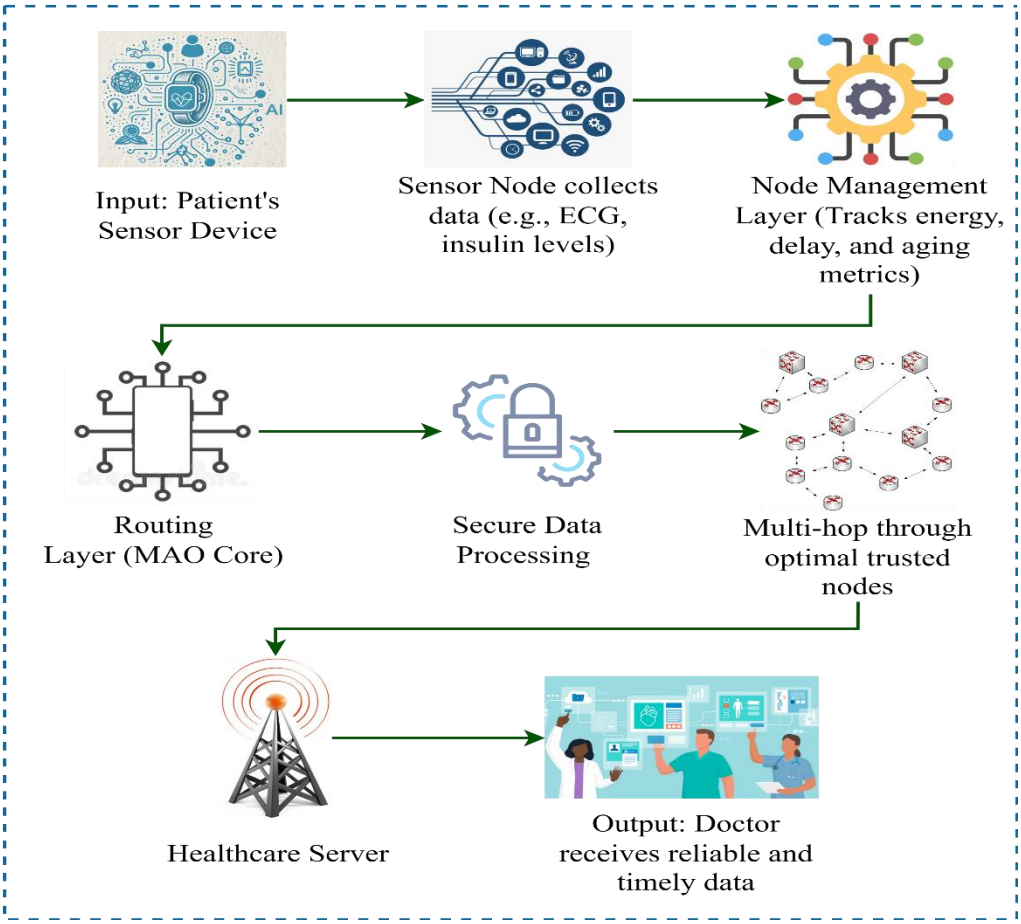


**Figure 2: Modular Aging Optimization (MAO) Architecture**

The provided figure 2 outlines the Modular Aging Optimization (MAO) framework for secure multi-hop routing for WSNs in the healthcare domain. The MAO process begins with obtaining patient data from a clinical sensor device, tracking various vitals such as electrocardiogram (ECG) reading and insulin measurements. At this point, the sensor node management apparatus will be keeping track of necessary inputs including energy, delay, and aging to determine how effective (or efficient) the node is with respect to transmitting. Data is routed using the MAO core algorithm, which manages and routes the gathered data only through trusted nodes, depending on energy used and data secure. Secure data processing protects patient's sensitive data before routed through the healthcare server. The end output will verify that healthcare providers can receive accurate and timely health information in order to make better health-related decisions.

$$NAF_i(t) = \alpha\left(1 - \frac{E_i(t)}{E_{i0}}\right) + \beta\left(\frac{T_{active}}{T_{total}}\right) \text{ ---------- (1)}$$

Equation (1) defines the Node Aging Factor $NAF_i(t)$, which represents the node aging of node $i$, based on its energy consumption and ratio of active time. In this equation, $\alpha$ and $\beta$ are weights; $\frac{E_i(t)}{E_{i0}}$ is the ratio of remaining energy, and $\frac{T_{active}}{T_{total}}$ indicates how long the node has been active.

$$TES_i = \delta \cdot \left(\frac{P_{succ}}{P_{total}}\right) + \gamma \cdot \left(1 - \frac{P_{drop}}{P_{total}}\right) \text{ ---------- (2)}$$

Equation (2) shows the Trust Evaluation Score $TES_i$ for node $i$, encompassing its successful transmission rate and low packet drop rate. In this case, $\delta$ and $\gamma$ are weights, $\frac{P_{succ}}{P_{total}}$ estimates reliability, and $1 - \frac{P_{drop}}{P_{total}}$ determines trustworthiness by minimizing data loss.

$$RCF_{ij} = \lambda_1 \cdot NAF_j + \lambda_2 \cdot \left(1 - TES_j\right) + \lambda_3 \cdot \frac{1}{E_j(t)} + \lambda_4 \cdot D_{ij} \text{ ---------- (3)}$$

Equation (3) defines the Routing Cost Function $RCF_{ij}$ for selecting the best next-hop node $j$ from node $i$. It combines four factors: the node aging factor $NAF_j$, the inverse trust score$\left(1 - TES_j\right)$, the inverse residual energy $\frac{1}{E_j(t)}$, and the distance $D_{ij}$ between nodes, each weighted by $\lambda_1$ to $\lambda_4$. Lower RCF means a better and safer routing decision.

$$OFN_i = \arg \min_{j \in N_i} (RCF_{ij}) \text{ ---------- (4)}$$

The Optimal Forwarding Node $OFN_i$ for node $i$ is defined by equation (4) as neighbor node j among the set of neighbors $N_i$ with the lowest Routing Cost Function $RCF_{ij}$. In other words, node i will select the next-hop node j which has the lowest routing cost, allowing for energy-efficient and secure multi-hop communications.

$$EPR_{path} = \prod_{(i,j) \in Path} TES_j \text{ ---------- (5)}$$

Equation (5) states that Effective Path Reliability $EPR_{path}$ is defined as the product of trust evaluation scores $TES_j$ for all intermediate nodes $j$ in the communication path. Accordingly, a routing route's overall dependability is determined by multiplying the trustworthiness of each node along the path; the greater the number, the more safe and reliable the data.

**Algorithm 1: Modular Aging Optimization**

```
Input:
   N ← Set of sensor nodes
   E_i ← Residual energy of node i
   E_i0 ← Initial energy of node i
   D_ij ← Distance between node i and node j
   P_succ, P_drop ← Packet statistics for trust
   α, β, δ, γ, λ1, λ2, λ3, λ4 ← Weight parameters
   Trust_Threshold, Energy_Threshold ← Predefined thresholds
Output:
   Secure Multi-hop Path from source to sink
Begin
Initialize each node i in N:
   Set E_i to E_i0
   Set TES_i to 1.0
   Set Aging_i to 0
For each node i in N:
   Compute NAF_i = α * (1 - E_i / E_i0) + β * (T_active / T_total)
   Compute TES_i = δ * (P_succ / (P_succ + P_drop)) + γ * (1 - (P_drop / (P_succ + P_drop)))
   If TES_i is below Trust_Threshold:
      Mark node i as UNTRUSTED
      Skip to next node
   For each neighbor j of node i:
      If TES_j < Trust_Threshold or E_j < Energy_Threshold:
         Skip to next neighbor
      Compute RCF_ij = λ1 * NAF_j + λ2 * (1 - TES_j) + λ3 * (1 / E_j) + λ4 * D_ij
      Store RCF_ij in cost_table[i][j]
   Select OFN_i as neighbor j with the minimum RCF_ij
   Append OFN_i to Routing_Path
   If OFN_i is the Sink:
      Exit the loop
Evaluate EPR_path = product of TES_x for all nodes x in Routing_Path
If EPR_path is below Trust_Threshold:
   Discard Routing_Path and repeat neighbor evaluation
Encrypt healthcare data using ECC or symmetric key encryption
Transmit data through Routing_Path
Periodically update:
   Energy levels E_i
   Trust scores TES_i
   Aging values NAF_i
End
```

The Modular Aging Optimization methodology forms an optimal secure multi-hop routing path within healthcare-based WSNs by evaluating harmonization of trust, energy, and aging factors. Each sensor node produces a Node Aging Factor (NAF) and Trust Evaluation Score (TES) to measure its qualification. When routing, the adjacent nodes are evaluated by a Route Cost Function (RCF) that is defined by the trustworthiness of the node, the energy status of the node, and the distance from the node to the destination. The optimal forward node (OFN) is clearly developed as node that produces the lowest value for the RCF, and thus the routing path is progressively developed. If the Effective Path Reliability (EPR) of

the routing path diminishes under an established threshold either because of decisions made by a node in the routing path, or to interruptions of data transmission, the routing optimization process is rerun. The data is encrypted, and securely sent along the routing path, and periodically captured updates provide an endless level of protection for a secure and dependable health care communication.

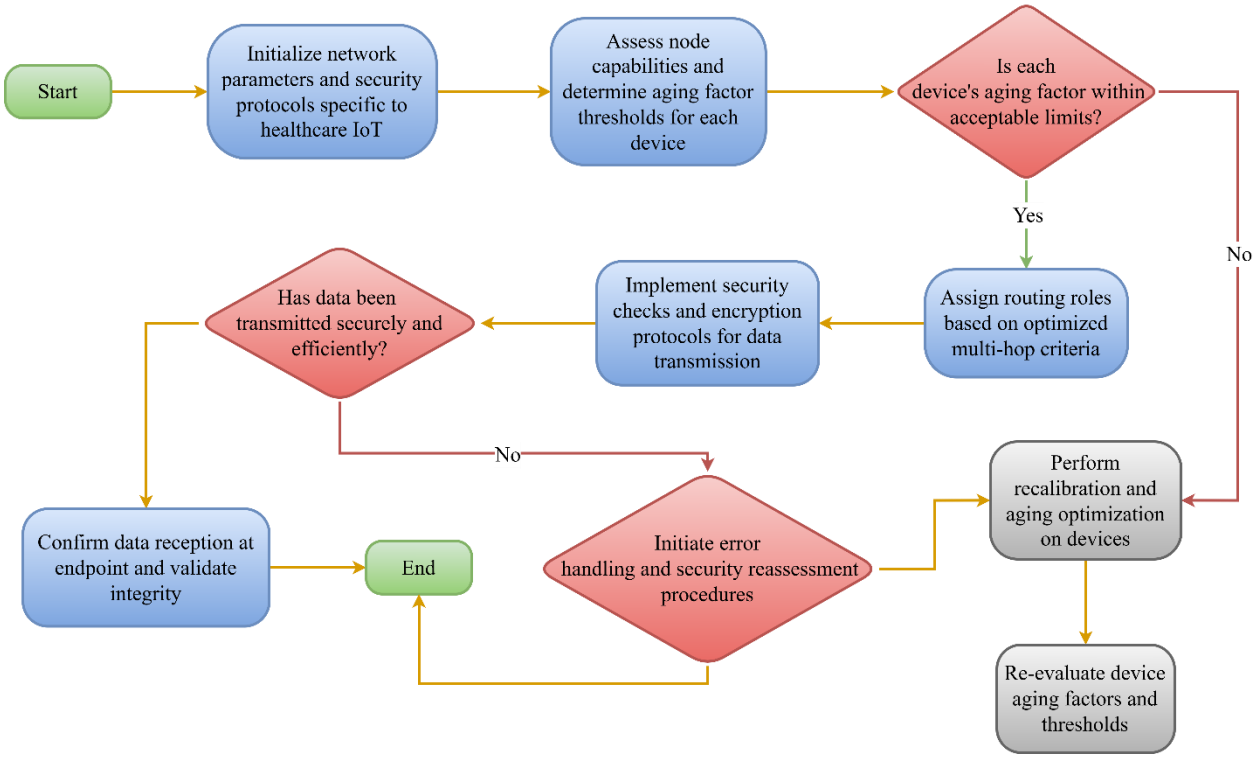


**Figure 3: Flow Chart of Modular Aging Optimization (MAO)**

The figure 3 depicted details a secure and adaptive routing protocol specific to healthcare IoT networks in WSNs. Initially, the routing protocol processes will initialize network parameters and review node capabilities, including aging thresholds. When the node's aging factor is below the acceptable threshold, the appropriate device will be selected and assigned the routing role based on optimized multi-hop selection criteria. If the node is above the reset threshold and will need to modify or have a recalibration event, the re-evaluation processes begin. The nodes of the WSN will apply their security protocols and encrypted mechanisms before the transmission of data. If the transmission is not secure, error handling, and re-evaluation event occurs. When the data has been successfully transmitted, the destination point integrity is verified for reliable patient monitoring over time. The iterative nature of the structure will permit the protocols to operate in near real-time modes, to develop optimal, aging aware routing protocols with real-time security factors involved in sensitive environments such as IoT healthcare settings.

### 1.4 Energy Conversion Optimization for Healthcare IoT in WSNs

Energy Conversion Optimization (ECO) for healthcare IoT in Wireless Sensor Networks (WSNs) is important as it ensures the sustainable implementation of medical devices throughout their lifecycle - which, as we learned previously, is often constrained in a resource-constrained environment. In healthcare IoT applications, the battery-powered sensor nodes typically possess limited energy resources to accomplish their work. ECO strategies aim to optimize the node(s) energy consumption requirements through the efficient management of energy consumption by efficiently managing their energy consumption and through their ability to convert available energy resources from specific sources such as harnessed energy (solar and kinetic), as well as environmental energy available. The objective is to optimize the use of sensor nodes' available energy, in consideration of maintaining operational performance for safety-critical applications that involve real-time monitoring of patients, emergency alarm initiation, and medical data transmission.

The characteristics of ECO strategies are applied in energy-aware routing protocols by prioritizing energy-efficient transmission paths while optimizing energy usage of each node in the network. Under this approach, when designing the routing protocol, a data management schema should be considered for each node (i.e., energy status, processing capability, communication protocols), and how to optimize the data-transmission with respect to non-strategic concerns surrounding energy conservation. This is going to be of particular concern in healthcare systems that require the transmission of critical patient data to healthcare receivers and/or storage files, where data loss and latency in processing and acknowledge can have real-world consequence.

Furthermore, ECO can encompass the application of adaptive techniques that allow for the real-time adjustment of the communication protocols and behavior of all nodes based on energy availability. For instance, nodes may enter low-power sleep modes when idle, wake for brief intervals to transmit data as needed, or decrease signaling power based on the distance of nearby nodes. This optimization not only prevents premature battery depletion but can also ensure that healthcare monitoring activity and service continues uninterrupted, thereby promoting healthcare IoT reliability and longevity.

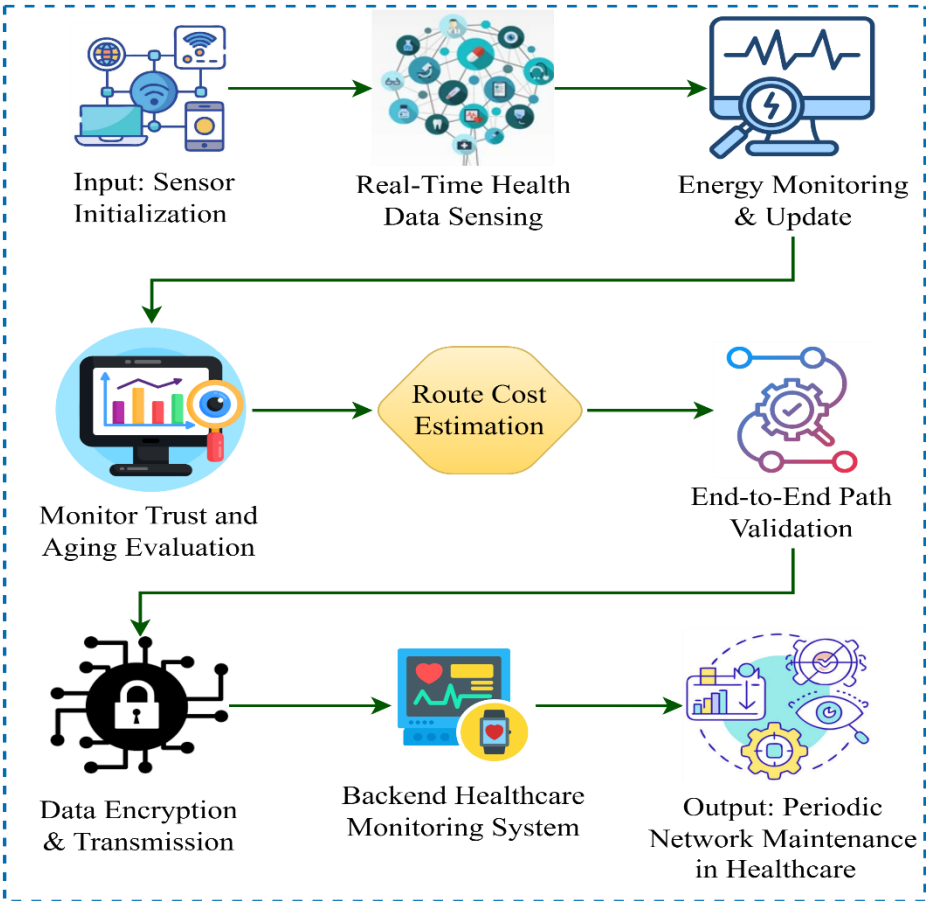


**Figure 4: Energy Conversion Optimization (ECO) Architecture**

The figure 4 shows the Energy Conversion Optimization architecture for a healthcare IoT system using WSNs. It starts by initializing the input sensors to sense health data, and these sensors will monitor continuously as they also constantly monitor their energy levels. A critical node reliability measure is done using trust and age evaluations, which provides inputs to the route cost estimation module that estimates the optimal routes with the least cost in terms of energy consumed for transmission and the most secure routing protocols available. Once a route is selected, an end-to-end route is validated to be sure the information is not lost in the process. After encryption, it allows for transmission towards a cloud-based healthcare monitoring system. Overall, this can enable the ability to perform periodic maintenance and manage the reliability of the network over the long term in a critical healthcare IoT context.

$E_t = P_{trans} \cdot T_{trans}$ ---------- (6)

The energy consumption $E_t$ during a transmission is determined in equation (6). The equation multiplies the transmission power $P_{trans}$ a node requires to transmit the data by the duration of the transmission $T_{trans}$, and ttheseresults in the total energy used by a node to send data.

$E_h = \eta \cdot A \cdot I$ ---------- (7)

Equation (7) represents the energy harvested $E_h$ from a sensor node in a wireless sensor network. The energy harvested is modeled by the efficiency value $\eta$ and the area $A$ available for energy harvesting, and the incident energy intensity $I$ (energy received over a unit area). This equation allows us to model the amount of energy a node can harvest from environmental energy sources like solar or vibrational energy.

$E_i(t+1) = E_i(t) - E_t + E_h$ ---------- (8)

The change in energy level $E_i(t+1)$, for sensor node $i$ in the next time step $t+1$, is modeled in equation (8) by taking the current energy level $E_i(t)$, removing the energy consumed $E_t$, and adding back the energy harvested $E_h$. This equation encapsulates both the energy losses from transmission and the energy replenishment from harvesting. It is specific in nature and provides a time dependent condition for a node's energy.

$$RCF_{ij} = \lambda_1 \cdot \left(\frac{1}{E_i(t)}\right) + \lambda_2 \cdot D_{ij} + \lambda_3 \cdot NAF_j + \lambda_4 \cdot (1 - TES_j) \text{ ---------- (9)}$$

Equation (9) gives the Routing Cost Function (RCF) between two nodes $i$ and $j$ in a Wireless Sensor Network (WSN) for healthcare-related Internet of Things (IoT) systems. The RCF combines several factors to identify an optimal path for the transmission of data. The first term, $\lambda_1 \cdot \left(\frac{1}{E_i(t)}\right)$, penalizes routes that go through nodes whose remaining energy is low, thus motivating nodes with higher energy. The second term,$\lambda_2 \cdot D_{ij}$, incorporates the physical distance between the nodes and longer distances increase the routing cost. The third term, $\lambda_3 \cdot NAF_j$, accounts for the node aging factor (NAF) of node $j$. The NAF is a measure of degradation of a node's performance over time due to factors, such as loss of energy. Then, $\lambda_4 \cdot (1 - TES_j)$, acknowledges the trust evaluation score (TES) of node $j$. Since lower TES yields a higher risk, thus increasing cost. The RCF is combining all the terms to try to find the route that consumes the least energy, reliable and most secure, when sending data in terms of telecommunications. All of these enhancements should help preserve quality of service (QoS) for healthcare IoT systems.

$$EPR_{path} = \prod_{(i,j)\in Path} TES_j \text{ ---------- (10)}$$

The End-to-End Path Reliability (EPR) described by Equation (10) defines the reliability of a communication path based on the cumulative trust scores of each node in a healthcare IoT environment. The formula represents the product of the Trust Evaluation Score (TES) for each node $j$ along the selected communication path $(i,j) \in Path$. A product approach demonstrates that the accumulated trustworthiness of each node along the path contributes to the overall reliability of the path. Since each node influences the reliability of the path, a low TES from just one node could significantly reduce the path's reliability. The product approach also ensures that paths containing nodes with higher trustworthiness are preferred, which are important for securing and reliably transmitting sensitive healthcare data in the IoT environment of a wireless sensor network. The higher the $EPR_{path}$ value of a potential path, the higher the reliability of a path for transmitting healthcare data.

$$\eta E = \frac{Energy\ Output}{Energy\ Input} \text{ ---------- (11)}$$

In equation (11), I denote the energy conversion efficiency ($\eta E$) of a system as the size of the energy output versus the input. This indicates how well energy is being harnessed, or better yet, how energy is applied. It is incredibly important to have high energy efficiency in healthcare's Internet of Thing (IoT) system because many of the devices and sensors in the Internet of Things are small, and sensors will have to do so in order to last longer and continue to work. Higher $\eta E$ means more of the input energy is being utilized, but lower $\eta E$ means that more of the energy is being wasted as heat or loss. For instance, greater $\eta E$ on wearable health monitors helps lower power use, increase battery life and sustained use over time within healthcare.

**Algorithm 2: Energy Conversion Optimization**

Input:
N ← Set of sensor nodes
E_i ← Residual energy of node i
E_i0 ← Initial energy of node i
D_ij ← Distance between node i and node j
P_trans ← Transmission power of node i
T_trans ← Transmission time of node i
A ← Area of energy harvesting system
I ← Intensity of ambient energy source
η ← Efficiency factor of energy harvesting system
α, β, λ1, λ2, λ3, λ4 ← Weight parameters
E_threshold ← Energy threshold for decision-making
Output:
Optimized energy conversion and routing path
Begin
Initialize each node i in N:
Set E_i to E_i0
Set Energy_harvested = 0
For each node i in N:

```
    Compute energy consumption E_t = P_trans * T_trans
    Compute energy harvested E_h = η * A * I
    Update residual energy: E_i(t+1) = E_i(t) - E_t + E_h
    If E_i(t+1) < E_threshold:
      Mark node i as energy-depleted
      Continue to next node
  For each node i:
    For each neighbor j of node i:
      If E_j < E_threshold:
        Skip to next neighbor
      Compute RCF_ij = λ1 * (1 / E_i(t)) + λ2 * D_ij + λ3 * NAF_j + λ4 * (1 - TES_j)
      Store RCF_ij in cost_table[i][j]
    Select OFN_i = arg min_j(RCF_ij) from cost_table[i]
    Add OFN_i to Routing_Path
    If OFN_i is the Sink:
      Exit loop
  Compute EPR_path = product(TES_j for all nodes j in Routing_Path)
  If EPR_path < Trust_Threshold:
    Discard Routing_Path
    Repeat neighbor evaluation
  Encrypt healthcare data using ECC or symmetric key encryption
  Transmit data through Routing_Path
  Periodically update:
    Energy levels E_i
    Trust scores TES_i
    Aging values NAF_i
End
```

The Energy Conversion Optimization algorithm for ensuring healthcare data transmission through IoT is designed here for WSNs to be conscious of energy consumption of resources and achieve reliable data transmission within the network while keeping integrity and security of the network. The algorithm calculates energy consumption for each node in the wireless sensor networks and takes into account energy transfer via energy harvesting, and updates the residual energy of the node. Subsequently, the algorithm calculates the routing cost factor (RCF) for each possible neighbor to choose the best forwarding node as recipient considering energy, distance, trust, aging, and takes into consideration resources. The protocols ensure that it only considers forwarding nodes with enough energy and trust to forward the data and completing the multi hop route. The remaining energy, trust, and RCF path is always monitored and the data is transmitted securely and in an encrypted form. Trust scores, and energy levels on the path are periodically updated so the network can respond to accumulated trust and energy levels of the devices in the network. This approach ensures reliable healthcare data transmission while addressing energy constraints of resource-constrained IoT devices and service providers.

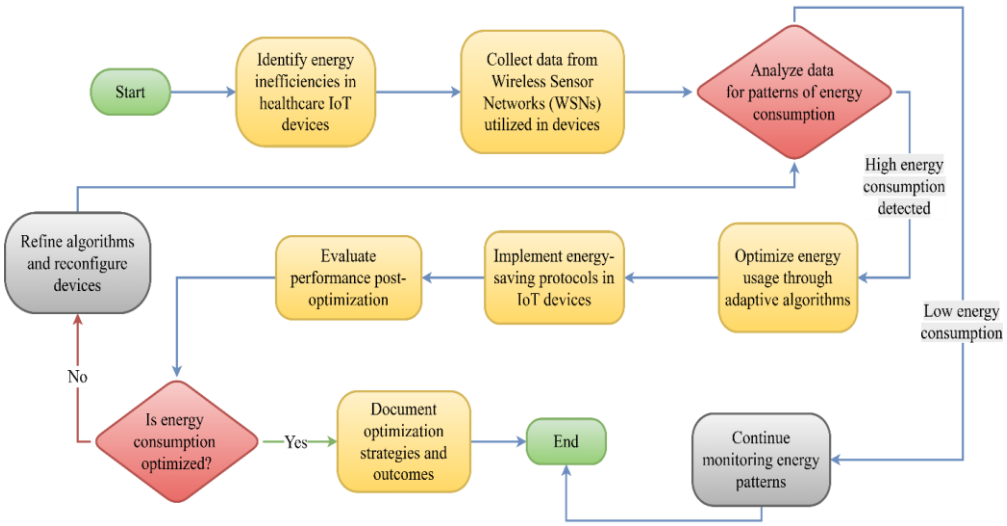


**Figure 5: Flow Chart of Energy Conversion Optimization (ECO)**

This figure 5 shows how energy optimization is done in healthcare IoT devices in Wireless Sensor Networks (WSNs). The process begins with identifying energy inefficiencies and collecting appropriate data from the healthcare IoT devices. The WSN system then analyzes the data for consumption trends, followed by detecting if the device energy use is high. If inefficiencies are detected, the system includes adaptive algorithms that optimize the energy consumption and energy-saving protocols are triggered. The system then evaluates performance and energy efficiency after the optimization of energy. If the goals of optimization are not met, the system will fit algorithms and reconfigure devices. When the energy consumption is optimized, the outputs of the optimization are reported and the WSN system continues to monitor for energy trends, so that optimizations are sustained in real-time healthcare environments.

# RESULTS AND DISCUSSION

The ability to compare networks through six routing protocols and a number of metrics makes for better value and visibility than any previous study and demonstrates the optimality of the proposed MAO with ECO; during the advanced analysis of all metrics including throughput, packet delivery ratio (PDR), end-to-end delay (E2E), routing overhead, security overhead, false positive rate, and trust convergence time, MAO with ECO consistently outperformed the comparison in TBRF, MALP, PEGASIS, RPAR, and MCMP. As the network scales, MAO with ECO has shown to continue the forwarding of data with low overhead and low delay for high data delivery while still maintaining a low false positive rate which is consistent with the efficient nature of trust as well as the increased security advertisements and increased efficacy of proposed security means, having yet to succumb to the latent presence of PDR delays in energy-constrained conditions of WSN in larger networks.

**Table 2: Comparison table on Throughput**

| Node Size | TBRF [31] | MALP [32] | PEGASIS [33] | RPAR [34] | MCMP [35] | MAO with ECO (Proposed) |
|---|---|---|---|---|---|---|
| **10** | 45 | 48 | 52 | 51 | 54 | 60 |
| **20** | 42 | 46 | 50 | 48 | 52 | 58 |
| **30** | 39 | 43 | 47 | 45 | 50 | 55 |
| **40** | 36 | 40 | 44 | 42 | 48 | 53 |
| **50** | 34 | 38 | 42 | 40 | 46 | 51 |

Table 2 displays the throughput performance values of six routing protocols consisting of TBRF, MALP, PEGASIS, RPAR, MCMP, and our proposed MAO with ECO's across varying node sizes. At all node sizes, throughput declines gradually as the node size increases from 10 to 50. This decline is expected because as the node size increases, the complexity of communicating with a larger area is likely terribly congestive when the networks scale. The proposed MAO with ECO surpasses the throughput performance of every protocol at every node size, indicating highly efficient data transmission. The worst case performance was TBRF where the overall lowest throughput performance was observed, suggesting not only ineffective scaling for the condition but also ineffective management of the network. Looking at all protocols, this study has shown that the MAO with ECO design is the most resilient and efficient protocol for sustaining high throughput in productive growing network environments.

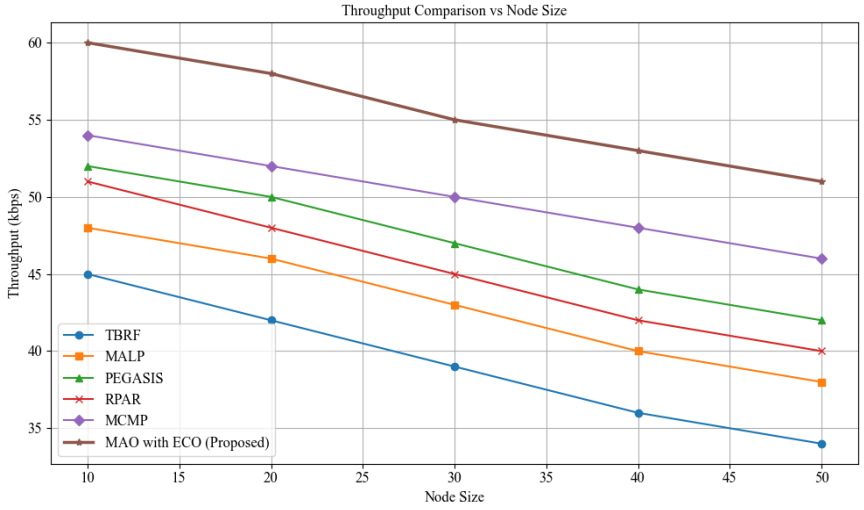


**Figure 6: Throughput Comparison Chart**

The figure 6 demonstrates the throughput values for various node sizes for six routing protocols in wireless sensor networks (WSNs). It is clear that all protocols see decreased throughput as node size increases due to increased communication overhead and energy consumption. The proposed MAO with ECO has the highest throughput in every node size and has shown consistently best overall throughput performance out of all protocols examined. This emphasizes the protocol's performance in data transmission and resource management. On the contrary, TBRF reported the lowest throughput, which can be seen as a limitation for handling scalability. Overall, the results support that MAO with ECO is the preferred means of maintaining throughput performance with larger and more complex WSN applications.

**Table 3: Comparison table on False Positive Rate (FPR)**

| Node Size | TBRF [31] | MALP [32] | PEGASIS [33] | RPAR [34] | MCMP [35] | MAO with ECO (Proposed) |
|---|---|---|---|---|---|---|
| **10** | 6.2 | 5.8 | 5.3 | 5.6 | 5.1 | 3.9 |
| **20** | 6.8 | 6.4 | 6.0 | 6.2 | 5.8 | 4.3 |
| **30** | 7.5 | 7.1 | 6.6 | 6.9 | 6.4 | 4.7 |
| **40** | 8.1 | 7.6 | 7.2 | 7.4 | 6.9 | 5.0 |
| **50** | 8.7 | 8.1 | 7.7 | 8.0 | 7.3 | 5.4 |

Table 3 compares the False Positive Rate (FPR) of six routing protocols (TBRF, MALP, PEGASIS, RPAR, MCMP, and the proposed MAO with ECO). As node size increases from 10 to 50, the False Positive Rate increases for all tested protocols, indicating that it becomes more difficult to distinguish legitimate nodes from malicious nodes in larger density networks. Among the protocols, the TBRF shows the highest FPR . On the other hand, the MAO with ECO shows the lowest FPR across all node size. This means the proposed MAO with ECO protocol is better at minimizing incorrect identifications of threats, enhancing the security and reliability of the network in many more challenging or sprawling network deployment scenarios.

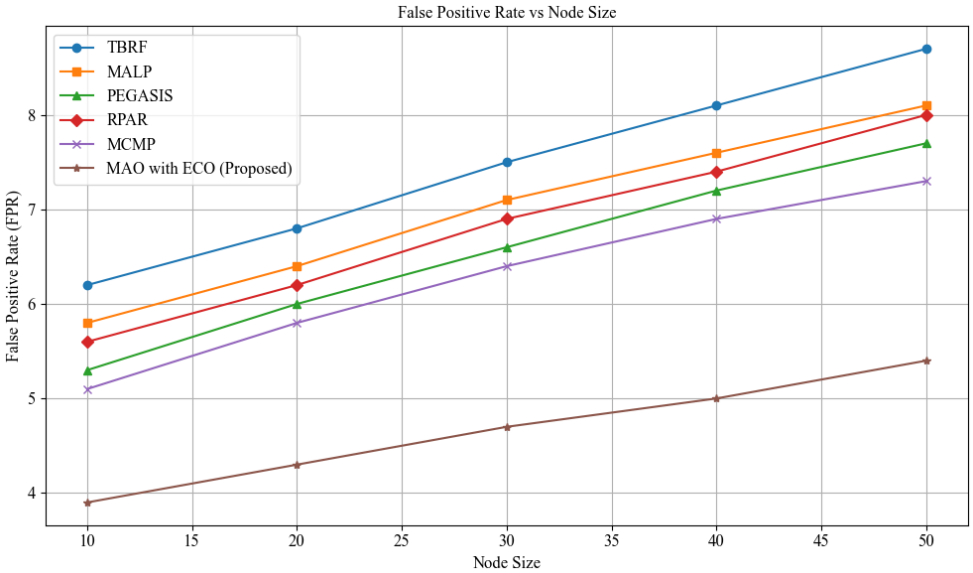


**Figure 7: False Positive Rate (FPR) Comparison Chart**

The figure 7 displays False Positive Rate (FPR) comparisons of different routing protocols as the size of the nodes in a WSN increases. As noted, the FPR increases with the node size for each method; this is mainly due to the complexity and clear uncertainty with larger networks. Again, TBRF has the highest measured FPR with all of the candidate protocols. This means TBRF has the highest probability of misclassifying benign nodes as malicious nodes. The MAO with ECO (Proposed) protocol rendered the lowest FPR across all assessed node sizes. The low FPR exhibited by the MAO with ECO (proposed) protocol shows that it has more accuracy and reliability with regard to intrusion detection. This is in-line with our assertion that this method deals well with false alarms and provides additional assurance for trusted network communications.

**Table 4: Comparison table on Security Overhead**

| Node Size | TBRF [31] | | | RPAR [34] | | |
|---|---|---|---|---|---|---|

| | | **MALP [32]** | **PEGASIS [33]** | | **MCMP [35]** | **MAO with ECO (Proposed)** |
|---|---|---|---|---|---|---|
| **10** | 7.5 | 7.2 | 6.8 | 6.9 | 6.5 | 5.1 |
| **20** | 8.3 | 7.9 | 7.3 | 7.5 | 7.1 | 5.6 |
| **30** | 9.1 | 8.7 | 8.1 | 8.3 | 7.8 | 6.0 |
| **40** | 10.0 | 9.4 | 8.9 | 9.1 | 8.6 | 6.4 |
| **50** | 10.8 | 10.1 | 9.6 | 9.9 | 9.2 | 6.9 |

Table 4 presents the security overhead suffered by six different routing protocols: TBRF, MALP, PEGASIS, RPAR, MCMP, and the proposed MAO with ECO, for an increasing number of nodes. As the number of nodes increases from 10 to 50, so does the security overhead for all protocols. This is to be expected as securing more communication paths contributes to increased overhead. TBRF consistently suffers the most overhead, whereas the proposed MAO with ECO incurred the least overhead across each node size. This reinforces the ability of MAO with ECO to provide strong security while maintaining efficient consumption of limited resources and energy, making it an efficient option in large scale, energy constrained networks.

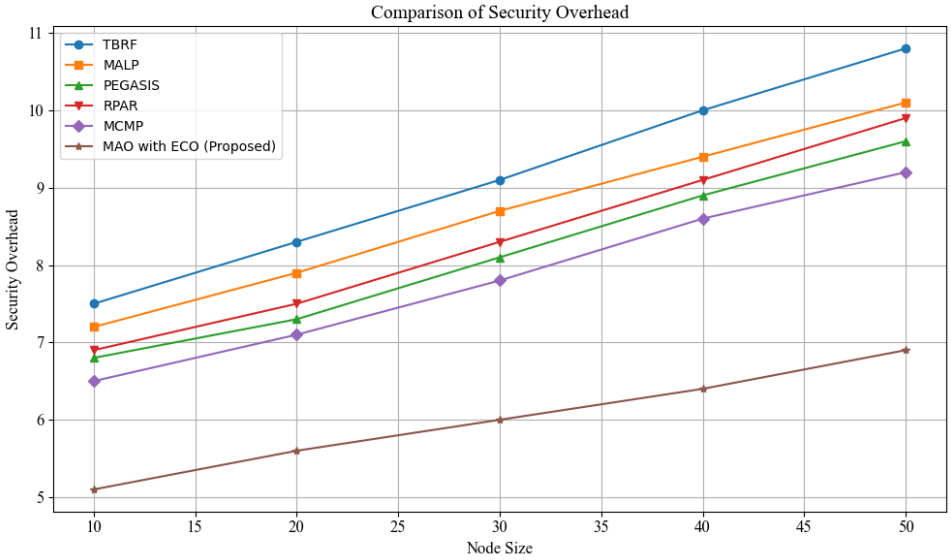


**Figure 8: Security Overhead Comparison Chart**

The figure 8 shows the Security Overhead for several routing protocols as a function of the increasing node size in a wireless sensor network. As you expect, Security Overhead increased as the size of the node increased due to the need for more encryption, authentication, and transmitted. TBRF and MALP incur the most overhead and exhibit limited efficiency to maintain secure communication in the WSN network. As depicted in the graph, the MAO with ECO (Proposed) protocol always maintains the least security overhead with the node sizes measured. This indicates that it is lightweight and efficient based on its design specifications, especially for wireless sensor networks needs such as healthcare or real-time monitoring protocols that are resource-constrained.

**Table 5: Comparison table on End-to-End Delay (latency)**

| **Node Size** | **TBRF [31]** | **MALP [32]** | **PEGASIS [33]** | **RPAR [34]** | **MCMP [35]** | **MAO with ECO (Proposed)** |
|---|---|---|---|---|---|---|
| **10** | 121 | 115 | 110 | 105 | 112 | 91 |
| **20** | 138 | 130 | 122 | 118 | 126 | 99 |
| **30** | 149 | 143 | 134 | 129 | 138 | 107 |
| **40** | 158 | 153 | 144 | 139 | 149 | 116 |
| **50** | 170 | 161 | 151 | 145 | 157 | 121 |

Table 5 compares the end-to-end delay (latency) of six routing protocols (TBRF, MALP, PEGASIS, RPAR, MCMP, and the proposed MAO with ECO) for node sizes of 10 through 50. With the increase in node size, latency increased across all protocols, as expected due to the diameter of the network causing additional transmission time and also delays due to

congestion in larger networks. TBRF has the largest delay by far, and MAO with ECO has the lowest latency by far across all node sizes. This demonstrates in conjunction with our metrics that the proposed protocol effectively optimizes the path in lieu of reducing delays in general, and can promote faster and more responsive communication even under increased loads in a dense network.

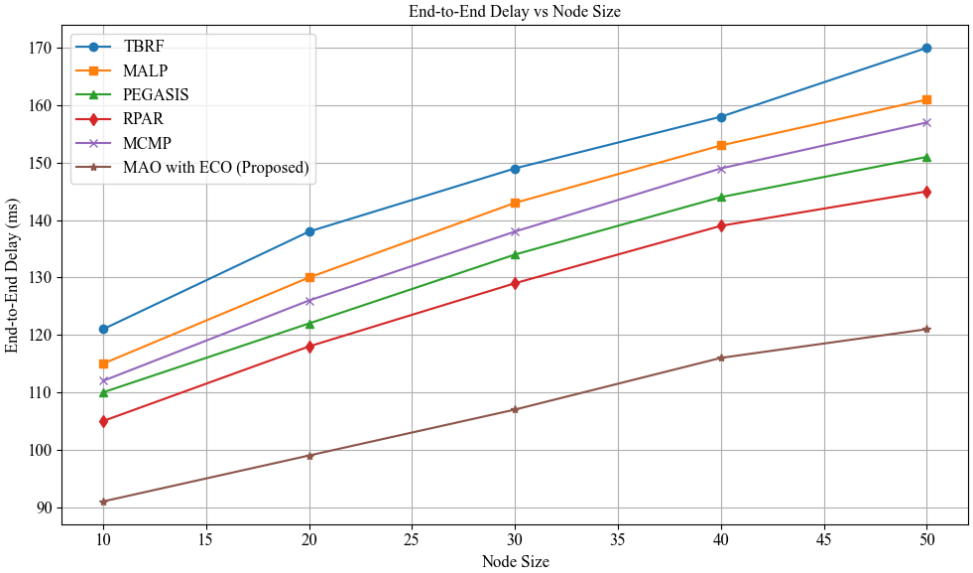


**Figure 9: End-to-End Delay (latency) Comparison Chart**

The figure 9 displays the end-to-end delay for different node sizes by the route protocols of TBRF, MALP, PEGASIS, RPAR, MCMP, and the proposed MAO with ECO route protocol. Overall, we see that as the node size increases from 10 to 50, the end-to-end delay also increases across all protocols suggesting that there is more delay in larger networks than smaller networks. We also observe that TBRF experiences the highest delay across all node sizes, and that the proposed MAO with ECO operates with the least amount of delay across all node sizes. The MAO with ECO route protocol demonstrates significantly superior efficiency in terms of reducing delay than the other protocols, likely due to incorporating more efficient path selections and energy-aware operation. As evidenced in the performance of the proposed MAO and ECO routing protocol scheme, new schemes could offer a significant improvement of performance to existing schemes when applied to very large scale networks.

**Table 6: Comparison table on Packet Delivery Ratio (PDR)**

| Node Size | TBRF [31] | MALP [32] | PEGASIS [33] | RPAR [34] | MCMP [35] | MAO with ECO (Proposed) |
|---|---|---|---|---|---|---|
| **10** | 85.1 | 86.3 | 88.9 | 87.4 | 89.5 | 94.2 |
| **20** | 82.3 | 84.2 | 87.6 | 85.5 | 88.2 | 93.1 |
| **30** | 78.5 | 80.6 | 84.4 | 83.2 | 85.6 | 91.4 |
| **40** | 74.2 | 77.9 | 81.3 | 80.1 | 82.7 | 89.6 |
| **50** | 70.5 | 75.1 | 79.1 | 77.4 | 80.9 | 88.3 |

**Table 6 shows the performance of Packet Delivery Ratio (PDR) by six routing protocols, TBRF, MALP, PEGASIS,**

RPAR, MCMP and the proposed MAO with ECO, regarding the increasing node sizes. PDR decreases for all the protocols, showing the challenge of preserving reliable delivery in larger, complex networks, as the network size increases from 10 to 50 nodes. MAO with ECO always achieves the highest PDR regardless of node size, and shows greater reliability for transmission of data, while TBRF achieves the lowest PDR, especially in larger networks. These results validate the robustness of MAO with ECO for ensuring reliable quality communication within scalable environments.

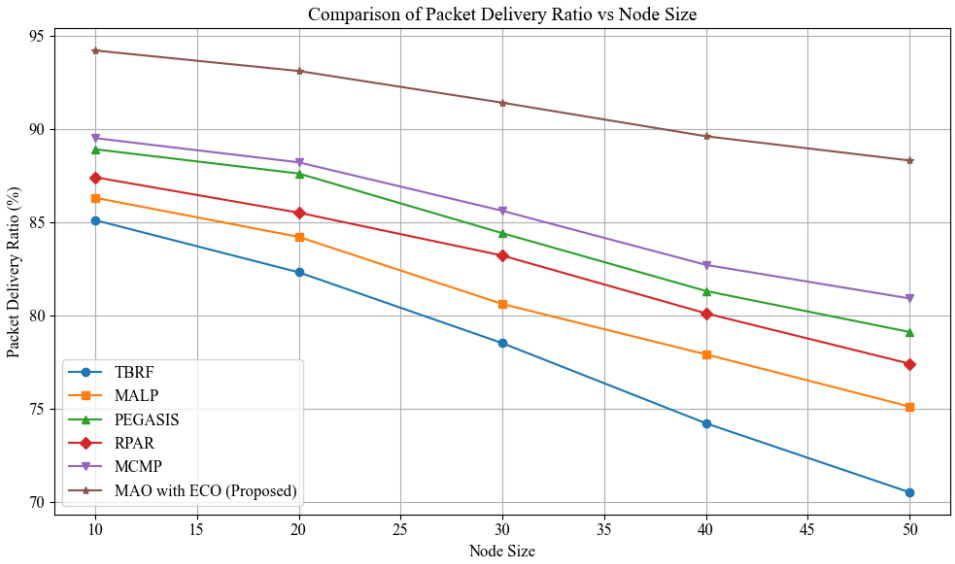


**Figure 10: Packet Delivery Ratio (PDR) Comparison Chart**

The figure 10 depicts the performance of six different routing protocols, TBRF, MALP, PEGASIS, RPAR, MCMP, and the proposed MAO with ECO, using packet delivery ratio (PDR) as the metric within different node sizes. With an increase in node size from 10 to 50, each of the protocols has a PDR decline, implying that dense networks lead to less reliability in the packet transmission process. The proposed MAO with ECO protocol has a delivery ratio which remains the highest consistently across node sizes, demonstrating stronger resiliency for the proposed course of action. The TBRF has a dramatic drop off demonstrating least efficiency and lowest delivery ratio as node sizes increase, highlighting the advantage of MAO with ECO to sustain quality of communication in scalable environments.

**Table 7: Comparison table on Trust Convergence Time**

| Node Size | TBRF [31] | MALP [32] | PEGASIS [33] | RPAR [34] | MCMP [35] | MAO with ECO (Proposed) |
|---|---|---|---|---|---|---|
| **10** | 45 | 43 | 41 | 42 | 39 | 30 |
| **20** | 52 | 49 | 47 | 46 | 44 | 34 |
| **30** | 60 | 58 | 53 | 51 | 49 | 39 |
| **40** | 68 | 63 | 60 | 58 | 55 | 43 |
| **50** | 75 | 70 | 66 | 63 | 60 | 47 |

The table 7 above present's trusts convergence time for various protocols from different node sizes, and it can be seen that trust convergence time increases as node size increases for each protocol. The MAO with ECO (Proposed) protocol tends to use the least amount of convergence time in arriving at trust convergence, which is evident by the fact it has the least convergence time at all node sizes. At 50 nodes, it has a convergence time of 47; TBRF is next at 75, followed by MALP at 70, for example. Since the MAO with ECO protocol shows a much lower trust convergence time than the next protocols, it reflects its efficiency in arriving at trust convergence. The MAO with ECO protocol's efficient trust convergence time likely is a result of its optimized approach versus neighboring protocol methods. Importantly, MAO with ECO provided more efficiency than its competitors through appropriate handling of network dynamics.

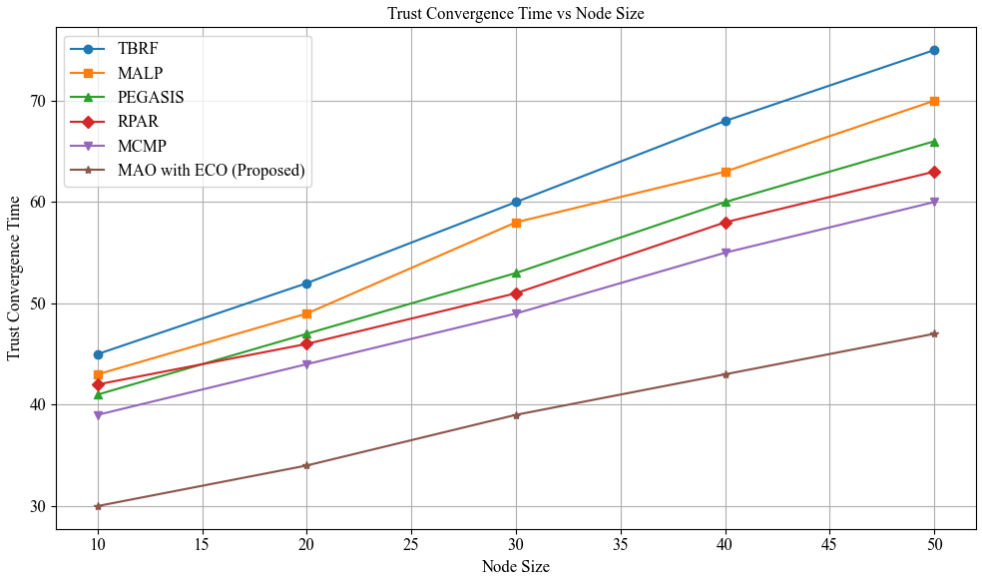


**Figure 11: Trust Convergence Time Comparison Chart**

The figure 11 illustrates the trust convergence time with respect to node size for six different protocols TBRF, MALP, PEGASIS, RPAR, MCMP, and the proposed MAO with eco. As node size increases from 10 to 50, trust convergence time also increases for all protocols, reflecting the increased complexity of trust establishment over larger networks. Among the protocols, TBRF and MALP demonstrated the highest convergence times, indicating they are slower to evaluate trust; conversely, the proposed MAO with eco consistently demonstrated trust convergence time shorter than the other protocols, suggesting it can very rapidly establish trustworthy communication paths. This also demonstrates the scalability and reliability of the proposed protocol in dynamic network environments.

**Table 8: Comparison table on Routing Overhead**

| Node Size | TBRF [31] | MALP [32] | PEGASIS [33] | RPAR [34] | MCMP [35] | MAO with ECO (Proposed) |
|---|---|---|---|---|---|---|
| **10** | 12.1 | 11.3 | 10.8 | 10.5 | 9.9 | 7.8 |
| **20** | 13.4 | 12.6 | 11.9 | 11.4 | 10.7 | 8.3 |
| **30** | 14.8 | 13.7 | 13.1 | 12.5 | 11.6 | 9.0 |
| **40** | 16.1 | 14.3 | 14.3 | 13.5 | 12.5 | 9.6 |
| **50** | 17.3 | 15.5 | 15.5 | 14.6 | 13.4 | 10.2 |

The table 8 comparison of routing overheads shows that MAO with ECO (Proposed) has the least overhead in all node sizes. As the number of nodes increases from 10 to 50 for all protocols, routing overhead increases. This is expected because everyone needs to communicate, which rises the routing overhead. The expression proposed protocol shows efficiency compared to others with a significant lower maximum cost or overhead (10.2 compared to 17.3 in TBRF and 15.5 in MALP and PEGASIS) at 50 nodes. This matches our prior statements that MAO with ECO maintains simplicity, controls routing information exchanges, is adaptable, and can be supportive of sustainable energy addition to lower hypothesis.

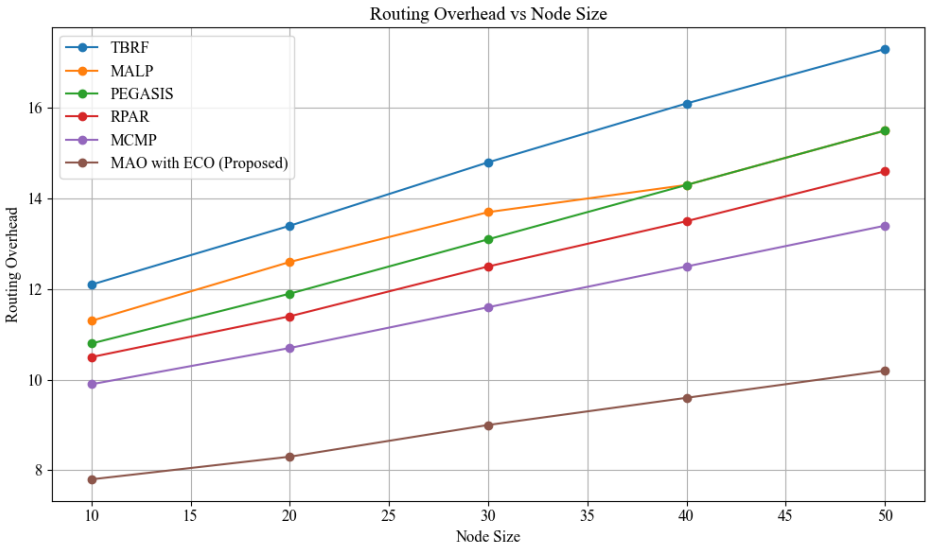


**Figure 12: Routing Overhead Comparison Chart**

The figure 12 illustrates the routing or control overhead with varying node sizes for TBRF, MALP, PEGASIS, RPAR, MCMP and the proposed MAO with ECO. Globally across the various different node sizes of 10 to 50 node size both the routing overhead is increasing depending on the protocol, this is a reflect of the added overhead of control messages when the network increases in size. Of the protocols and respective overhead TBRF shows the largest overhead consistently, whereas proposed routing overhead with MAO and ECO shows the smallest overhead for any given node size. Taken together, and through the proposed model's minimal communication and control traffic means it is scalable and suitable for energy and resource constrained devices and networks.

## CONCLUSION

In conclusion, this research proposes a Comprehensive and Generative Secure, Energy-efficient and High-performance routing approach appropriate for Wireless Sensor Networks (WSNs) in healthcare Internet of Things (IoT) applications based on the Modular Aging Optimization (MAO) with Energy Conversion Optimization (ECO) framework. The proposed model is unique in its inclusion of trust evaluation, dynamic node aging, and energy conversion mechanisms to achieve a secure and adaptive multi-hop routing approach that can overcome the problems of prior schemes. Through the combined use of trust-aware CH selection and real-time energy harvesting models, MAO with ECO extends the reliability, availability and lifespan of healthcare WSNs while providing secure transmission of sensitive healthcare information. To demonstrate the established performance of the system, performance analysis has been conducted using multiple performance metrics, including throughput, packet-delivery ratio, end-to-end delay, routing and security overhead, false positive rate, and trust convergence time. The performance validated the effectiveness of the proposed system in securing; energy-efficient and high-performance route through healthcare applications using WSNs. MAO with ECO demonstrated the strongest performance no matter the network size, illustrating the robustness and flexibility of the method across complex, large-scale environments. This framework could be especially relevant for healthcare use cases where real-time data monitoring and the preservation of data integrity is paramount. The framework provides an intelligent routing strategy while using light-weight cryptographic methods to achieve strong protection without heavy resource utilization. Furthermore, the adaptability of trust and energy periodically updates will help keep the system responsive and resilient against dynamic conditions, such as node failures and mobility. This research provides an opportunity for more intelligent, secure, and sustainable IoT Systems in critical applications with novel WSN routing methods. The MAO and ECO combination therefore shows potential to advance both performance and scalability of healthcare IoT infrastructure, in environments where energy is constrained and latencies show sensitivity. We look forward to extending the framework to support AI-enabled bulk anomaly detection for proactive threat response and adaptive routing decisions. We will also have a real-world deployment to test it in various healthcare situations, to assess both its practical usability and possible performance.

## DECLARATIONS

**-Ethical Approval: not applicable**

. **Funding**: nil

**Conflicts of interest/Competing interests**

No conflicts of interest

**Availability of data and material: nil**

**Author's contribution**

- **Prema K** made a contribution with his full support, both technically and in the development of the project.

- **Dr.N. Thenmozhi** made a significant contribution, providing complete support as well as the supervision and development.

**ACKNOWLEDGMENT:(Dr.N. Thenmozhi)**

# REFERENCES:


1. Shakeri, M., Sadeghi-Niaraki, A., Choi, S. M., & Islam, S. R. (2020). Performance analysis of IoT-based health and environment WSN deployment. *Sensors*, *20*(20), 5923.
2. Ray, P. P., Dash, D., & De, D. (2019). Internet of things-based real-time model study on e-healthcare: Device, message service and dew computing. *Computer Networks*, *149*, 226-239.
3. Swami Durai, S. K., Duraisamy, B., & Thirukrishna, J. T. (2023). Certain investigation on healthcare monitoring for enhancing data transmission in WSN. *International journal of wireless information networks*, *30*(1), 103-110.
4. Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuhaya, M. A., Bairagi, A. K., Khan, M. A. M., & Kee, S. H. (2022, October). IoT-based healthcare-monitoring system towards improving quality of life: A review. In *Healthcare* (Vol. 10, No. 10, p. 1993). MDPI.
5. Al Shahrani, A. M., Rizwan, A., Sánchez-Chero, M., Rosas-Prado, C. E., Salazar, E. B., & Awad, N. A. (2022). An internet of things (IoT)-based optimization to enhance security in healthcare applications. *Mathematical Problems in Engineering*, *2022*(1), 6802967.
6. Pardeshi, D. K. (2022). Implementation of fault detection framework for healthcare monitoring system using IoT, sensors in wireless environment. *Telematique*, *21*(1), 5451-5460.
7. Kashyap, R. (2020). Applications of wireless sensor networks in healthcare. In *IoT and WSN applications for modern agricultural advancements: Emerging research and opportunities* (pp. 8-40). IGI Global.
8. Li, W., Chai, Y., Khan, F., Jan, S. R. U., Verma, S., Menon, V. G., ... & Li, X. (2021). A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system. *Mobile networks and applications*, *26*, 234-252.
9. Gurewitz, O., Shifrin, M., & Dvir, E. (2022). Data gathering techniques in wsn: a cross-layer view. *Sensors*, *22*(7), 2650.
10. Almaiah, M. A., Yelisetti, S., Arya, L., Babu Christopher, N. K., Kaliappan, K., Vellaisamy, P., ... & Alkdour, T. (2023). A novel approach for improving the security of IoT–medical data systems using an enhanced dynamic Bayesian network. *Electronics*, *12*(20), 4316.
11. Begum, B. A., & Nandury, S. V. (2022). A survey of data aggregation protocols for energy conservation in wsn and iot. *Wireless Communications and Mobile Computing*, *2022*(1), 8765335.
12. Zahid, N., Sodhro, A. H., Kamboh, U. R., Alkhayyat, A., & Wang, L. (2022). AI-driven adaptive reliable and sustainable approach for internet of things enabled healthcare system. *Math. Biosci. Eng*, *19*(4), 3953-3971.
13. Fischer, G. S., Ramos, G. D. O., Costa, C. A. D., Alberti, A. M., Griebler, D., Singh, D., & Righi, R. D. R. (2024). Multi-Hospital Management: Combining Vital Signs IoT Data and the Elasticity Technique to Support Healthcare 4.0. *IoT*, *5*(2), 381-408.
14. Dahan, F., Alroobaea, R., Alghamdi, W. Y., Mohammed, M. K., Hajjej, F., & Raahemifar, K. (2023). A smart IoMT based architecture for E-healthcare patient monitoring system using artificial intelligence algorithms. *Frontiers in Physiology*, *14*, 1125952.
15. Alhasan, W., Ahmad, R., Wazirali, R., Aleisa, N., & Shdeed, W. A. (2023). Adaptive mean center of mass particle swarm optimizer for auto-localization in 3D wireless sensor networks. *Journal of King Saud University-Computer and Information Sciences*, *35*(9), 101782.
16. Said, G., Ghani, A., Ullah, A., Azeem, M., Bilal, M., & Kwak, K. S. (2022). Light-weight secure aggregated data sharing in IoT-enabled wireless sensor networks. *IEEE Access*, *10*, 33571-33585.
17. Rathee, D., Ahuja, K., & Nayyar, A. (2019). Sustainable future IoT services with touch-enabled handheld devices. *Security and privacy of electronic healthcare records: concepts, paradigms and solutions*, *131*, 131-152.
18. Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., & Kim, S. W. (2020). The future of healthcare internet of things: a survey of emerging technologies. *IEEE Communications Surveys & Tutorials*, *22*(2), 1121-1167.
19. Albahri, O. S., Alamleh, A., Al-Quraishi, T., & Thakkar, R. (2023). Smart Real-Time IoT mHealth-based Conceptual Framework for Healthcare Services Provision during Network Failures. *Applied Data Science and Analysis*, *2023*, 110-117.
20. Tiwari, A., Dhiman, V., Iesa, M. A., Alsarhan, H., Mehbodniya, A., & Shabaz, M. (2021). Patient behavioral analysis with smart healthcare and IoT. *Behavioural Neurology*, *2021*(1), 4028761.
21. Ali, A., Almaiah, M. A., Hajjej, F., Pasha, M. F., Fang, O. H., Khan, R., ... & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. *Sensors*, *22*(2), 572.
22. Elhoseny, M., Thilakarathne, N. N., Alghamdi, M. I., Mahendran, R. K., Gardezi, A. A., Weerasinghe, H., & Welhenge, A. (2021). Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions. *Sustainability*, *13*(21), 11645.

23. Aldahiri, A., Alrashed, B., & Hussain, W. (2021). Trends in using IoT with machine learning in health prediction system. *Forecasting*, *3*(1), 181-206.
24. Devi, K. N., & Muthuselvi, R. (2016). Secret sharing of IoT healthcare data using cryptographic algorithm. *Int. J. Eng. Res*, *5*(4), 790-991.
25. Peng, Y., Wang, X., Guo, L., Wang, Y., & Deng, Q. (2017). An efficient network coding-based fault-tolerant mechanism in WBAN for smart healthcare monitoring systems. *Applied Sciences*, *7*(8), 817.
26. Dang, V. A., Vu Khanh, Q., Nguyen, V. H., Nguyen, T., & Nguyen, D. C. (2023). Intelligent healthcare: Integration of emerging technologies and Internet of Things for humanity. *Sensors*, *23*(9), 4200.
27. Ali, I., Ahmedy, I., Gani, A., Munir, M. U., & Anisi, M. H. (2022). Data collection in studies on Internet of things (IoT), wireless sensor networks (WSNs), and sensor cloud (SC): Similarities and differences. *IEEE Access*, *10*, 33909-33931.
28. Gowda, D., Sharma, A., Rao, B. K., Shankar, R., Sarma, P., Chaturvedi, A., & Hussain, N. (2022). Industrial quality healthcare services using Internet of Things and fog computing approach. *Measurement: Sensors*, *24*, 100517.
29. Wu, T. Y., Wang, L., & Chen, C. M. (2023). Enhancing the security: A lightweight authentication and key agreement protocol for smart medical services in the ioht. *Mathematics*, *11*(17), 3701.
30. Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S. H., & Hosen, A. S. (2023). Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues. *Electronics*, *12*(9), 2050.
31. Gulaskar, K., Patel, A., Raut, R., & Japkar, M. (2014). TBRF: trust based routing framework for WSNs. *International Journal of Electronics Communication and Computer Engineering*, *5*(2), 384-392.
32. Dhande, M. T., Tiwari, S., & Rathod, N. (2025). Design of an efficient Malware Prediction Model using Auto Encoded & Attention-based Recurrent Graph Relationship Analysis. *International Research Journal of Multidisciplinary Technovation*, *7*(1), 71-87.
33. Asmael, A. A. A., & Al-Nedawe, B. (2021). Energy efficient WSN using hybrid modification PEGASIS with ant lion optimization. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, *23*(1), 273-284.
34. Duobiene, S., Ratautas, K., Trusovas, R., Ragulis, P., Šlekas, G., Simniškis, R., & Račiukaitis, G. (2022). Development of wireless sensor network for environment monitoring and its implementation using SSAIL technology. *Sensors*, *22*(14), 5343.
35. Reddy, G. V., Thandapani, K., Sendhilkumar, N. C., Senthilkumar, C., Hemanth, S. V., Periannasamy, S. M., & Hemanand, D. (2022). Optimizing QoS-based clustering using a multi-hop with single cluster communication for efficient packet routing. *International Journal of Electrical and Electronics Research*, *10*(2), 69-73.