Energy-Aware Cluster-Based Routing with Federated Learning Integration for Scalable IoT Environments

Submitted: 16th July 2025; accepted: 1st October 2025

Ankur Sisodia, Swati Vishnoi, Shivshanker Singh, Nandini Sharma, Ajay Kumar Yadav

DOI: 10.14313/jamris-2026-013

Abstract:
As a result of the Internet of Things' (IoT) explosive growth secure routing, energy optimization, and privacy preservation in resource-constrained environments have become major challenges. High overhead, static decision-making and susceptibility to malevolent attacks are common problems with traditional routing protocols. Federated Learning-Assisted Encrypted Routing based on Cost Function (FL-ERCF), an improved routing protocol that combines encrypted transmission with intelligent, privacy-preserving cluster head (CH) selection, is proposed in this paper to address these issues. The proposed protocol consists of three key operations: link quality assessment based on Received Signal Strength Indicator (RSS)I, SNR, and variance measurements trustbased clustering led by federated learning(FL) that has been trained using distributed IoT nodes to dynamically select the most suitable CHs and secure data transmission via a lightweight symmetric encryption algorithm that has been improved with digital certificates (DCs). FL can preserve the privacy of nodes at the local level and provide strong robustness to model flexibility and network dynamics. The proposed FL-ERCF protocol is implemented in the NetSim simulator and compared with stronger protocols such as Energy Efficient Secure Routing (EESR) and Hybrid Secure Routing (HSR). The performance evaluation demonstrates an improved packet delivery ratio (PDR) and reduced routing overhead and throughput even against on adversary attack. In addition, the adaptive and secure nature of FL-ERCF also makes it suitable for other mobile robotic networks like drone swarms and industrial robots, where trust, energy efficiency, and mobility are essential.

Keywords: *Federated Learning (FL), Secure IoT Routing, Cluster Head (CH) Selection, Trust Score Evaluation, Energy-Efficient Communication.*

1. Introduction

The Internet of Things (IoT) has rapidly evolved into revolutionary advancement in a world populated with billions of smart things that generate and exchange data across different domains, such as health, smart cities, smart agriculture and transportation, and industrial automation (precise wiring). More than 75 billion devices will be connected worldwide by 2025, creating an ecosystem that is both dynamic and complex, and which mandates intelligent, secure, and reliable communication protocols. Despite advances in the adoption of IoT, several challenges continue to prevent proper functioning, particularly in security, energy and routing aspects. In route setup and cluster head (CH) selection, conventional routing protocols often use static metric or predetermined thresholds, which make it less efficient in dynamic network. Moreover, most of IoT devices have constrained memory, computational capacity, and energy resources which also make them highly susceptible against packet loss, network congestion, and other cyber threats, i.e., spoofing, Sybil attacks, and data forgery. Security and privacy concerns are even exacerbated in the case of distributed IoT setups. Although, this kind of traditional centralized or cryptographic-based schemes, are not suitable and often suffer from the high communication overhead and non-scalability issues especially for large-scale and heterogeneous IoT networks. Also when raw data cannot be shared between nodes and privacy constraints can be compromised, existing secure routing solutions are likely to struggle to meet the requirement of real-time adaptability or privacy preserving management of data. Past and recent IoT and robot-related challenges also point to the requirement for novel routing solutions. For example, mobility-related latency and coordination in robotic swarms of large sizes require protocols that effectively trade security, flexibility, and low overhead against privacy. Resilient communication infrastructure is essential in industrial automation and intelligent manufacturing for real-time control and anomaly detection.

In this paper, we propose an augmented routing protocol named Federated Learning-assisted Encrypted Routing using Cost Function (Fl-ERCF). Federated learning (FL) is a decentralized machine learning (ML) technique to jointly train a global model via cooperation of local IoT nodes without sharing the raw data, which is the principle idea for introducing the intelligence and privacy awareness into the deployment of the routing. This ensures routing decisions, especially the selection of CH, are also resilient to data leakage and adaptive towards network changes. The operation of the FL-ERCF protocol consists of three independent yet interrelated phases:

Link Quality Assessment – A Quality Indicator for Link (QIL) is derived based on consideration of key

transmission parameters such as RSSI, SNR, quality variance. These metrics help to find reliable communication paths with little-energy overhead and low interference.

Federated Learning-Guided Cluster Formation – A post-trained FL model predicting the optimal CHs is supplementary to standard cost-based CH selection, based on historical information, residual energy, trust ratings and the number of nodes. Integrating local learning updates of each node into a global model, it avoids raw data exchange and enhances security.

Secure Encrypted Data Transmission – Symmetric key encryption (SKE) and DC based authentication are the types of lightweight cryptographic techniques employed [4]. These schemes ensure computational efficiency on devices with constrained resources as well as ensure safe, low-latency data forwarding between CHs and the sink.

We use the NetSim simulator to validate the proposed protocol under different community types and network settings. The performance of the proposed scheme is analyzed in terms of throughput, routing overhead and packet delivery ratio (PDR) against two existing secure protocols, namely Energy Efficient Secure Routing (EESR) and Hybrid Secure Routing (HSR). According to simulation results, FLERCF performs better than the current methods in both typical and attack-prone environments, exhibiting improved security compliance, scalability, and energy efficiency. This paper's main contributions are as follows:

1. A secure routing framework that combines link quality metrics, trust-based clustering, and lightweight encryption;
2. FL integration for intelligent and privacypreserving CH selection in IoT networks.
3. A thorough assessment of performance using simulation and comparison with modern protocols.
4. The rest of the paper is organized as follows: The relevant literature on FL strategies and secure IoT routing is reviewed in Section 2. The suggested FLERCF protocol's operation is described in detail in Section 3. The simulation setup and performance metrics are described in Section 4. Results are presented and discussed in Section 5. Section 6 brings the study to a close and identifies areas for further research.

2. Literature Review

The dynamic nature of wireless sensor environments and the exponential growth of IoT devices have made secure and effective routing an essential research topic. Numerous studies have concentrated on enhancing data transmission using cryptographic schemes, energy-aware routing, and clustering. Existing methods are still constrained by issues like real-time adaptability, privacy-preserving intelligence, and attack resilience. In order to get around these limitations, there is also growing interest in incorporating FL and ML into IoT protocols, according to recent literature. In order to ensure integrity and authentication in IoT communications, secure routing protocols have developed. Cluster-based routing is an emerging technology that adopts traditional energy-efficient protocols such as LEACH, HEED, and SEP, however these protocols do not have a sound security mechanism. Even though it is a challenge to have the fixed selection of selection in dynamic environments is a bottleneck, in author [1] presented a trust aware clustering technique in which selection of cluster heads is carried out based on link quality and energy metrics. It is worth noting that in [2] authors presented a protocol combining digital signatures and encrypted routing to provide a higher level of resilience to attacks despite being both energyefficient and avoiding intrusion. In the same line we can also find a work [3], where an HSR mechanism is proposed and, where traffic monitoring for malicious node detection is combined with lightweight cryptographic functions. However, these mechanisms depend on centralized decision and fixed thresholds, which may not be feasible in mobile or heterogeneous IoT networks. In resource-constrained environments, trust-based techniques have gained popularity in detecting malicious behavior. A fuzzy clustering protocol developed by the author [4] to improve energy usage and node selection trust. According to the author [5], it is less possible to have data spoofing and selective forwarding attacks if we incorporate trust values calculated through physical, bandwidth, and congestion scores. Despite their effectiveness, these methods frequently lack flexibility and rely on preset formulas. There is still a research gap in the integration of adaptive, data-driven trust evaluation. Furthermore, distributed intelligence and real-time learning based on node behavior evolution are rarely supported by the trust models in use today. FL is a decentralized ML paradigm that has gained popularity recently. It is perfect for environments like the IoT that are bandwidth-constrained and privacysensitive. To protect data privacy in FL, each node trains a local model using its own data and only communicates model updates to a central aggregator. The foundation of FL was laid by Google's groundbreaking work by [6], which has since been applied to fields like smart transportation and mobile health. FL has been used for predictive maintenance, anomaly detection, and dynamic resource allocation in the context of the IoT. A safe FL-based intrusion detection system for edge devices was presented by [7], who achieved precise results without jeopardizing data privacy. In a similar vein [8] used FL in wireless networks to facilitate group decisionmaking without exchanging raw data. Nevertheless, little is known about the application of FL in CH selection. Current clustering algorithms don't take advantage of local intelligence or adjust to quickly shifting network conditions. This paper attempts to fill the gap by predicting optimal nodes based on energy, trust, and link quality by incorporating FL into CH selection. Hybrid models that combine intelligence and security have been studied recently. For lightweight

data security in the IoT [9] suggested a cryptographic method based on Unicode. By combining several levels of trust and authentication, [10] highlighted the necessity of secure IoT design. Although few of these studies use FL or address realtime intelligence, they do highlight the significance of hybrid designs.

New contributions also point out weaknesses in resilience to adversarial learning conditions. For instance, [11] addressed the issue of non-IID data and poisoning in FL by employing adversarial synthetic data, whereas [13] introduced gradient scale monitoring as a security mechanism for FL systems. These developments show that FL in IoT has to consider not just communication efficiency but also robustness to poisoning attacks.

Concurrently, IoT energy efficiency is also of critical concern. In [12], a comprehensive evaluation of multi-hop mesh-based IoUT networks' protocols emphasized the compromises between energy consumption and secure transmission. Likewise, [15] presented a numerical IoT-big data integration model for reducing energy consumption in smart buildings in accordance with sustainability needs. Studies like [16] and [18] used IoT data compression algorithms (e.g., LZW) to improve performance over land, and [14] showed improved reliability for underwater WSNs in Society 5.0 applications. Collectively, these studies highlight that security and energy efficiency need to co-evolve together in diverse IoT settings.

Hybrid and robotic systems also shed light on how intelligence and communication are integrated. In [17], RGB-D perception-based multimodal robot programming interface, and [19] designed an inverse kinematics model for an 18-degree of freedom robot. Likewise, [20] showed a hybrid navigation method that allows robots to drive elevators autonomously. Although these robotics applications are distinct from IoT routing, they reflect the increasing use of distributed intelligence, adaptive algorithms, and realtime decision-making, which are similar to the requirements for IoT clustering mechanisms.

Upon these observations, the new FL-ERCF protocol improves upon existing contributions in the following ways:

- In contrast to static clustering methods [1–5, 12, 14–16, 18], FL-ERCF involves federated learning-based CH selection, rendering adaptive, data-informed decisions highly responsive to dynamic network conditions.
- Security-oriented models [2, 3, 9–11, 13] lack incorporating symmetric encryption with low computational complexity and DC checking for strong trust estimation.
- Unique compared to earlier FL deployments in IoT [6–8, 11, 13], such as anomaly detection or data exchange, FL-ERCF explicitly extends FL to CH selection and routing and thereby facilitates real-time privacy-preserving intelligence.
- With the synergistic use of link quality estimation, trust scoring, and FL-based clustering, FL-ERCF provides improved adversarial robustness at the cost of no scalability or energy efficiency [12, 15, 16].
- By being based on robotics-inspired distributed intelligence [17, 19, 20], the protocol is scalable and adaptable in heterogeneous IoT deployments.

Consequently, FL-ERCF offers itself as a paradigm for scalable IoT systems to combine privacypreserving learning with secure, real-time, and flexible routing schemes, filling the loopholes left open by previous research.

3. Methodology

The suggested FL-ERCF protocol divides the routing process into three methodical and interconnected stages in order to provide secure, effective, and intelligent routing in IoT networks:

1. Link Quality Assessment
2. Cluster Formation Assisted by FL
3. Lightweight DCs for Encrypted Transmission

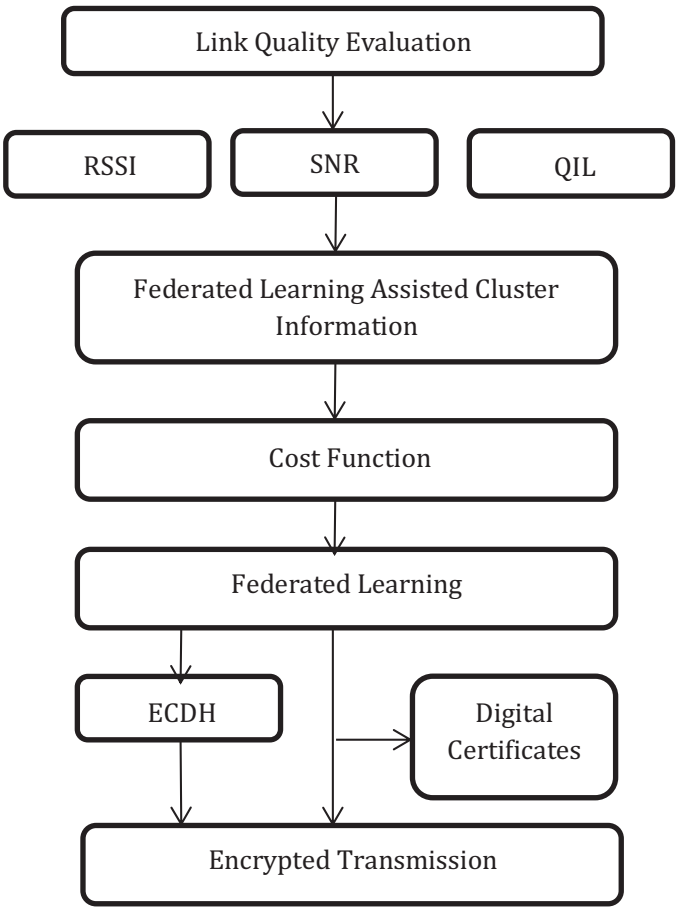

Figure 1. Block diagram of FL-ERCF protocol showing three core phases: Link Quality Evaluation, Federated Learning-Assisted Cluster Formation, and Encrypted Transmission

Figures 1 and 2 display a block diagram of FLERCF. Below is an explanation of each element.

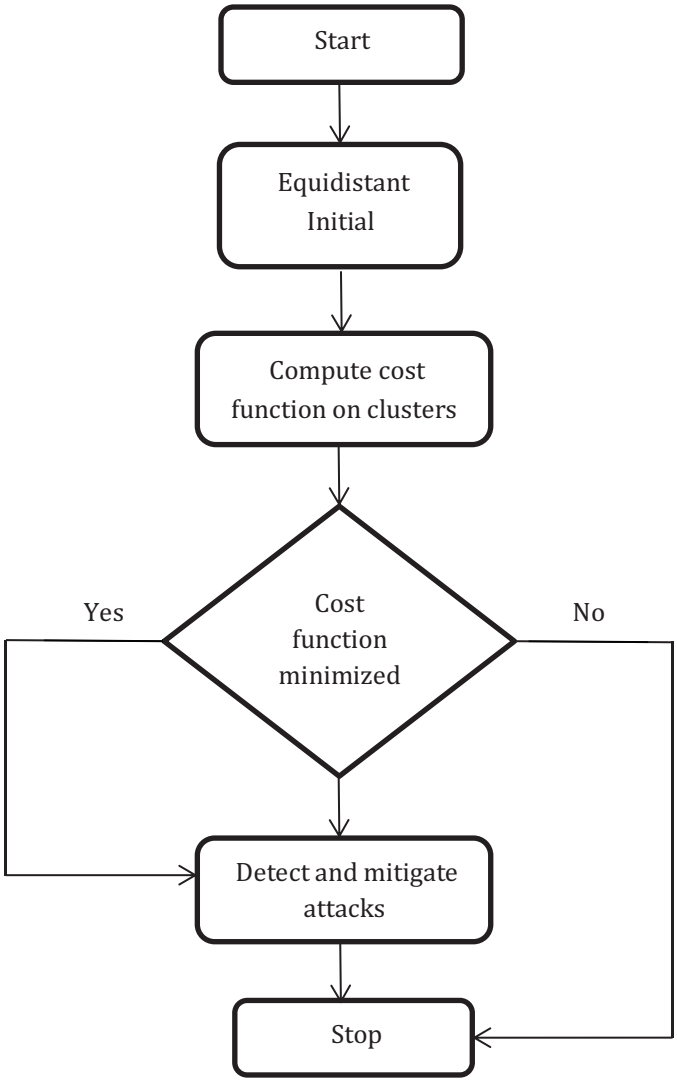

Figure 2. Flow of secure cluster formation and attack detection using cost function and trust scores in FLERCF

3.1. Phase I - Link Quality Evaluation

Choosing routes with minimal interference and high link stability is necessary for reliable data routing. Three primary parameters are used in this phase to calculate the QIL:

- The RSSI, or Received Signal Strength Indicator
- SNR, or signal-to-noise ratio
- Link Variance

These metrics are essential for subsequent CH selection and are computed using real-time data gathered from each node's transceiver.

Step 1: Compute RSSI

A signal metric called RSSI indicates how strong the signal was when it was received. For node I, the RSSI is provided by Eq. 1 and Eq. 2.

$$RI_{dBm} = RI_{value} + RSSI_{offset} \quad (...Eq.1)$$

$$P_{rec\_packet} = RI_{dBm} - B_n \quad (...Eq.2)$$

Where:

- RIvalue: register reading
- RSSIoffset: a hardware-specific value (e.g., -45 dBm)
- Bn: background noise

Step 2: Compute Signal-to-Noise Ratio (SNR)

SNR can be evaluated using Eq. 3.

$$SNR = \frac{P_{rec\_packet}}{P_n} \quad \text{or in dB:} \quad SNR_{dB} - RI_{dBm} - B_{ndBm} \quad (...Eq.3)$$

Step 3: Calculate Quality Indicator for Link (QIL)

QIL can be evaluated using Eq. 4.

$$QIL = C \cdot x \cdot \frac{RSSI}{SNR} + y \quad (...Eq.4)$$

Where:

- C: hardware correlation coefficient (range: 50100)
- x, y : empirically derived constants

Each node's communication stability is reflected in the QIL score that is produced by this phase. For intelligent clustering, the QIL moves on to the following stage.

3.2. Phase II - Federated Learning-Assisted Cluster Formation

Conventional CH selection that relies on direct metrics or static thresholds frequently results in less-than-ideal routing choices. We present a FL framework that uses distributed training to choose CHs and Cluster Gateways (CGs) in an adaptive and intelligent manner.

3.2.1. Cost Function Computation

Each node calculates a local cost function that weighs energy efficiency, link quality, and sink distance as in Eq. 5:

$$\text{Cost}_i = \alpha E_{residual} + \beta QIL_i - \gamma D_i \quad (...Eq.5)$$

Where:

- Eresidual: residual energy
- QILi: computed link quality
- Di: distance to sink node
- α, β, γ : tunable constants (e.g., 0.4, 0.4, 0.2)

3.2.2. Trust Score Calculation

Three factors are used to calculate a Trust Score (TS), which protects CHs from malicious activity:

- Bandwidth Trust Score (BTS):

BTS is used to evaluate the reliability of packet forwarding as shown in Eq. 6.

$$BTS = \frac{N_{recv}}{N_{sent}} \quad (...Eq.6)$$

- Congestion Trust Score (CTS):

CTS is used to evaluate how nodes are handling the overall load shown in Eq. 7.

$$CTS = 1 - \frac{L_{queue}}{T_{traffic}} \quad (...Eq.7)$$

- Physical Trust Score (PTS):

PTS is used to evaluate how the residual energy combines packet success ratio shown in Eq. 8.

$$PTS = \frac{E_{residual}}{E_{initial}} * \frac{N_{recv}}{N_{sent}} \quad (...Eq.8)$$

The final TS is calculated with the help of weighted combination as shown in Eq. 9.

$$TS = a^{*}BTS + b * CTS + c * PTS \text{ where } a + b + c = 1 \quad (...Eq.9)$$

Nodes with TS<0.35 are excluded from clustering.

3.2.3. Federated Learning (FL) Model for CH Selection

Every node trains a local CH prediction model, such as a lightweight neural net or decision tree, using local values (QIL, TS, Cost, and Energy).

- Nodes share model weights or gradients rather than sending data.
- A global CH prediction model is created by combining updates from a central aggregator (or decentralized aggregators via secure aggregation).
- All nodes receive the updated model back for inference.
- Every node predicts if it should function as a CH using the global model.

To adjust to changes in topology and energy dynamics, this procedure is repeated on a regular basis (e.g., every 5-10 rounds).

3.2.4. Final Cluster Formation

The network creates clusters with one-hop or twohop coverage after CHs and CGs are chosen using the FL model and trust validation. Nodes join the closest CH with the highest QIL value and trust.

3.3. Phase III - Encrypted Transmission Using Lightweight Certificates

- Elliptic Curve Diffie-Hellman (ECDH) for key exchange is one of the hybrid techniques used to secure data transmission.
- DCESC, or DC-based authentication
- For real message transfer, SKE

Every node keeps a pair of private and public keys:

- PKi ∈ [1, n − 1], and
- PUKi = PKi · B, where B is the base point on the elliptic curve.

Digital Certificate (DC) Exchange:

- IoT nodes ask the gateway for a DC.
- Gateway issues a signed DC after confirming the identity of the node.
- To mutually confirm identities, nodes use DCs.

Encryption Process (Algorithm 2):

- Determine the shared key SH=PKs · PUKd.
- Use a symmetric key generated from SH to encrypt the message.
- Deliver the encrypted message to the recipient along with a verification signature.

Decryption Process (Algorithm 3):

- Verify sender using DC
- Compute SH = PKd · PUKs
- Decrypt message using derived key

This guards against impersonation and eavesdropping attacks and guarantees low-energy, secure transmission appropriate for IoT devices.

3.4. Computational Considerations

While FL allows for flexibility and privacy, its application to IoT networks and robot swarms brings with it some computational constraints. Local training on every node demands extra CPU cycles and transitory memory allocation for update of gradients, and periodic model aggregation contributes to communication overhead. Such overheads may lead to raised energy consumption, which is especially important for low-resource devices. To counter this, the suggested FL-ERCF framework is architected with light-weight ML models like shallow neural networks rather than computationally demanding deep architectures. Additionally, the learning process is conducted periodically instead of in real-time, thus cutting down on the update frequency and saving energy and bandwidth. To further enhance communication efficiency, updates to models are compressed prior to sending, making FL possible for even low-power IoT devices. This manner, FL-ERCF strike a balance among distributed intelligence, privacy protection, and the realistic resource constraints present in actual IoT and robotic settings.

4. Performance Evaluation and Experimental Setup

We used the NetSim simulator with extensions that support FL components through Python integration to create a comprehensive simulation environment in order to assess the performance of the suggested FL-ERCF protocol and its simulation environment parameters are shown in Table 1. The simulation's main objective is to evaluate how FLassisted CH selection and encrypted routing affect important network performance metrics in contrast to two popular secure routing protocols: EESR and HSR.

These protocols were selected as they exhibited strong properties of energy-aware secured routing as well as clustering protocols.

The purpose of the simulation used in this study is to thoroughly evaluate how well the proposed (FLERCF protocol ameliorates issues of safe, costeffective, and flexible routing for IoT environments. A primary aim of the evaluation is to validate the effect of selecting the CH driven by FL on

Table 1. Simulation Environment

Parameter	Value / Range
IoT Nodes	50, 100, 200, 300, 400, 500
Simulation Area	500 m × 500 m
Initial Energy per Node	0.6 Joules
Simulation Time	200 seconds
Communication Range	50 m
Node Deployment	Random Uniform
Mobility	Static
Routing Protocols Evaluated	FL-ERCF, EESR, HSR
Attackers (Malicious Nodes)	10% and 20% of total nodes
FL Round Interval	Every 10 simulation seconds
FL Model	Decision Tree Classifier (Scikit-learn)
FL Optimizer	FedAvg (Federated Averaging)
Security Technique	ECDH with Digital Certificates (DCESC)

the applications infrastructure overall performance: especially concerning routing effectiveness and robustness. To evaluate the protocol's relative merit in scalability, energy preservation, and trust management, we compare it against two popular secure routing strategies: EESR and HSR. Furthermore, the simulation extends into analysis of the protocol's level of resistance to malicious attacks, namely by observing trends in the throughput, PDR, and routing overhead, according to increasing adversarial behavior. A variety of metrics will be used to ensure a thorough performance evaluation. Throughput or successful data reception per second, yields insight into how well a protocol maintains communication in measure of regard to the relative circumstances. The network's reliability is measured via the PDR, as the ratio of packets successfully received, relative to sent packets from source nodes. Routing overhead, i.e. number of control packets generated during route discovery and maintenance, is indicative of how well the protocol communicates. In addition, network lifetime will be captured using three indicators: First Node Dies (FND), Half Nodes Dead (HND), and Last Node Dies (LND), which captures the full perspective of the energy sustainability rate across time. The next step is to evaluate the energy efficiency of the protocol by calculating the average energy consumption by node on each simulation round. Finally, by calculating the percentage degradation in throughput and PDR as the number of malicious nodes increases, the robustness of the protocol to attacks is assessed. To evaluate the FL-ERCF protocol under varying operational conditions, three simulation scenarios were created. In the first scenario, 10% of the nodes are malicious and the protocol is evaluated for scalability and performance at increasing node densities by varying the number of IoT nodes from 50 to 500 . In the second simulation scenario, the number of nodes is held constant (300) and the percentage of malicious nodes (simulating a form of Sybil and selective packet-dropping) where malicious nodes are changed from 10% to 20%, is varied in order to assess in detail how the protocol operated under increasing levels of security risks. The third simulation scenario aimed to test the specific impacts of FL by simulating the same network in each scenario with one network using FL with CH prediction and the other using standard CH selection condition. The findings from the comparison reveal how the integration of distributed intelligence enables PDR to be enhanced while reducing routing overhead and improving energy efficiency. To initiate the simulation process, IoT nodes are first deployed in a specified area of size 500 m × 500 m, with each node preset with an initial energy level. Nodes evaluate the quality of their communication link (i.e. RSSI, SNR, and QIL) to quantify a set of values as part of the communication link quality phase of PDR. After establishing a communication link, nodes derive trust score values and local cost functions using these metrics. Values derived from these metrics serve as inputs for a lightweight ML model which is trained locally at each node. Instead of transmitting raw data to a central aggregator, nodes transmit only the model parameters securely, and the central aggregator calculates the global model using FedAvg. The global model is then sent back to the nodes in order to predict CH eligibility that is privacy-conscious and adaptive. During simulation, this FL cycle is repeated at regular time intervals to factor in node energy states and changes to network topology. At the final stage, secure routing is established by using an ECDHbased key exchange and lightweight DC-based authentication (DCESC). Once communications have been enabled with encryption, sensor nodes transfer data to the sink node safely via CHs. Throughout the simulation process metrics such as throughput, energy consumption, routing overhead, and successful delivery characteristics are recorded continuously. The deployment of malicious nodes during the simulation and evaluation process enhances our evaluation of the protocol's resiliency, robustness, and performance concerning other attacks by simulating real-world security threats.

5. Results and Discussion

Results of the suggested FL-ERCF protocol and a discussion of those results are presented in this section. Among the performance metrics considered to compare the results to two baseline protocols, EESR and HSR are throughput, PDR, routing overhead, network lifetime, and energy consumption. Also evaluated in the simulations are the effects of integrating FL in the CH selection process and how resilient the protocol is to adversarial threats.

Figures 3, 4, and 5 illustrate the performance of FL-ERCF, EESR, and HSR under varying node densities of 50, 150, 250, 350, 450, and 500. In Figure 3, FLERCF consistently produced greater throughput than EESR and HSR. Although all protocols had their throughput curves lowered by increasing node density, FL-ERCF kept its throughput curve relatively steady, and these lower throughput rates were caused by increased channel contention and interference. A majority of the drop in throughput can be attributed to the intelligent cluster formation based off of the FL which provided adaptive routing and optimal load balancing.

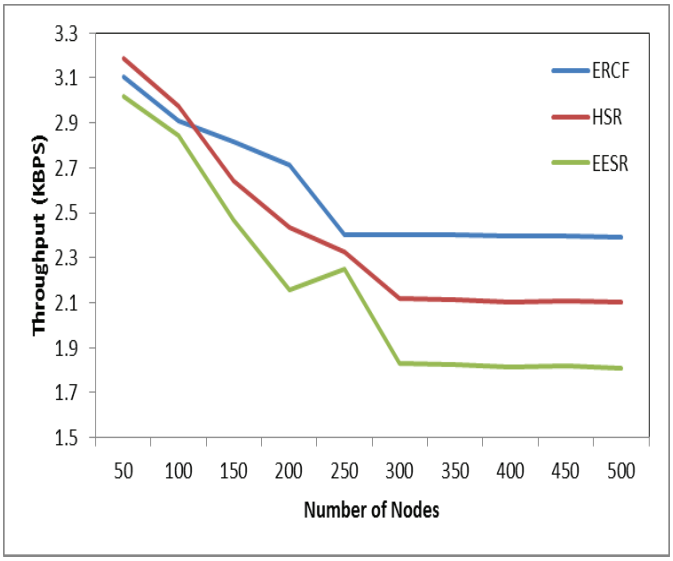

Figure 3. Throughput of IoT network with different count of IoT nodes

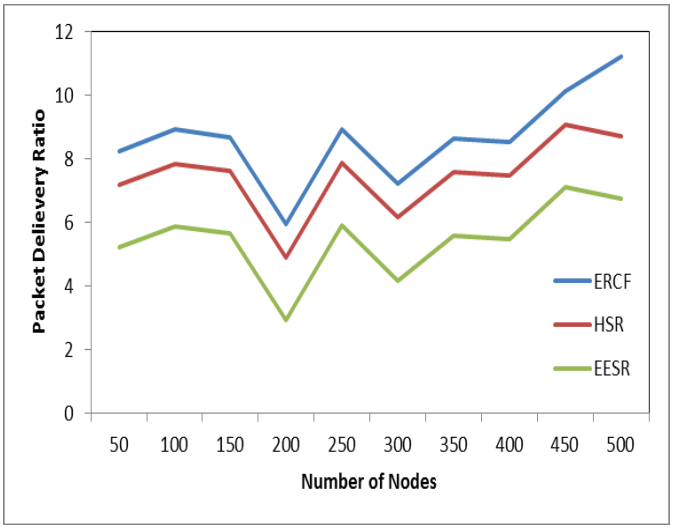

Figure 4. Packet Delivery Ratio (PDR) (%) of IoT network with different count of IoT nodes

FL-ERCF maintains a higher PDR at all node densities, as shown in Figure 4. FL-ERCF maintains a PDR of roughly 92% when the network reaches 500 nodes, whereas HSR and EESR decrease to 83% and 78%, respectively. The FL model, which adjusts routing paths in response to changing network conditions, and the trust-aware CH selection, which steers clear of unreliable nodes, is the two main drivers of this improvement.

Figure 5 illustrates how routing overhead raises with node density across all protocols as a result of more control message exchanges. In contrast to the other protocols, FL-ERCF shows a noticeably lower overhead. This is because the FL model makes predictive CH decisions, which reduces the need for frequent control message exchanges and eliminates needless re-clustering and route discovery processes.

Table 2 presents the average throughput trend over varied node densities. FL-ERCF performs 1825% better than EESR and 12 – 20% better than HSR, validating the strength of its adaptive routing mechanism.

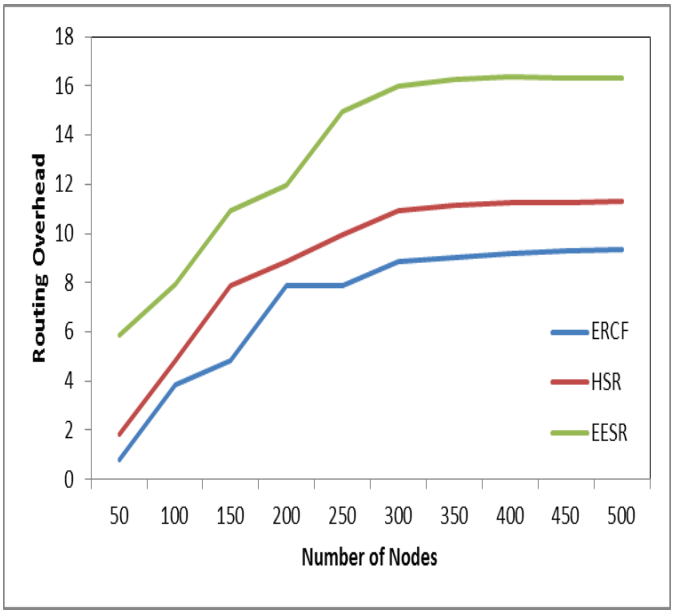

Figure 5. Routing Overhead of IoT network with different count of IoT nodes

Table 2. Average Throughput (%) under different node densities

Nodes	FL-ERCF	HSR	EESR	p-value (FL-ERCF vs HSR)	p-value (FL- ERCF vs EESR)
50	96.2	84.1	79.3	< 0.01	< 0.01
250	91.8	82.5	76.4	< 0.01	< 0.01
500	87.5	83.0	78.2	< 0.05	< 0.01

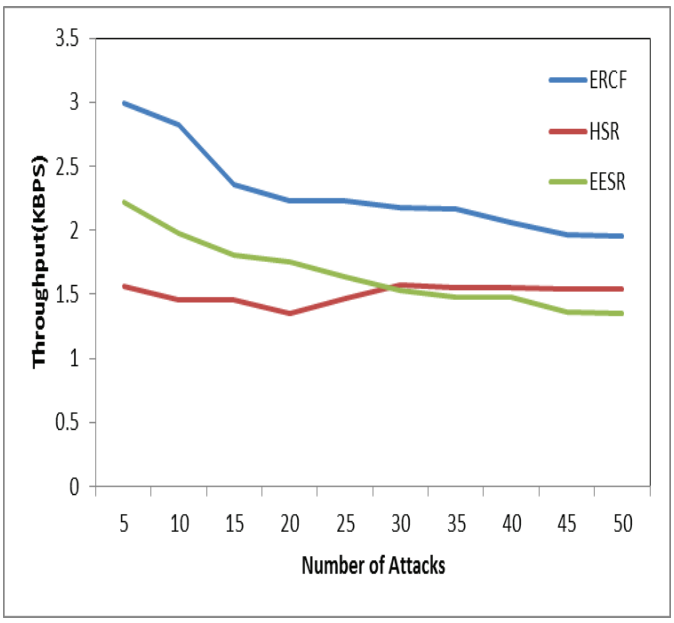

Figure 6. Throughput of IoT network with different count of attacks

Figures 6, 7, and 8 show the performance when the proportion of malicious nodes rises from 10% to

20% in order to assess the security and robustness of the protocols. These nodes mimic selective forwarding and Sybil attacks. Under attack conditions, all protocols' throughput deteriorates, as shown in Figure 6. However, FL-ERCF sees the least amount of reduction, about 12%, while HSR and EESR see reductions of 20% and 28%, respectively. The TS computation, which successfully eliminates low-trust nodes from the CH selection process, and the DCbased authentication, which stops unwanted data exchange, are responsible for FL-ERCF's superior performance.

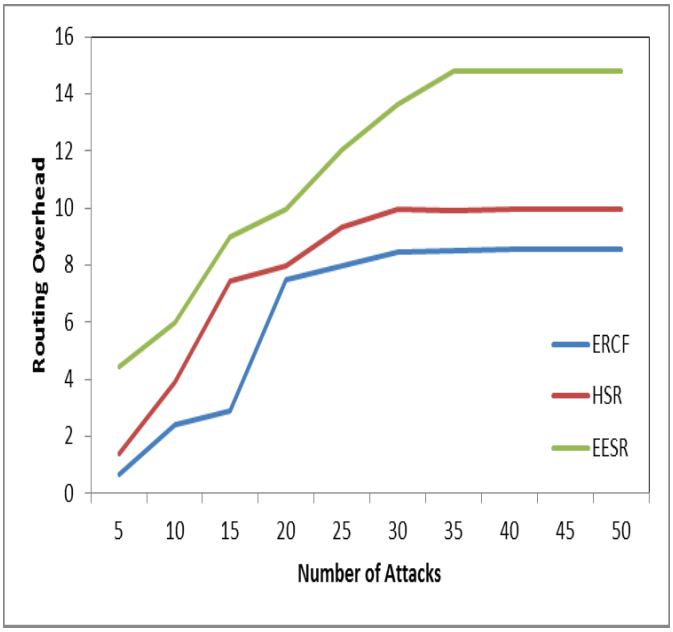

Figure 7. Routing overhead of IoT network with different count of attacks

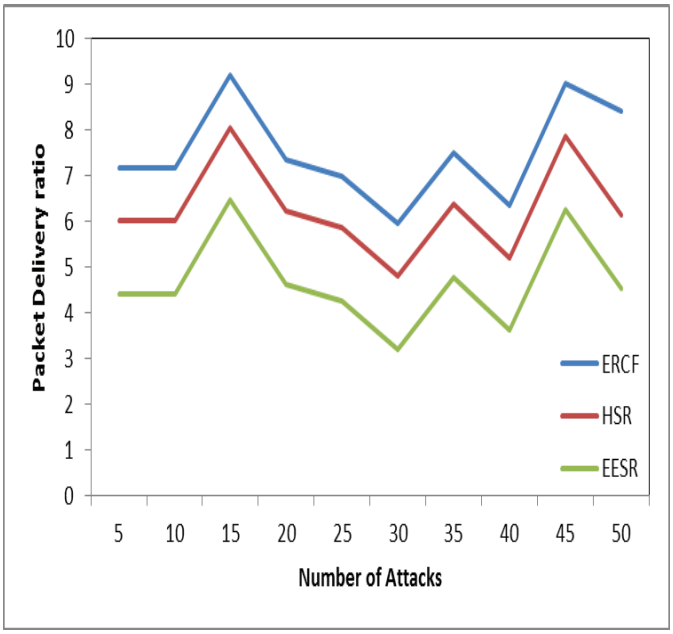

Figure 8. Packet Delivery Ratio (PDR) (%) of IoT network with different count of attacks

Even when the intensity of the attack increases, FL-ERCF maintains a lower routing overhead, as seen in Figure 7. The reason for this is that during the TSevaluation phase, compromised nodes are quickly located and isolated, negating the need for rerouting or reclustering. On the other hand, frequent path repairs brought on by packet drops and trust failures result in significant overhead increases for both EESR and HSR.

The robustness of FL-ERCF is further confirmed in Figure 8, which displays a PDR reduction of less than 9% when 20% of nodes are malicious. PDR declines of 15% and 21%, respectively, are experienced by HSR and EESR in contrast. CHs can adaptively reconfigure based on local observations thanks to FL-ERCF's FL framework, improving fault tolerance and minimizing data loss.

Based on the results, the FL-ERCF protocol provides a notable increase in network lifetime at every stage of operation. The FND is much longer compared to the benchmark protocols EESR and HSR about 28% longer compared to EESR and 20% longer compared to HSR. The energy-aware CH selection process, which aims to ensure balanced energy use of nodes, largely contributed to this result. Furthermore, the fair load distribution via federated learning, and lower overhead due to control message exchanges, work to also extend operation. The energy optimization aspect of FL-ERCF is particularly consequential when taking into consideration long-term deployment in largescale IoT networks where battery replacement is not an option.

Table 3 presents the attack-based performance trends, wherein FL-ERCF outperforms baselines in all cases with statistical significance.

Table 3. Performance under attack conditions (20% malicious nodes)

Metric	FLERCF	HSR	EESR	pvalue (FLERCF vs HSR)	pvalue (FLERCF vs EESR)
Throughput drop (%)	12	20	28	<0.01	<0.01
PDR drop (%)	9	15	21	<0.01	<0.01
Overhead increase (%)	14	23	31	<0.01	<0.01

There is also considerable performance improvements associated with FL into the cluster formation procedure. The FL-assisted method produces a 12% improvement in the PDR and reduces routing overhead by 18% compared to a variant of the protocol that uses static threshold-based CH selection. This is largely due to the predictive abilities of the global federated model to avoid unnecessary re-clustering and selecting reliable and energyefficient CHs. These results clearly demonstrate that FL is very effective for dynamic and large-scale IoT scenarios by preserving node-level privacy and simultaneously improving routing efficiency and energy management.

Outside of static IoT environments, the new FLERCF protocol is highly viable in mobile robotic networks like drone swarms and industrial autonomous robots. These networks have a number of the same characteristics as IoT deployments, including dynamic topologies, resource limitation, and the requirement for low-latency, secure communication. The FL aspect of FL-ERCF can be used to forecast stable cluster heads in the most mobile environments by using mobility attributes like relative velocity and link lifetime as inputs to the cost and trust functions. This provides adaptive CH changeover even with high-frequency topology changes. Additionally, FL-ERCF's lightweight cryptographic primitives enable it to be applicable for battery-restricted robots and drones, and the trust-based security layer can resist attacks like compromised or spoofed robotic nodes. Hence, FLERCF is not restricted to traditional IoT applications but can also improve mission success, energy savings, and robustness in robotic networks deployed in industrial or outdoor settings.

6. Conclusion and Future Work

In this work, we present FL-ERCF, a novel routing protocol developed to address the few but essential requirements of safe, low-cost, and flexible communication in IoT environments. In FL-ERCF, the concept of a three-phase process, for identifying reliable communication, captures our key notions. First, the evaluation of the quality of links (link quality), use of metrics based on RSSI, and SNR is performed as a first phase for link quality assessment. The second phase involves the actual intelligent formation of clusters, guided by a FL model which is flexible, privacy-preserving, and allows for CH selection based on TSs, costs function, link quality, and residual energy. The last phase guarantees secure data transmission leveraging encryption with lightweight algorithms such as elliptic curve cryptology and a DC-based authentication scheme. As part of a comprehensive simulation capability in support of this work, we undertook an examination of FL-ERCF using simulations based on the NetSim simulator. The FL-ERCF performance was compared against the other two protocols in two established areas, HSR and EESR, using several different sized networks and with several different attacks. The results revealed that FLERCF outperforming the existing protocols was consistent across all key performance indicators throughput, PDR, routing overhead, network lifetime, etc. Furthermore, by applying the FL model in CH selection, energy consumption was better balanced, re-clustering overhead was lower, and the flexibility of the network to adapt to the varying conditions was improved without exposing raw node data, and therefore ensuring privacy. The resistance to Sybil and selective forwarding attacks was enhanced with the inclusion of a trust-based attack detection algorithm, and the lightweight cryptographic design allowed for data integrity and authenticity at a relatively low computational cost.

There are many possibilities for following work in this area of research. The FL-ERCF could be deployed in actual physical IoT testbeds to perform real-time validation in applications such as smart agriculture, smart healthcare, or industrial automation in subsequent studies. In addition, the FL aspect of FLERCF could also be advanced by means of more complex approaches, such as deep learning or reinforcement learning for more sophisticated decision-making as there are still challenges related to mobile networks and delay-tolerant networks. Additionally, the FL process could incorporate concepts like secure aggregation principles and differential privacy mechanisms to strengthen data privacy guarantees. Overall, FL-ERCF combines a robust IoT model which includes the features of decentralized intelligence, strong trust management, more lightweight forms of encryption, which provides an implementable, scalable and secure approach for next-generation IoT networks.

Apart from massive-scale IoT settings, FL-ERCF also promises to be deployed in mobile robotics like drone networks and autonomous factory robots. Such systems necessitate adaptive routing because of perpetual mobility and need secure security against spoofing attacks as well as selective forwarding attacks. The adaptive selection of cluster heads using FL-driven adaptation in FL-ERCF can be expanded by considering mobility metrics, making the protocol more effective in supporting dynamic topologies. Future research can involve applying FL framework to mobility prediction, reducing handover latency, and assessing performance over real-world robotic testbeds. Such an extension may make FL-ERCF a general-purpose protocol that can be used with both stationary IoT infrastructures and intensely dynamic robotic settings.

AUTHORS

Ankur Sisodia* – Department of Computer Science Engineering and IoT, Noida Institute of Engineering and Technology, Greater Noida, Uttar Pradesh, India, e-mail: ankur22887@gmail.com.

Swati Vishnoi – Department of Computer Science and Engineering, Noida Institute of Engineering and Technology, Greater Noida, Uttar Pradesh, India, e-mail: swativishnoi1@gmail.com.

Shivshanker Singh – Department of Computer Science and Engineering, G L Bajaj Group of Institutions, Mathura, Uttar Pradesh, India, e-mail: shivshanker.singh@gmail.com.

Nandini Sharma – Department of Computer Science and Engineering, Anand School of Engineering & Technology, Sharda University, Agra, Uttar Pradesh, India, e-mail: nandini72@gmail.com.

Ajay Kumar Yadav – comSchool of Cyber Security and Digital Forensics, National Forensic Sciences University, Bhopal, Madhya Pradesh, India, e-mail: ajay.iitdhn@gmail.com.

*Corresponding author

References

[1] Y. Li et al, "Energy-aware Edge Association for Cluster-Based Personalized Federated Learning", IEEE Transactions on Vehicular Technology, vol. 71 no. 6, 2022, pp. 6756–6761; doi: 10.1109/TVT.2022.3161503.

[2] S. Suresh et al, "Intelligent Data Routing Strategy Based on Federated Deep Reinforcement Learning for IOT-Enabled Wireless Sensor Networks", Measurement: Sensors, vol. 31, no. 101012, 2024. Doi: 10.1016/j.measen.2023.101012.

[3] S. Li et al., "Towards Enhanced Energy Aware Resource Optimization for Edge Devices Through Multi-cluster Communication Systems", Journal of Grid Computing, vol. 22, no. 2, 2024, p. 56; doi: 10.1007/s10723-024-09773-3.

[4] N. Prabakaran, "Optimized Adaptive Multi-Scale Dual An for Multi-Objective CHS and EnergyAware Routing in 6G WC", IETE Journal of Research, vol. 70, no. 12, 2024 pp. 8692–8701; doi: 10.1080/03772063.2024.2387288.

[5] A. Das et al., "Energy Aware DBSCAN and Mobility Aware Balanced q-Learning Based Opportunistic Routing Protocol in MANET", Peer-to-Peer Networking and Applications, vol. 18, no. 4, 2025, pp. 1–19; doi: 10.1007/s12083-025-02004-w

[6] R. Alkanhel, "Dedg: Cluster-based Delay And Energy-Aware Data Gathering in 3d-Uwsn With Optimal Movement Of Multi-Auv", Drones, vol. 6, no. 10, 2022, p. 283; doi: 10.3390/drones6100283.

[7] E. Dritsas and M. Trigeka, "Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications", Journal of Sensor and Actuator Networks, vol. 14, no. 1, 2025, p. 9; doi: 10.3390/jsan14010009.

[8] E.C. Pinto Neto et al., "Federated Reinforcement Learning in Iot: Applications, Opportunities and Open Challenges", Applied Sciences, vol. 13, no. 11, 2023, p. 6497; doi: 10.3390/app13116497.

[9] D. Rupanetti and N. Kaabouch, "Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities", Applied Sciences, vol. 14, no. 16, 2024, p. 7104; doi: 10.3390/app14167104.

[10] R. Kumar et al., "From Efficiency to Sustainability: Exploring the Potential of 6G for a Greener Future", Sustainability, vol. 15, no. 23, 2023, p. 16387; doi: 10.3390/su152316387.

[11] A. Danilenka, "Tackling Non-IID Data And Data Poisoning in Federated Learning using Adversarial Synthetic Data", Journal of Automation Mobile Robotics and Intelligent Systems, vol. *18*, 2024; doi: 10.14313/JAMRIS/3-2024/17.

[12] A. Sisodia et al, "Enhancing energy efficiency: a protocol assessment in multi-hop mesh-based IOUT networks", Multimedia Tools and Applications, vol. *83*, no. 37, 2024, p.p. 8499985026; doi: 10.1007/s11042-024-19345-y.

[13] K. Bogacka et al., "Gradient Scale Monitoring for Federated Learning Systems", Journal of Automation Mobile Robotics and Intelligent Systems, *vol. 18*, 2024; doi: 10.14313/JAMRIS/32024/18.

[14] A. Sisodia et al., "To Brace Society 5.0: Enhanced Reliability with a Cost-Effective Protocol for Underwater Wireless Sensor Network", Sustainable Computing: Transforming Industry 4.0 to Society 5.0, Springer International Publishing, 2023, pp. 171–185; doi: 10.1007/978-3-031-13577-4_10.

[15] A. Zouhri, "A Numerical Analysis Based Internet of Things (IOT) and Big Data Analytics to Minimize Energy Consumption in Smart Buildings", Journal of Automation Mobile Robotics and Intelligent Systems, vol. *18*, 2024; doi: 10.14313/JAMRIS/2-2024/12.

[16] A. Sisodia and A.K. Yadav, "Performance Analysis of IoT Networks in Terrestrial Environment utilizing LZW Data Compression Technique", Review of Computer Engineering Research, vol. 10, no. 4, 2023, pp. 165–181; doi: 10.18488/76.v10i4.3550..

[17] B. Kulecki, "Multimodal Robot Programming Interface Based on RGB-D Perception and Neural Scene Understanding Modules", Journal of Automation, Mobile Robotics and Intelligent Systems, 2023, pp. 29–37; doi: 10.14313/JAMRIS/3-2023/20.

[18] A. Sisodia and A.K. Yadav , "Internet of Things: A Comparative Analysis of Network Terminologies with and without Data Compression Techniques" *2022* 11th International Conference on System Modeling & Advancement in Research Trends (SMART), 2022, pp. 236–242; doi: 10.1109/SMART55829.2022.10047640.

[19] M.A. Ortega-Palacios, A.D. Palomino-Merino, and F. Reyes-Cortes, "Inverse Kinematics Model for a 18 Degrees of Freedom Robot", Journal of Automation, Mobile Robotics and Intelligent Systems, 2023, pp. 22–29; doi: 10.14313/t4yf9254.

[20] P.L. Wu et al., "Hybrid Navigation of an Autonomous Mobile Robot to Depress an Elevator Button", Journal of Automation, Mobile Robotics and Intelligent Systems, 2022, pp. 2535; doi: 10.14313/JAMRIS/4-2022/30.