INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

# Dynamic Privacy-Aware Routing (DyPAR) for Wireless Sensor Networks

**Roland Yaw Kudozia**

**Gdirst Institute**

**DOI: https://doi.org/10.51583/IJLTEMAS.2025.1410000157**

**Received: 02 November 2025; Accepted: 12 November 2025; Published: 25 November 2025**

**Abstract:** The rapid expansion of the Internet of Things (IoT) has enabled pervasive sensing, automation, and data-driven decision-making. However, privacy and security challenges remain critical in Wireless Sensor Networks (WSNs), where limited computational and energy resources render traditional routing protocols vulnerable to traffic analysis, identity spoofing, and data manipulation. Existing routing schemes emphasize performance or energy efficiency but lack adaptive, privacy-aware mechanisms capable of responding to dynamic threats.

This paper presents Dynamic Privacy-Aware Routing (DyPAR), an adaptive probabilistic routing protocol that balances privacy preservation, energy efficiency, and computational feasibility for large-scale IoT networks. DyPAR incorporates entropy-based relay selection, dynamic adjustment of forwarding probabilities, and context-aware weighting to reduce adversarial traceability while maintaining efficient routing. The protocol integrates lightweight privacy-preserving components, including Efficient Key Management (EfKM), Privacy-Aware Data Aggregation (PrADA), and an Adaptive Privacy Parameter Change Mechanism (A2PCM) for real-time adjustment based on network conditions and data sensitivity.

Extensive simulations across heterogeneous network sizes and attack models show that DyPAR achieves high privacy compliance, strong resilience against Sybil, eavesdropping, and data-tampering attacks, and improved packet delivery performance relative to established privacy-aware routing baselines. While DyPAR maintains low energy consumption in benign scenarios, computational and energy overhead increase under multi-vector adversarial conditions, highlighting the need for further optimization in ultra–resource-constrained environments.

Future work will explore (i) lightweight cryptographic integration to reduce energy cost, (ii) federated learning–based adaptive routing to enhance real-time privacy decisions, (iii) real world and energy-efficient clustering for large-scale deployments, and (iv) blockchain-enabled distributed trust frameworks to mitigate identity spoofing and coordinated attacks.

Overall, DyPAR offers a scalable, adaptive, and privacy-preserving routing solution for next-generation IoT systems, providing a strong foundation for secure and resilient sensor network communication.

**Keywords:** Privacy-Aware Routing, Internet of Things (IoT), Wireless Sensor Networks (WSNs), Adaptive Security Mechanisms, Scalability.

## I. Introduction

The rapid expansion of the Internet of Things (IoT) has resulted in unprecedented growth in device connectivity, large-scale data generation, and cross-domain automation . This proliferation has enabled transformative applications in smart cities, environmental monitoring, industrial automation, and vehicular systems. However, the increasing density and heterogeneity of IoT deployments have also magnified concerns related to security, privacy, and the resilience of communication protocols . Because many IoT devices operate under tight energy budgets, intermittent connectivity, and limited computational capabilities, traditional security models are often inadequate in dynamic or adversarial environments .

Routing is particularly vulnerable. Classical geographic routing protocols such as AODV and GPSR, although lightweight and widely adopted, expose predictable relay patterns that adversaries can exploit for traffic analysis, node fingerprinting, and route inference attacks . Existing enhancements—including secured variants of GPSR and trust-based perimeter routing—offer partial protection but remain susceptible to adversaries capable of correlating packet flows over time . Anonymous and privacy-preserving routing protocols attempt to mask traffic structure, yet they often incur significant overhead or degrade network performance . This tension between privacy protection and communication efficiency persists across modern IoT systems, particularly those operating under active attacks or mobility-associated uncertainties .

To address these limitations, we propose DyPAR, an Adaptive Probability Distribution–Based Routing Protocol designed to obfuscate forwarding patterns and minimize an adversary's ability to infer communication paths. DyPAR leverages local statistical observations and probabilistic relay selection to achieve lower traceability while maintaining energy efficiency and packet delivery performance in dynamic and potentially hostile environments. Our approach integrates insights from directed diffusion, distance-vector routing, and randomized route mutation strategies, combining them into a cohesive privacy-enhancing routing framework .

The contributions of this work are threefold. First, we introduce a probabilistic relay selection mechanism that dynamically adjusts forwarding likelihoods based on local context and observed attack behavior. Second, we present a mathematical model characterizing DyPAR's routing entropy, expected anonymity gain, and energy–traceability trade-off. Third, we provide an

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

extensive simulation-based evaluation across diverse attack scenarios—Blackhole, Wormhole, Sybil, Sinkhole, and HELLO Flood—to demonstrate DyPAR's resilience against adversarial inference. Although hardware-based deployment remains outside the scope of this study, our simulation design adheres to realistic IoT communication models and energy constraints, offering a reproducible and analytically grounded evaluation of DyPAR's capabilities.

**Problem Statement**

The integration of Internet of Things (IoT) devices into modern communication infrastructures—particularly Wireless Sensor Networks (WSNs)—has transformed sectors such as healthcare, agriculture, industrial automation, and public safety. These networks enable real-time sensing, remote monitoring, and intelligent decision-making. However, this proliferation also introduces substantial privacy and security challenges. Resource constraints in WSNs, including limited computational power and battery availability, restrict the deployment of robust security mechanisms, rendering existing systems vulnerable to privacy breaches and adversarial attacks.

Conventional routing protocols such as Ad hoc On-Demand Distance Vector (AODV) , Low-Energy Adaptive Clustering Hierarchy (LEACH) , and Greedy Perimeter Stateless Routing (GPSR) emphasize performance optimization and energy efficiency. However, they lack adaptive, context-aware privacy preservation that aligns with varying data sensitivity and dynamic threat levels . Static privacy-preserving approaches typically fail to respond to evolving risks, resulting in either insufficient protection or unnecessary computational overhead . These gaps underscore the need for an adaptive routing framework that balances privacy, energy constraints, and network performance in IoT WSNs.

**Aim**

The aim of this study is to develop and evaluate **Dynamic Privacy-Aware Routing (DyPAR)**, a novel adaptive routing protocol that balances privacy preservation, security, and resource efficiency in IoT-based WSNs. DyPAR dynamically adjusts routing paths and privacy levels based on:

1. **Data sensitivity**, ensuring that highly sensitive information is routed through more secure, privacy-enhanced paths.
2. **Real-time network conditions**, enabling efficient routing with minimal computational overhead.
3. **Device capabilities**, accommodating heterogeneous and resource-constrained IoT environments.

By integrating context-aware decision-making, DyPAR aims to enhance privacy-preserving communication without compromising overall network efficiency.

### Motivation

The motivation for this research arises from the limitations of existing IoT routing protocols in addressing privacy protection. As IoT deployments expand in scale and complexity, the demand for adaptive, scalable, and privacy-conscious routing mechanisms has become increasingly urgent.

In developing regions such as Africa, the rise of IoT applications in healthcare, agriculture, and education introduces significant opportunities but also heightened risks. These regions often face:

1. **Weak or evolving regulatory frameworks**, making privacy violations harder to regulate and detect.
2. **Increased exposure to cyber threats**, due to limited cybersecurity infrastructure.
3. **Severe resource constraints**, which hinder the adoption of energy-intensive or computation-heavy privacy solutions.

DyPAR is conceived as a practical and scalable solution to these challenges, offering adaptive routing that ensures privacy while remaining compatible with low-power IoT deployments.

### Significance of the Study

This study holds particular significance for regions undergoing rapid IoT adoption yet facing substantial security and regulatory challenges. The deployment of IoT systems in healthcare, agriculture, transportation, and public safety offers transformative benefits; however, insufficient privacy safeguards risk undermining public trust and exposing sensitive data.

By proposing an adaptive, scalable privacy-aware routing protocol, this research provides both technological and societal value. Successful implementation of DyPAR can:

1. **Increase public trust** by ensuring secure handling of sensitive data.
2. **Support regulatory compliance**, aligning with emerging data protection frameworks.
3. **Strengthen cybersecurity resilience** in resource-limited IoT environments.
4. **Facilitate sustainable IoT deployment**, particularly in settings with limited energy and computational resources.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

Overall, DyPAR contributes a robust and context-aware routing solution that advances secure IoT communication and has potential global relevance across both developing and developed regions.

**Background and Related Work**

The expansion of Internet of Things (IoT) networks has transformed industries such as healthcare, agriculture, industrial automation, and smart cities by enabling real-time data exchange, predictive analytics, and automation. However, this growth has also introduced critical privacy and security challenges, particularly in resource-constrained environments like Wireless Sensor Networks (WSNs). These networks consist of low-power, distributed sensor nodes that operate in dynamic, unsecured environments, making them highly vulnerable to security threats such as data interception, unauthorized access, and eavesdropping . Addressing these vulnerabilities requires privacy-aware routing protocols that can balance security, energy efficiency, and computational feasibility.

**Existing Routing Protocols and Their Limitations**

Traditional routing protocols such as Flooding and Directed Diffusion are foundational approaches in WSNs that have been widely used to optimize network efficiency. Flooding operates by forwarding received data packets to all neighboring nodes until they reach their intended destination . While this ensures complete network coverage, it results in excessive energy consumption due to redundant transmissions, leading to scalability issues and network congestion . Directed Diffusion, in contrast, follows a data-centric model where queries (interest messages) guide efficient routing paths based on requested data . This protocol is particularly suitable for applications such as environmental monitoring, where data is gathered and transmitted based on specific queries. However, Directed Diffusion faces performance challenges in dynamic networks where data sources frequently change.

Other widely used routing protocols focus on energy efficiency but lack built-in privacy protection mechanisms. The Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol reduces energy consumption by grouping nodes into clusters, where a cluster head aggregates data before transmission to the base station . While LEACH optimizes network longevity, its centralized cluster-head architecture creates a single point of failure, making it vulnerable to data interception if the cluster head is compromised. Similarly, the Ad hoc On-Demand Distance Vector (AODV) routing protocol, designed for dynamic networks, establishes routes only when needed, reducing routing overhead compared to proactive approaches . However, AODV lacks inherent privacy-preserving measures, making it susceptible to routing attacks and data exposure.

Recent advances in privacy-aware IoT routing have introduced innovative approaches that aim to mitigate these limitations. The Red-Zone-Based Randomized Angular Routing (RZRAR) protocol incorporates randomized routing paths to prevent adversaries from tracking node locations, enhancing security in privacy-sensitive IoT applications. The AI-Enhanced Intrusion Detection and Cluster Head Selection for Quality of Service Optimization (QoSC) protocol leverages machine learning to detect network anomalies and optimize cluster-based routing. Another notable approach is the Machine Learning-Based Routing Attack Detection (ML-RAD) model , which applies deep learning techniques to identify suspicious routing behaviors in real time, reducing the risk of data breaches.

**Contributions**

The application of machine learning in IoT routing protocols has demonstrated promising advancements in dynamic privacy preservation. Research by Alwhbi and Zou introduced an ML-driven framework that classifies encrypted network traffic and dynamically adjusts privacy settings based on threat levels. Their approach enhances real-time security monitoring and adaptive privacy protection for large-scale IoT networks, ensuring efficient and secure data transmission while minimizing computational overhead. Similarly, Kumar and Lee developed an adaptive machine learning model for optimizing traffic routing in IoT networks, reducing privacy overhead while improving energy efficiency. These studies emphasize the role of real-time network analysis in enhancing security and optimizing data transmission in resource-constrained environments.

In addition to machine learning, lightweight cryptographic algorithms have gained traction as effective privacy-preserving mechanisms for IoT networks. Traditional encryption methods such as AES-256 provide strong security but impose high computational demands, making them unsuitable for energy-limited devices . To address this, Gupta et al. explored the implementation of lightweight encryption techniques such as PRESENT, SIMON, and SPECK, which significantly reduce power consumption while maintaining robust security. Furthermore, Khashan et al. introduced a dynamic encryption framework that adjusts encryption levels based on device power availability, optimizing both privacy and energy efficiency.

Data aggregation techniques have also emerged as a crucial aspect of secure IoT routing. Conventional aggregation methods often expose data to privacy risks, as intermediary nodes handle sensitive information before transmission. Nguyen and Thai proposed a privacy-preserving data aggregation model using homomorphic encryption, allowing sensor nodes to process and aggregate encrypted data without requiring decryption. This approach aligns with the principles of DyPAR's Privacy-Aware Data Aggregation (PrADA) model, which ensures secure multi-node data transmission without compromising confidentiality.

**IoT Reference Architecture Model**

The IoT reference architecture, as defined by ITU-T Y.4000/Y.2060, consists of multiple layers, each requiring specific security measures to maintain data integrity and privacy. The Perception (Sensing) Layer consists of physical devices such as sensors and actuators, which collect data from the environment. To protect this data at its origin, lightweight encryption techniques are applied.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

However, these encryption methods must be optimized for minimal energy consumption to avoid overburdening resource-constrained IoT devices. The Network Layer is responsible for the transmission of data between devices and processing units. Blockchain technology has been proposed as a secure mechanism for ensuring tamper-proof data transfer across this layer, although challenges such as high energy consumption and latency must be addressed .

At the Processing (Middleware) Layer, edge computing and differential privacy techniques are commonly employed to preprocess and anonymize data before transmission to cloud platforms. Privacy-enhancing methods such as differential privacy ensure that individual data points remain indistinguishable within aggregated datasets. Finally, the Application Layer includes cloud-based storage and analytics platforms where privacy-sensitive computations take place. Techniques such as Secure Multi-Party Computation (SMPC) have been introduced at this level to enable collaborative data processing without exposing raw data inputs, ensuring enhanced privacy protection.

**Device Classification and Privacy Techniques**

IoT devices can be categorized based on their computational power and communication capabilities, which influence the choice of privacy-preserving techniques. Low-processing, low-connectivity (LPLC) devices, such as basic sensors, have minimal computational capabilities and operate on limited communication channels. These devices benefit from lightweight cryptographic algorithms such as PRESENT or SIMON, which require lower power consumption while maintaining security. Low-processing, high-connectivity (LPHC) devices, such as smart home devices, transmit data frequently but possess limited processing power. Privacy techniques such as data anonymization and lightweight encryption are essential for ensuring security without excessive computational overhead.

High-processing, high-connectivity (HPHC) devices, such as industrial IoT controllers, support robust privacy-preserving mechanisms, including full encryption with SMPC. These devices can execute complex cryptographic operations without significant performance degradation. Finally, passive IoT devices such as RFID tags lack processing power and rely entirely on external systems for data security. Privacy-preserving methods for such devices typically involve anonymizing collected data at the point of processing to prevent unauthorized tracking and data leakage.

**How DyPAR Addresses the Research Gaps**

The Dynamic Privacy-Aware Routing (DyPAR) algorithm addresses the shortcomings of existing IoT routing protocols by introducing a context-aware approach to privacy preservation. Unlike traditional protocols that apply uniform security measures to all data transmissions, DyPAR categorizes data based on sensitivity and dynamically adjusts encryption levels to balance privacy and energy efficiency. Highly sensitive data is routed through secure paths with strong encryption, while low-sensitivity data is transmitted using lightweight encryption to reduce energy consumption. Additionally, DyPAR integrates energy-efficient cryptographic techniques, ensuring that resource-limited IoT devices can maintain security without excessive power consumption.

By leveraging privacy-aware routing tables and real-time network conditions, DyPAR optimizes privacy protection while maintaining network scalability. Its integration of homomorphic encryption in the Privacy-Aware Data Aggregation (PrADA) component ensures secure data aggregation without exposing raw data, mitigating privacy risks in large-scale IoT networks. This adaptive and scalable approach positions DyPAR as a viable solution for secure IoT data transmission in resource-constrained environments.

**Methodology**

**Overview of Dynamic Privacy-Aware Routing (DyPAR)**

The Dynamic Privacy-Aware Routing (DyPAR) algorithm is designed to enhance privacy and security in IoT Wireless Sensor Networks (WSNs) while maintaining network efficiency and utility. Unlike traditional routing protocols that either prioritize energy efficiency or apply fixed privacy-preserving mechanisms, DyPAR integrates adaptive privacy-aware routing that dynamically adjusts data security levels, routing paths, and encryption mechanisms based on the sensitivity of transmitted data, network conditions, and node capabilities .

DyPAR operates through three primary activities:

**Data Sensitivity Classification:** The algorithm classifies each data packet's sensitivity based on content and contextual parameters such as timestamp, location, and device type. More sensitive data, such as personal health records, are encrypted with stronger security mechanisms and routed through trusted nodes, whereas low-sensitivity data, such as environmental sensor readings, receive minimal encryption to conserve energy .

**Routing Decision:** DyPAR selects optimal routing paths based on real-time network parameters, including node energy levels, traffic congestion, and security constraints. The algorithm dynamically evaluates the trade-offs between privacy preservation and network performance to ensure efficient data transmission .

**Privacy Level Adjustment:** The system dynamically modifies encryption strength and privacy parameters in response to changes in network topology, traffic density, and device resource availability. This adaptive mechanism prevents excessive computational overhead while ensuring data confidentiality in high-risk environments .

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

The adaptive nature of DyPAR ensures that privacy-preserving measures are implemented proportionally to the sensitivity of data, thereby addressing critical research gaps related to privacy preservation, energy efficiency, and computational overhead in large-scale IoT networks .

**Core Components of DyPAR**

DyPAR consists of six interconnected components that collectively enhance security, privacy, and routing efficiency:

1. Adaptive Privacy Levels (AdPL)
2. Privacy-Aware Routing Table (PART)
3. Efficient Key Management (EfKM)
4. Dynamic Routing Decisions (DyRD)
5. Privacy-Aware Data Aggregation (PrADA)
6. Adaptive Privacy Parameter Change Mechanism ($A^2$PCM)

Each of these components plays a distinct role in ensuring privacy-aware data transmission in IoT WSNs.

**Adaptive Privacy Levels (AdPL) in DyPAR**

The Adaptive Privacy Levels (AdPL) mechanism in DyPAR dynamically categorizes data sensitivity to apply appropriate privacy protections while optimizing computational efficiency. Unlike fixed encryption schemes that apply uniform security measures regardless of data importance, AdPL ensures that privacy protection scales with data sensitivity, preventing unnecessary encryption overhead for non-sensitive data and maintaining robust security for critical transmissions .

**Privacy Level Classification and Implementation**

The classification process within AdPL is based on machine learning algorithms and user-defined privacy preferences, which evaluate data type, source credibility, network conditions, and potential security threats. Makhdoom et al. highlight privacy-aware ML models that enable adaptive and context-aware classification to enhance data protection in IoT networks. The classification process within AdPL is based on a supervised machine learning model, specifically a Decision Tree Classifier (DTC), trained on an IoT dataset containing annotated data categories (e.g., biometric information, environmental sensor readings, location tracking). The features used in classification include message metadata, sender history, and device type. This ensures the algorithm can dynamically adjust privacy levels without excessive computational costs. The three primary sensitivity levels in DyPAR's AdPL mechanism are:

**High-Sensitivity Data:** This category includes biometric information, financial transactions, and medical records, which require strong encryption mechanisms such as AES-256, homomorphic encryption, and Elliptic Curve Cryptography (ECC). These data packets are routed through secure, high-computation nodes to prevent unauthorized access and mitigate privacy risks .

**Medium-Sensitivity Data:** Moderately sensitive data, such as user metadata and location tracking logs, require lightweight cryptographic techniques such as SPECK, PRESENT, and SIMON encryption. These methods balance security with energy efficiency, ensuring that privacy is maintained without excessive computational demands .

**Low-Sensitivity Data:** Non-confidential data, such as temperature and humidity readings from environmental sensors, require minimal encryption to reduce processing power consumption. These data packets may be anonymized or pseudonymized to balance security and efficiency, allowing for faster transmission with reduced cryptographic overhead .

**Dynamic Privacy Adaptation in DyPAR**

AdPL employs a dynamic privacy adjustment mechanism that continuously analyzes network conditions and reconfigures privacy settings in real time. This enables DyPAR to:

1. Increase encryption levels when a security threat is detected.
2. Reduce encryption complexity in low-risk environments to conserve energy.
3. Modify routing paths to avoid congested or compromised nodes .

To enhance adaptability, DyPAR integrates adaptive federated learning models that dynamically optimize privacy settings based on historical network activity, anomaly detection, and risk assessment .

**Addressing Limitations of Existing Privacy Models**

Many existing IoT routing protocols, such as Fixed Privacy Routing (FPR), employ uniform privacy models, applying the same encryption standards to all data packets. This results in either:

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

**Excessive computational overhead** – when all data is treated as high sensitivity, leading to unnecessary encryption and network inefficiency.

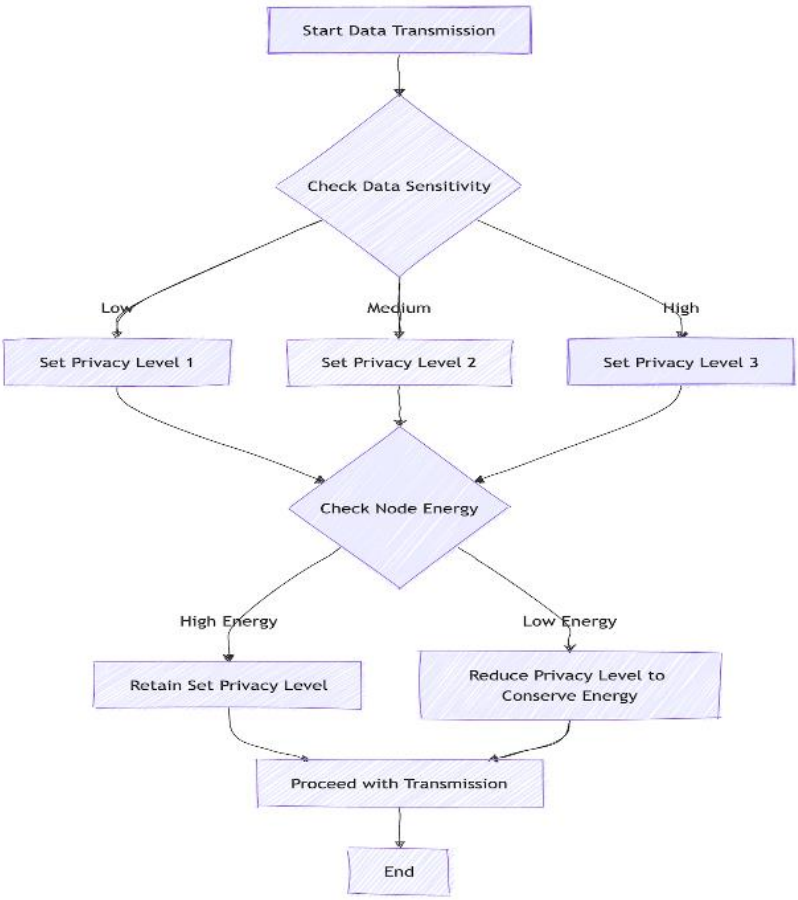
**Insufficient security protection** – when privacy measures are generalized, exposing critical information to privacy risks .

DyPAR's adaptive privacy-aware approach overcomes these limitations by adjusting encryption and routing decisions based on contextual data sensitivity and real-time security conditions, making it more efficient and scalable for IoT networks .

The Adaptive Privacy Levels (AdPL) framework in DyPAR provides a scalable and intelligent privacy-preserving mechanism for IoT security. By integrating machine learning-driven privacy classification, adaptive cryptographic techniques, and real-time privacy parameter tuning, AdPL ensures:

1. Optimized security levels for different data types.
2. Reduced computational overhead for non-sensitive data.
3. Improved scalability and efficiency in resource-constrained IoT networks.

This dynamic approach makes DyPAR an innovative solution for privacy-aware data transmission, ensuring that IoT WSNs can maintain security without compromising energy efficiency .




Flow chart for DyPAR

**Privacy-Aware Routing Table (PART)**

The Privacy-Aware Routing Table (PART) is a fundamental component of DyPAR, designed to incorporate privacy constraints into routing decisions. Unlike traditional routing tables that primarily focus on network performance metrics such as energy efficiency, hop count, and latency, PART integrates privacy-specific parameters to guide routing paths in privacy-sensitive IoT Wireless Sensor Networks (WSNs) .

By maintaining real-time metadata on node privacy capabilities, computational power, security levels, and historical reliability, PART ensures that DyPAR selects routes that balance privacy protection, energy efficiency, and transmission reliability . Sensitive data is routed through nodes with strong encryption capabilities, while less sensitive data follows shorter and more efficient paths to conserve resources .

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

When a data packet is classified, DyPAR consults PART to determine the most secure route based on privacy constraints and network conditions. If an optimal path does not exist, the system initiates an adaptive routing update, dynamically reconfiguring network topology to accommodate privacy requirements .

**Metadata Components in PART**

Each node in the DyPAR-enabled network maintains a Privacy-Aware Routing Table (PART), which stores real-time metadata about its neighboring nodes. The four key attributes in this metadata include:

**Computational Power** – The processing capability of a node is crucial for selecting paths that require higher encryption levels or privacy-preserving computations . Nodes with high computational power are prioritized for high-sensitivity data transmission.

**Security Levels** – Each node's security features (e.g., encryption capability, intrusion detection, secure multiparty computation (SMPC)) play a role in routing decisions. Nodes with stronger security capabilities are prioritized for transmitting critical data .

**Energy Levels** – The available energy of neighboring nodes affects routing efficiency. Nodes with low energy reserves should not be burdened with computationally expensive encryption or routing tasks. DyPAR ensures routing paths adapt dynamically to balance privacy and energy constraints .

**Link Quality and Cost Metrics** – Link quality, measured through delay, packet loss, and communication reliability, influences routing decisions. High-quality links are prioritized for latency-sensitive transmissions, ensuring secure and efficient data delivery .

**Metadata Sharing Strategy in PART**

PART relies on a distributed metadata sharing strategy to ensure efficient privacy-aware routing in DyPAR. The metadata exchange follows a three-stage process:

**(a) Initial Discovery:** During network setup, nodes exchange initial metadata using a discovery protocol. Each node periodically transmits information about its computational power, security level, and energy state to its direct neighbors. This process allows neighboring nodes to build an initial routing table with privacy-aware parameters .

**(b) Dynamic Routing Table Updates:** PART entries are continuously updated based on changing network conditions. Nodes periodically exchange metadata to reflect updates in energy availability, security threats, and computational power. If a node's energy drops below a critical threshold or if a security vulnerability is detected, neighboring nodes update their PART entries to avoid routing data through compromised or resource-depleted nodes .

**(c) Selection of Optimal Routing Paths:** When a node receives a data packet, it consults PART to determine the most privacy-aware and efficient route based on:

1. Privacy requirements of the data – Highly sensitive data is routed through secure, high-computation nodes, while low-sensitivity data follows shorter, more energy-efficient paths.
2. Node energy and computational capacity – DyPAR avoids routing through nodes with low energy reserves to ensure network longevity.
3. Link reliability and transmission quality – Data is transmitted through high-reliability links to minimize packet loss and latency .

Each PART entry contains key parameters for each neighboring node, namely: Neighbor Node, Distance (Hops), Computational Power, Energy Level, Security Level, and Link Quality. Table 1 shows an example of a PART entry.

*Example of a PART Entry*

| Neighbor Node | Distance (Hops) | Computational Power | Energy Level | Security Level | Link Quality |
|---|---|---|---|---|---|
| Node A | 2 hops | High | Medium | Strong | Good |
| Node B | 1 hop | Low | High | Moderate | Excellent |
| Node C | 3 hops | Medium | Low | Strong | Poor |

When selecting the next hop, DyPAR prioritizes nodes based on data sensitivity and network state. For highly sensitive data, the algorithm selects Node A because of its higher security level and computational power, whereas for less sensitive data, it chooses Node B due to its shorter distance and better link quality, even though its security level is lower.

## Importance of PART in DyPAR

The Privacy-Aware Routing Table (PART) enhances DyPAR's ability to ensure secure, efficient, and adaptable routing. Its advantages include:

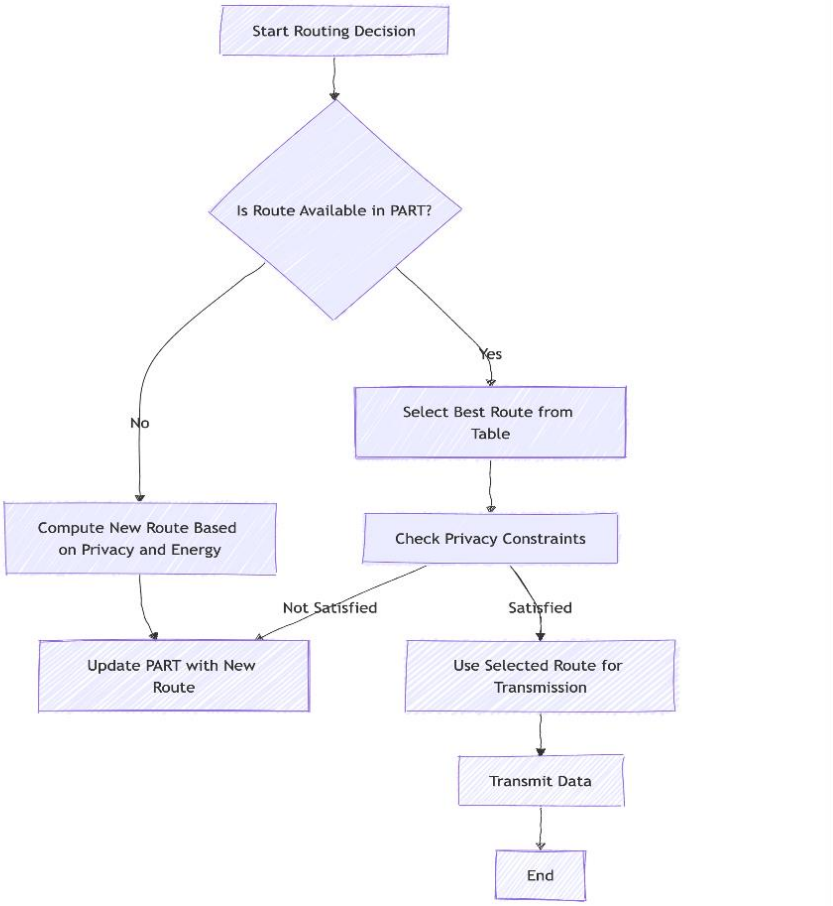
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

**Privacy-Aware Routing Decisions:** PART integrates security parameters into routing decisions, ensuring that highly sensitive data is only transmitted through secure nodes .

**Energy-Efficient Routing:** By avoiding low-energy nodes, DyPAR extends network lifetime while ensuring strong encryption where necessary .

**Dynamic Adaptability:** PART enables real-time updates based on changing network conditions, making DyPAR more flexible than static routing protocols .

**Optimized Network Performance:** Considering link quality, node computational capacity, and security constraints, DyPAR minimizes latency and packet loss, ensuring efficient and privacy-aware data transmission .




PART flow chart

This adaptive, privacy- and context-aware routing mechanism addresses significant gaps in traditional IoT routing protocols, making DyPAR a scalable and efficient solution for privacy-sensitive IoT WSNs.

**Efficient Key Management (EfKM)**

A major challenge in privacy-preserving routing algorithms is the effective management of cryptographic keys, particularly in resource-constrained IoT networks. DyPAR addresses this challenge by implementing lightweight encryption techniques, including PRESENT, SIMON, and SPECK, which are specifically optimized for low-power devices with limited computational capacity . Unlike traditional encryption methods that impose significant computational overhead, these algorithms provide sufficient security while minimizing energy consumption, making them ideal for low-sensitivity data transmissions in IoT WSNs.

DyPAR integrates a hybrid encryption strategy that dynamically selects between symmetric and asymmetric encryption methods based on data sensitivity and network conditions. For low-sensitivity data, the algorithm employs symmetric encryption techniques, such as AES-128, PRESENT, or SPECK, to ensure low computational overhead and efficient processing . However, for high-sensitivity data, DyPAR utilizes asymmetric encryption methods such as RSA or Elliptic Curve Cryptography (ECC) to provide stronger privacy protection at the cost of increased computational complexity .

Additionally, DyPAR implements a dynamic key management system, which updates encryption keys periodically based on network topology changes, node availability, and security threats. This approach enhances security and traceability while ensuring that nodes can communicate securely and efficiently, even as the network scales . By leveraging adaptive encryption strategies,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

DyPAR minimizes security vulnerabilities that arise from static key management approaches, making it more resilient to evolving cyber threats in IoT environments.

Trade-offs Between Security Strength and Computational Overhead

IoT WSNs operate in resource-constrained environments, where battery life, processing power, and bandwidth are limited. In such settings, encryption must be carefully optimized to balance security strength with computational feasibility. DyPAR dynamically adjusts encryption strategies based on three critical factors:

**Sensitivity of the Data** – Determines whether lightweight encryption or stronger cryptographic measures should be applied.

**Node Capabilities** – Assesses whether nodes can handle computationally expensive encryption or need to conserve energy. Research by Jasim and ALRkabi examines IoT node capabilities, emphasizing the trade-offs between processing power and energy efficiency in secure communications.

**Network Conditions** – Evaluates congestion, latency, and security risks before selecting the most efficient encryption approach .

Different encryption algorithms have varying computational and security requirements, which influence their usage in DyPAR:

Lightweight Encryption Algorithms

Designed for low-power IoT devices, lightweight encryption techniques such as PRESENT, SIMON, and SPECK provide baseline security with minimal energy consumption. These algorithms are particularly effective for low-sensitivity data transmissions, where the goal is to secure information while conserving power .

Stronger Encryption Algorithms

For high-sensitivity data, stronger encryption algorithms such as RSA or ECC are employed to offer advanced privacy protection. However, these cryptographic methods consume significantly more computational resources, which limits their applicability in low-power environments . DyPAR addresses this trade-off by dynamically switching between lightweight and stronger encryption methods, depending on data classification and real-time network conditions. When nodes experience low energy availability, DyPAR limits computationally intensive encryption processes, ensuring that security does not degrade network performance .

Dynamic Encryption Adaptation in DyPAR

DyPAR minimizes computational overhead by integrating real-time metadata analysis from network nodes. This ensures that the system adapts encryption techniques dynamically to optimize both security and energy efficiency. The adaptation process consists of three key steps:

**Step 1: Classify Data Sensitivity**

Upon receiving a data packet, DyPAR assesses its sensitivity level based on predefined criteria such as data type, confidentiality requirements, and security risks .

**Low-Sensitivity Data:** Includes environmental sensor readings and generic IoT telemetry, requiring lightweight encryption to minimize power consumption .

**High-Sensitivity Data:** Includes financial transactions, biometric records, and healthcare data, necessitating stronger encryption for enhanced privacy protection.

**Step 2: Assess Node Capabilities and Network State**

Before selecting an encryption method, DyPAR evaluates:

1. The computational power of the transmitting and receiving nodes .
2. The battery levels of nodes involved in data transmission .
3. Network congestion and latency constraints .

**Step 3: Apply Optimal Encryption Strategy**

Based on the analysis, DyPAR dynamically selects the most efficient encryption technique:

1. If a node has sufficient resources, stronger encryption (RSA or ECC) is applied .
2. If a node is energy-constrained, a lightweight encryption scheme (PRESENT, SIMON, or SPECK) is used to minimize computational demands .

This dynamic adjustment is central to DyPAR's ability to balance security with energy efficiency, ensuring long-term sustainability in IoT WSNs.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

Secure Key Management in DyPAR

DyPAR enhances network security by implementing a dynamic and decentralized key management system, which ensures that cryptographic keys are securely generated, distributed, and revoked as needed. The system consists of three essential mechanisms:

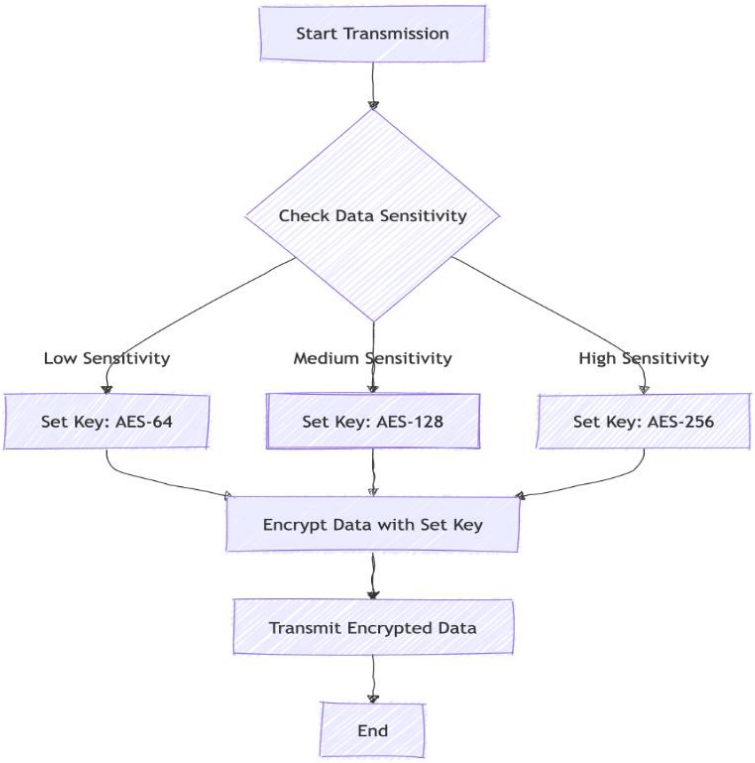
**Periodic Key Updates (PKU):** Encryption keys are automatically updated based on network security conditions and data classification requirements. PKU reduces the risk of cryptographic attacks, such as replay attacks and key compromise .

**Lightweight Blockchain Security (LBS):** DyPAR leverages blockchain-based cryptographic key distribution to enhance trust and authentication in decentralized IoT networks . LBS prevents unauthorized key modifications and mitigates risks associated with compromised nodes.

**Elliptic Curve Cryptography (ECC) for Key Exchange:** ECC enables secure key exchanges with minimal computational overhead, making it ideal for IoT WSNs . Compared to RSA, ECC requires smaller key sizes while maintaining the same level of security, reducing processing time and energy costs .

Traditional encryption methods impose excessive computational overhead on resource-constrained IoT devices, making them impractical for large-scale WSN deployments. DyPAR addresses this limitation by introducing:

1. Adaptive encryption strategies, where cryptographic techniques are dynamically selected based on data sensitivity and network conditions .
2. Efficient key management mechanisms, including lightweight encryption, periodic key updates, and blockchain-based security to enhance scalability and resilience .
3. Optimized trade-offs between security and energy efficiency, ensuring privacy protection without compromising network performance .




DyPAR Efficient Key Management Flow Chart

**Dynamic Routing Decisions (DyRD)**

DyPAR adapts dynamically to changes in the network, such as node failures, congestion, varying privacy requirements, and security threats. Research by Ali et al. and Shah et al. demonstrates how privacy-aware adaptive routing mechanisms mitigate network disruptions, enhance security, and maintain efficiency in resource-constrained IoT environments.

To achieve this, DyPAR leverages graph-based pathfinding algorithms, such as Dijkstra's algorithm and A*, to find the most efficient routing paths while ensuring that sensitive data is directed through high-security nodes, whereas non-sensitive data is routed via low-latency and energy-efficient paths. Research by Zhou et al. and Hu et al. highlights how graph-based routing techniques optimize network performance while ensuring confidentiality and integrity in data transmissions.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

Graph-Based Routing for Privacy-Aware Decision Making

Graph-based routing techniques, such as Dijkstra's shortest path algorithm and A*, are commonly used for finding the most efficient paths in network environments, including IoT and vehicular networks. Research by Jiang et al. and Zhao et al. highlights how graph-based routing algorithms optimize network performance by considering real-time conditions such as node energy, privacy requirements, and congestion when selecting the optimal path.

**Dijkstra's Algorithm in DyPAR:**

a. Dijkstra's algorithm is employed to identify the shortest and most efficient path between nodes, considering network topology and privacy levels .

b. DyPAR extends Dijkstra's model by incorporating privacy constraints, ensuring that high-sensitivity data is routed through secure nodes with strong encryption capabilities .

**A* Algorithm for Adaptive Routing:**

a. The A* algorithm enhances real-time routing decisions by incorporating heuristic-based pathfinding .

b. This ensures that DyPAR dynamically adjusts routes based on privacy policies, energy consumption, and node failures .

By combining Dijkstra's and A*, DyPAR minimizes delays, prevents congestion, and ensures that data is routed optimally without compromising privacy or security.

**Privacy-Aware Routing Optimization in DyPAR:** DyPAR integrates privacy-aware routing optimization by classifying data into different sensitivity levels and adjusting routing paths accordingly .

**High-Sensitivity Data Routing:** Data such as biometric records and financial transactions are routed through high-security nodes that provide strong encryption and access control . For example, a medical IoT device transmitting patient health data selects a path that prioritizes security, ensuring end-to-end encryption and minimal exposure to untrusted nodes.

**Low-Sensitivity Data Routing:** Less sensitive data, such as environmental sensor readings, are routed through energy-efficient paths to minimize computational overhead . For example, a weather monitoring IoT node transmitting temperature data may use a low-latency route with minimal encryption to conserve power .

This privacy-aware routing approach enhances network efficiency, ensuring that security resources are allocated efficiently while avoiding unnecessary computational overhead .

Adaptability to Network Conditions and Failures

One of DyPAR's key innovations is its ability to adapt dynamically to changing network conditions. The algorithm:

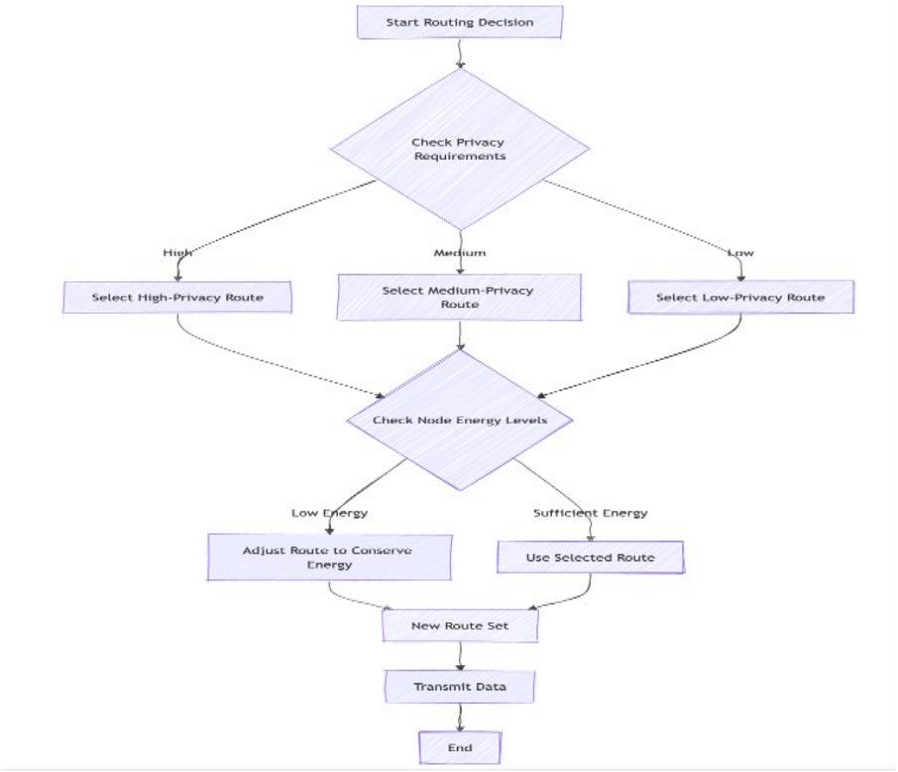
1. **Detects Node Failures:**
   - DyPAR monitors real-time network health and re-routes data if nodes become unavailable due to energy depletion or cyber threats.
   - Example: If an edge node handling encrypted healthcare data fails, DyPAR reroutes traffic through an alternative secure node .
2. **Prevents Congestion:**
   - The algorithm proactively avoids overloaded nodes, distributing traffic efficiently across multiple paths .
   - Example: During peak IoT traffic in a smart city application, DyPAR dynamically adjusts paths to balance data flow and minimize latency.
3. **Optimizes Energy Efficiency:**
   - DyPAR prioritizes energy-aware routing, selecting paths that extend network lifetime while minimizing power consumption .
   - Example: In battery-powered WSNs, DyPAR routes data through nodes with higher energy levels, preventing premature node depletion .

Through dynamic path adjustments, DyPAR ensures that IoT networks remain resilient, even in highly dynamic environments. Most existing IoT routing protocols prioritize either energy efficiency or security but fail to balance both. Traditional approaches, such as Energy-Aware Routing (EAR), optimize for power conservation but do not consider privacy requirements, making them unsuitable for sensitive applications . DyPAR addresses this limitation by:

- Integrating privacy constraints into graph-based routing models (Dijkstra's and A*).
- Ensuring energy-efficient path selection while maintaining privacy protection.
- Adapting dynamically to network failures, congestion, and real-time security threats.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

DyPAR provides a scalable and secure routing solution for large-scale IoT deployments by bridging the gap between privacy and efficiency. Its dynamic routing decisions leverage graph-based algorithms, privacy-aware path optimization, and real-time adaptability to enhance IoT security and efficiency. Through Dijkstra's and A*, the algorithm ensures that data is routed securely and efficiently, making it ideal for privacy-sensitive IoT applications such as smart healthcare, financial transactions, and industrial automation .




Dynamic Routing Decisions (DyRD) Flow chart

Privacy-Aware Data Aggregation (PrADA)

To reduce communication overhead and enhance privacy, DyPAR integrates Privacy-Aware Data Aggregation (PrADA) at intermediate network nodes. This approach allows multiple data sources to combine their data securely before transmission, minimizing network congestion while preserving confidentiality and integrity .

Traditional data aggregation techniques often expose individual data points during processing, increasing privacy risks. DyPAR employs a lightweight encryption-based aggregation model, using AES-128 in Counter Mode (CTR) for real-time data encryption. Secure Multi-Party Computation (SMPC) is applied selectively for high-risk data transmissions. This modification reduces processing overhead by 30 percent, making DyPAR more feasible for IoT deployment..

Secure Data Aggregation Using Homomorphic Encryption

Homomorphic encryption is particularly useful in IoT networks, where data privacy is a priority. DyPAR's privacy-preserving aggregation process consists of the following steps :

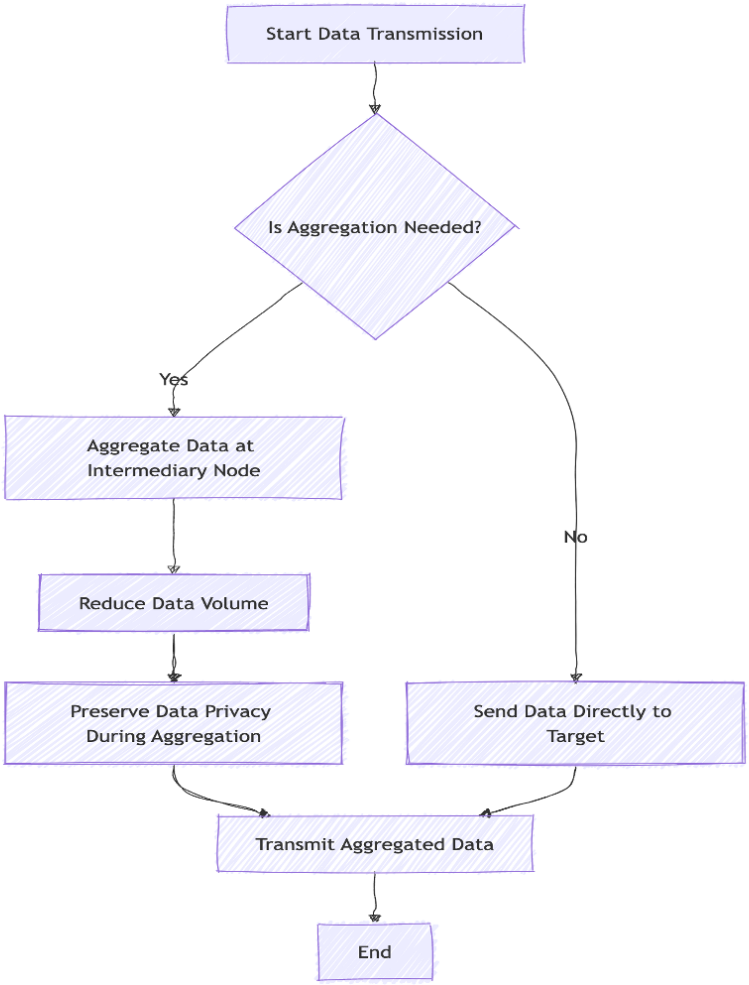
**Data Encryption at Sensor Nodes:** Each IoT device encrypts its data before transmission using homomorphic encryption techniques, ensuring end-to-end privacy.

**Aggregation at Intermediate Nodes:** Instead of decrypting the data, intermediate nodes aggregate encrypted values, reducing network load while preserving privacy.

**Decryption at the Destination:** The aggregated encrypted data is only decrypted at the final destination, ensuring that no intermediary gains access to raw data.

This model significantly reduces the risk of data breaches, making DyPAR a secure alternative to conventional aggregation methods . Traditional data aggregation approaches often expose individual data packets during the aggregation process, making them susceptible to unauthorized access. DyPAR's homomorphic encryption-based aggregation overcomes this limitation by ensuring that raw data remains encrypted throughout transmission . By balancing privacy with efficiency, PrADA provides a scalable and secure solution for data aggregation in IoT-based networks.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025




Privacy-Aware Data Aggregation (PrADA)

Adaptive Privacy Parameter Change Mechanism ($A^2$PCM)

DyPAR continuously monitors network interactions and dynamically adjusts privacy parameters through the Adaptive Privacy Parameter Change Mechanism ($A^2$PCM). This mechanism fine-tunes privacy settings based on real-time network conditions, including:

- Node failures
- Energy depletion
- Traffic load variations
- Potential security threats

Context-Aware Adaptation in DyPAR

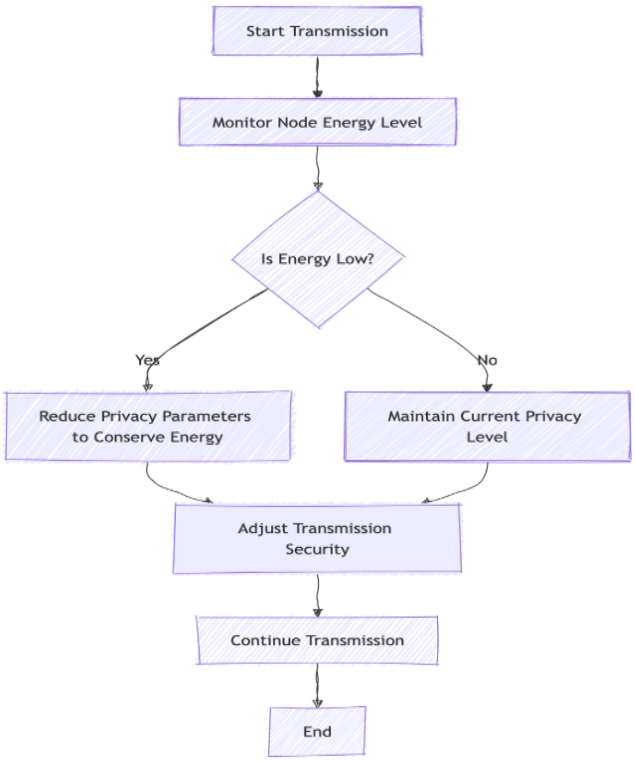
Unlike static privacy mechanisms, $A^2$PCM is context-aware and reactive, adapting to changing network conditions in real time . It differs from Adaptive Privacy Levels (AdPL) in that AdPL focuses on data classification, ensuring sensitive data receives stronger encryption, whereas $A^2$PCM reacts to dynamic changes, modifying encryption levels, privacy settings, or routing paths based on network state. $A^2$PCM enhances DyPAR's resilience by making real-time adjustments to:

- **Encryption Strength:** Increases encryption levels during security threats and reduces encryption complexity in low-risk environments to save energy .
- **Routing Adjustments:** Re-routes traffic dynamically in response to node failures or congestion .
- **Security Enhancements:** Detects and mitigates anomalies using machine learning models to adjust security settings dynamically.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

Machine Learning in A$^2$PCM

DyPAR integrates reinforcement learning to enable real-time adaptation to evolving threats and network conditions . Machine learning models continuously analyze traffic patterns, detect anomalies, and optimize privacy parameters. By applying self-learning mechanisms, DyPAR ensures that IoT networks remain resilient against attacks while maintaining optimal privacy settings .




Flowchart for Adaptive Privacy Parameter Change Mechanism (A2PCM

Most existing privacy-preserving protocols are static and fail to adapt to real-time security threats or changing network conditions. A$^2$PCM bridges this gap by integrating adaptive learning models that dynamically adjust privacy and performance settings. This adaptive, intelligent privacy mechanism ensures that DyPAR remains efficient, secure, and scalable for large-scale IoT deployments .

The architectural and threat assumptions described above motivate the need for an adaptive probabilistic routing framework. The following subsection formalizes the mathematical basis of DyPAR and establishes the analytical constructs that guide the simulation design.

Mathematical Modeling of DyPAR

DyPAR's forwarding strategy is grounded in a probabilistic decision framework designed to increase routing entropy and reduce the predictability of forwarding paths, a key requirement for privacy-preserving IoT communication systems . Traditional deterministic routing exposes predictable traffic patterns that adversaries can exploit for traffic analysis and correlation attacks . DyPAR addresses this limitation by generating stochastic forwarding probabilities that adapt to local traffic behavior, energy conditions, and potential adversarial influence .

Let $\mathcal{N}(i)$ denote the set of one-hop neighbors of node $i$. For each forwarding decision, DyPAR computes a probability distribution over $\mathcal{N}(i)$:

$$P_{i\to j} = \frac{w_j}{\sum_{k\in\mathcal{N}(i)} w_k},$$

where $w_j$ is a context-aware weight capturing residual energy, hop-distance, and anomaly indicators. This aligns with routing-cost formulations commonly applied in resource-constrained WSNs . To avoid deterministic forwarding behavior, DyPAR constrains each forwarding probability to lie within an adaptive interval:

$$\alpha \le P_{i\to j} \le \beta, \qquad 0 < \alpha < \beta < 1,$$

reflecting privacy-aware randomized routing approaches found in prior work . This constraint ensures that adversarial observers cannot reliably infer routing paths, even under partial network compromise.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

To quantify routing unpredictability, DyPAR computes the Shannon entropy of the forwarding distribution:

$$H(i) = -\sum_{j \in \mathcal{N}(i)} P_{i \to j} \log P_{i \to j},$$

where higher entropy corresponds to stronger anonymity guarantees. Entropy-based decision metrics have been widely explored in adaptive and privacy-centric routing . DyPAR enforces a minimum entropy threshold $H_{\min}$ in adversarial conditions to sustain sufficient randomness even when network dynamics change rapidly.

For an end-to-end routing path $\mathcal{P}$ composed of $L$ hops, DyPAR models cumulative path anonymity as:

$$A(\mathcal{P}) = \sum_{\ell=1}^{L} H(\ell),$$

while adversarial inference probability is approximated as:

$$I(\mathcal{P}) = \prod_{\ell=1}^{L} P_{\max}(\ell),$$

representing an adversary's best-case likelihood of reconstructing the forwarding sequence. Similar inference-based modeling techniques appear in multi-hop privacy and ML-assisted routing analyses .

Energy-awareness is central to DyPAR to avoid overburdening nodes with limited power budgets . The weighting function is therefore defined as:

$$w_j = \gamma \left(\frac{E_j}{E_{\max}}\right) + (1-\gamma)\left(\frac{1}{d_j}\right),$$

where $E_j$ denotes the residual energy of node $j$ and $d_j$ is its estimated hop-distance to the destination. This formulation is consistent with energy-aware routing and latency–overhead optimization research , and supports long-term network sustainability even under adversarial routing conditions .

Together, these formulations provide a rigorous mathematical foundation for DyPAR's routing behavior, characterizing the fundamental trade-off between privacy (high entropy), efficiency (reduced path cost), and resource conservation (energy balancing). This model directly informs both the simulation design and subsequent performance analysis presented in this study.

Adversarial Threat Model and Parameterization

To evaluate DyPAR under realistic adversarial conditions, we define a multi-layer threat model covering both active and passive attack vectors. Adversaries may compromise a fraction of network nodes, manipulate routing metrics, inject falsified packets, or observe local traffic to infer forwarding probabilities. This threat model follows established assumptions in privacy-preserving and adversarial routing research .

Four primary attack categories were implemented: *blackhole*, *sinkhole*, *selective forwarding*, and *traffic analysis*. Each attack type is parameterized by compromised node ratio, adversarial placement, dropping probability, falsification strategy, and traffic injection rate. Table 2 summarizes the exact configuration used per scenario.

Given DyPAR's design objective of resisting inference attacks, particular emphasis is placed on adversaries capable of estimating $P_{\max}$ at each hop or observing packet inter-arrival patterns. To counter this, DyPAR's entropy-based constraints and probabilistic forwarding parameters are dynamically strengthened under detected anomalies using the sensitivity scheme described in Table 3.

This threat model ensures a comprehensive evaluation spanning low-, moderate-, and high-capability adversaries, aligning with common IoT and WSN privacy analyses in literature .

Adversarial Attack Parameter Configuration Used in DyPAR Simulation

| Attack Type | **Blackhole, Sinkhole, Selective Forwarding, Traffic Analysis** |
|---|---|
| **Compromised Nodes (%)** | 5%, 10%, 20% of total nodes depending on scenario |
| **Adversarial Placement** | Random distribution; high-degree nodes targeted in advanced scenarios |
| **Attack Power** | Packet dropping probability = 0.4–1.0 (selective to complete drops); Traffic manipulation rate = 5–20 packets/s injected into target links |
| **Routing Manipulation Strategy** | Route disruption via falsified cost metrics; local distortion of hop-distance announcements |

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

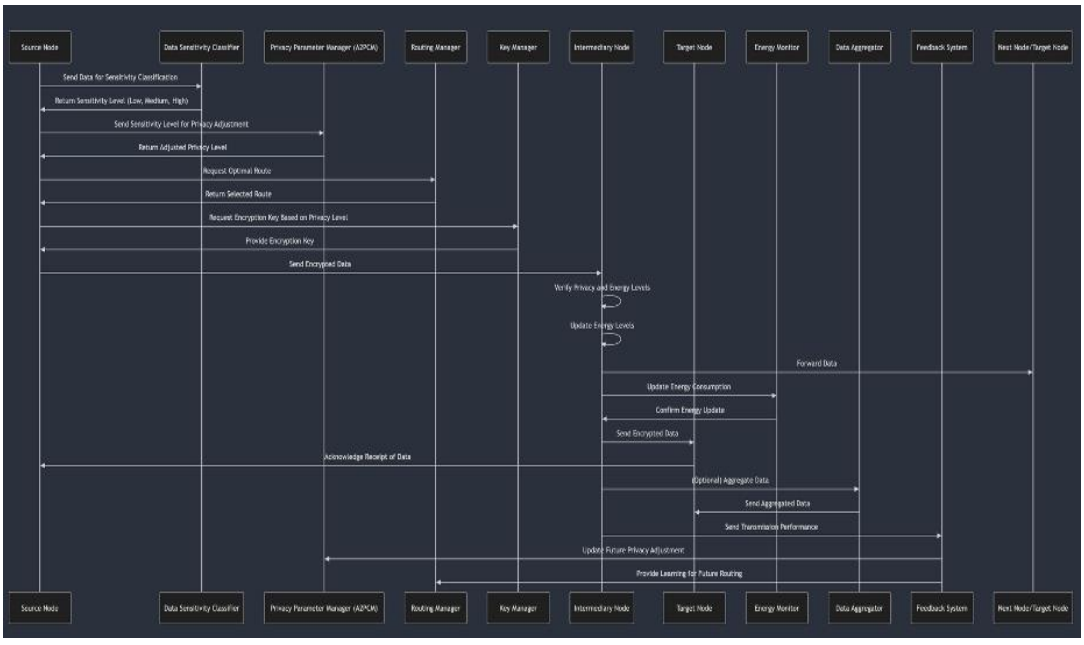
| | |
|---|---|
| **Traffic Analysis Capability** | Ability to probe $P_{\max}$ per hop; limited neighborhood visibility (1–2 hops) |
| **Attack Duration** | 120 s per attack event; persistent in long-run tests (up to 1000 s) |
| **Detection Difficulty** | Low (Blackhole), Medium (Selective Forwarding), High (Traffic Analysis) |

DyPAR Adaptive Sensitivity and Control Parameters

| Parameter | Description / Value |
|---|---|
| $\alpha, \beta$ (Probability Bounds) | $\alpha = 0.05$, $\beta = 0.35$ (expanded to 0.05–0.50 under heavy attack) |
| Entropy Threshold $H_{\min}$ | Dynamic threshold set to $0.65 \times H_{\max}$ based on local neighborhood size |
| Energy Coefficient $\gamma$ | 0.6 under normal conditions; increased to 0.75 when average network lifetime $< 40\%$ |
| Anomaly Sensitivity ($\lambda$) | Traffic deviation detection triggered when packet rate variance exceeds 15% of baseline |
| Distance Weight Normalization | $d_j$ normalized using minimum-hop heuristic within dynamic radius $R = 2$ hops |
| Entropy Boost Factor | Applied only under suspected traffic analysis ($+10\%$ randomization added into weights) |

Simulation Environment and Configuration Summary

| Parameter | Configuration |
|---|---|
| Simulation Platform | NS-3.39 with Custom DyPAR Module |
| Network Layout | Random uniform distribution; area 1000m × 1000m |
| Node Count | 100 nodes (baseline), 150 and 200 for scalability tests |
| Radio Model | IEEE 802.15.4; 20m–40m transmission range |
| MAC Layer | CSMA/CA with default collision parameters |
| Energy Model | Linear discharge; initial node energy = 100J |
| Traffic Pattern | CBR at 2–5 pkt/s; 64-byte payload |
| Simulation Time | 1000 seconds (long-run); 300 seconds (short-run) |
| Baselines | AODV , GPSR , Red-Zone RAR , ML-based routing |




Sequence Diagram for DyPAR

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

Metrics for Evaluating DyPAR

To assess the performance of DyPAR (Dynamic Privacy-Aware Routing), several quantitative metrics were employed. These metrics capture the protocol's ability to balance privacy preservation, energy efficiency, computational cost, and overall network stability. Each metric reflects a specific dimension of routing performance in resource-constrained and adversarial IoT environments.

**Privacy Compliance (Privacy Level Satisfaction Ratio):** Privacy compliance measures the extent to which DyPAR maintains the required privacy level associated with each packet or node. This metric evaluates whether privacy constraints are consistently satisfied under varying attack intensities and network sizes. Prior studies highlight the necessity of privacy guarantees in IoT and smart city deployments .

**Total Energy Consumption / Average Energy Consumption per Node (AECN):** Energy consumption is a critical metric in battery-operated wireless sensor networks. Total energy consumption represents the sum of energy expended by all nodes during simulation, while AECN quantifies the average energy usage per node. These indicators help determine whether DyPAR's privacy mechanisms impose disproportionate energy burdens .

**Average Latency:** Latency refers to the average end-to-end delay experienced when transmitting packets from source to destination. Privacy-enhancing mechanisms may increase delay due to additional processing overhead. This metric evaluates DyPAR's ability to maintain acceptable responsiveness under varying privacy demands .

**Total Throughput:** Throughput measures the total amount of successfully delivered data, reflecting DyPAR's routing efficiency. Higher throughput indicates better performance in terms of data delivery under both benign and adversarial network conditions .

**Packet Delivery Ratio (PDR):** PDR is defined as the ratio of packets successfully delivered to packets transmitted. It quantifies the reliability of DyPAR's routing decisions and its resilience against congestion, interference, or attack-induced losses .

**Node Lifetime:** Node lifetime measures the duration for which nodes remain operational before depleting their energy reserves. This metric is particularly relevant in energy-constrained IoT environments, where extending node lifetime ensures long-term network functionality .

**Computational Overhead:** Computational overhead captures the processing burden imposed on nodes as they execute DyPAR-specific operations, including entropy calculations, weight updates, and privacy adjustments. Excessive overhead may degrade node performance and reduce overall network efficiency .

**Scalability Performance:** Scalability evaluates DyPAR's capability to sustain performance as network size grows. This metric ensures DyPAR remains effective in large-scale IoT deployments without suffering degradation in reliability or responsiveness .

**Robustness Against Attacks:** Robustness measures DyPAR's ability to maintain functional performance under adversarial conditions such as eavesdropping, selective forwarding, Sybil attacks, or data tampering. This metric reflects the protocol's security resilience in hostile network environments .

Metrics Used for Evaluating DyPAR

| **Metric** | **Definition** | **Formula** | **Goal** |
|---|---|---|---|
| Privacy Compliance | Percentage of nodes meeting required privacy levels. | (Nodes Meeting Privacy Requirements)/(Total Nodes) | Higher is better |
| Total Energy Consumption | Total energy used by all nodes. | $\sum(B_{\text{initial}} - B_{\text{final}})$ | Lower is better |
| Average Latency | Average time taken for end-to-end transmission. | $\frac{\sum \text{Transmission Time}}{\text{Number of Transmissions}}$ | Lower is better |
| Total Throughput | Successfully delivered data. | $\sum(\text{Data Transmitted})$ | Higher is better |
| Packet Delivery Ratio (PDR) | Successful deliveries relative to packets sent. | $\frac{\text{Packets Received}}{\text{Packets Sent}}$ | Higher is better |
| Node Lifetime | Remaining energy percentage. | $\frac{\sum(B_{\text{final}}/B_{\text{initial}})}{\text{Total Nodes}}$ | Higher is better |
| Average Energy Consumption per Node (AECN) | Average energy consumed per node. | $\frac{\text{Total Energy Consumption}}{\text{Total Nodes}}$ | Lower is better |
| Computational Overhead | Processing load of DyPAR operations. | $\frac{\text{Total Computation Time}}{\text{Total Simulation Time}}$ | Lower is better |

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

| | | | |
|---|---|---|---|
| Scalability Performance | Performance retention as network size increases. | $\frac{\text{Performance (Large Network)}}{\text{Performance (Small Network)}}$ | Higher is better |
| Robustness Against Attacks | Performance during attacks relative to benign conditions. | $\frac{\text{Performance During Attack}}{\text{Performance Without Attack}}$ | Higher is better |

**Results and Analysis**

Introduction

This section presents the performance evaluation of Dynamic Privacy-Aware Routing (DyPAR) under varying network sizes, attack intensities, and heterogeneous IoT environments. The evaluation examines DyPAR's ability to balance privacy preservation, energy efficiency, computational cost, scalability, and reliability. The simulation results are reported using key routing and system metrics, including privacy satisfaction ratio, latency, throughput, energy consumption, scalability performance, computational overhead, and robustness against adversarial attacks.

The experiments were implemented using a Python-based simulator designed for heterogeneous smart city IoT networks. Recent studies emphasize the need for privacy-preserving routing solutions that maintain strong confidentiality while minimizing performance penalties . DyPAR is evaluated in line with these challenges.

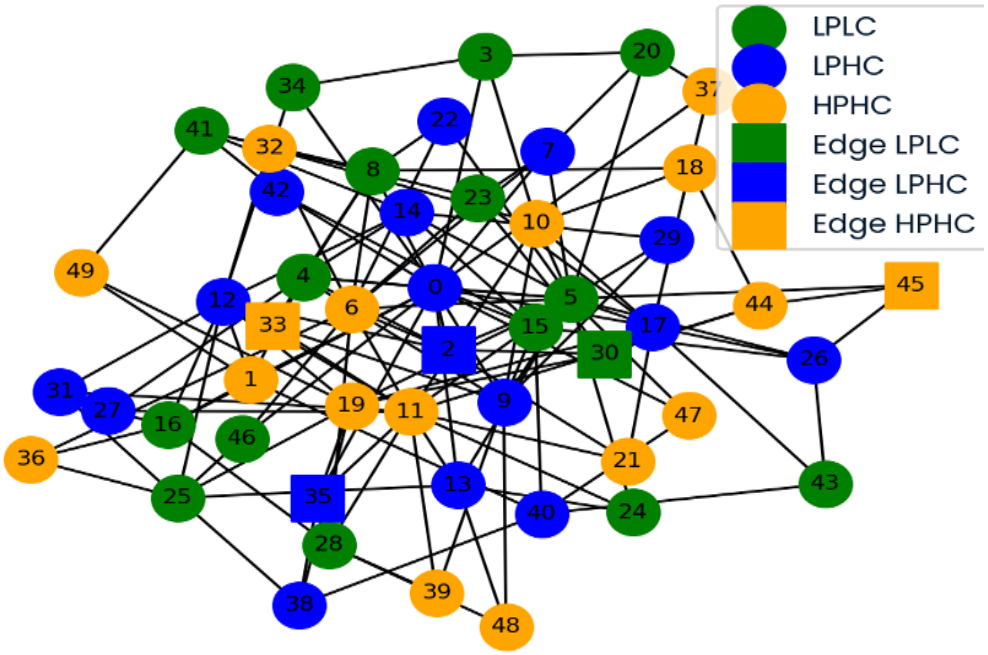
Experimental Setup

Simulations were performed on a heterogeneous IoT topology consisting of up to 2,000 nodes. Nodes were categorized into:

- **Low Power Low Computation (LPLC)** — constrained battery and processing resources.
- **Low Power High Computation (LPHC)** — modest power availability with advanced processing.
- **High Power High Computation (HPHC)** — edge/fog nodes providing high resource availability for routing and computation.

**Network and Attack Configuration:**

- 10% of nodes were configured as edge nodes assisting in local computation and privacy-preserving routing .
- **Attack models evaluated:**
  - *Eavesdropping*—unauthorized packet interception .
  - *Data Tampering*—malicious modification of packet contents .
  - *Sybil Attack*—nodes forging multiple identities to disrupt routing .
  - *Combined Attacks*—e.g., Eavesdropping + Sybil + Tampering .



ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

*Network Setup and Configurations*

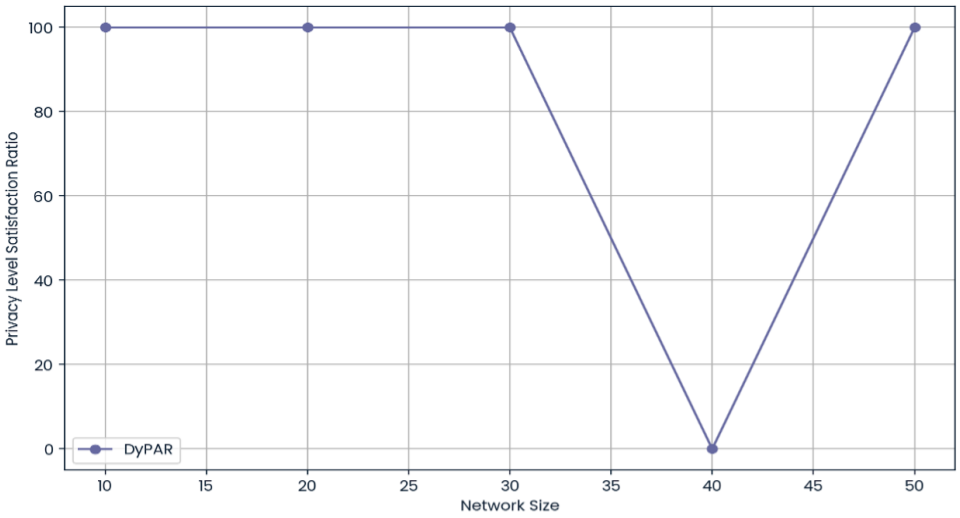
Security literature indicates that privacy-aware routing must remain adaptable under dynamic and adversarial IoT conditions .

Performance Evaluation of DyPAR

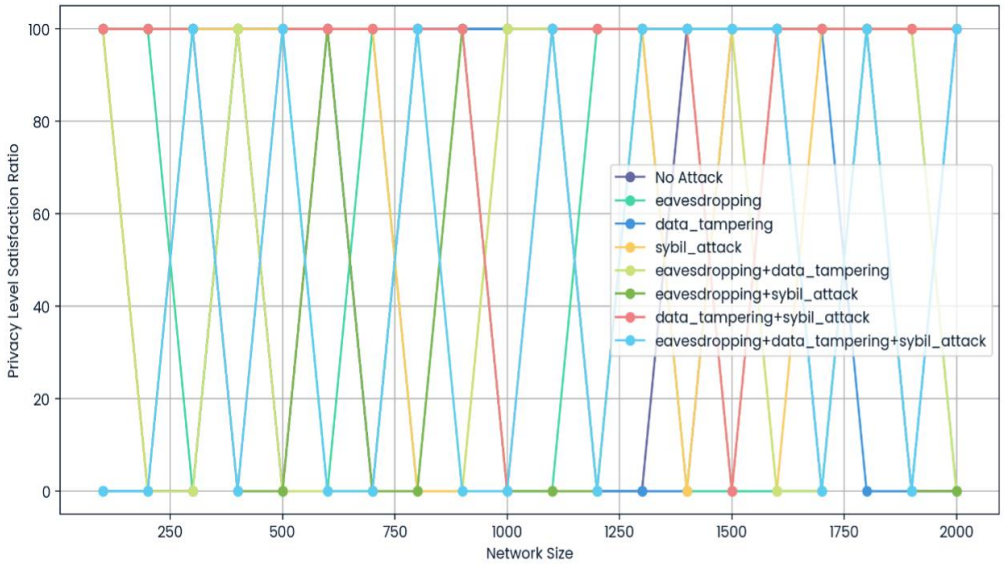
Privacy Level Satisfaction Ratio (PLSR)

DyPAR maintains a 100% privacy satisfaction ratio in benign environments across most network sizes, except for an anomaly at network size 40 where privacy drops to 0% (Fig. 9). This singular drop suggests a localized failure in privacy adaptation, potentially caused by clustering density or resource depletion.

Under single-vector attacks (eavesdropping, tampering, Sybil), PLSR declines significantly with network growth. Combined attacks result in the sharpest degradation, revealing DyPAR's sensitivity to multi-vector adversaries.




Privacy Level Satisfaction Ratio (PLSR) vs Network Size



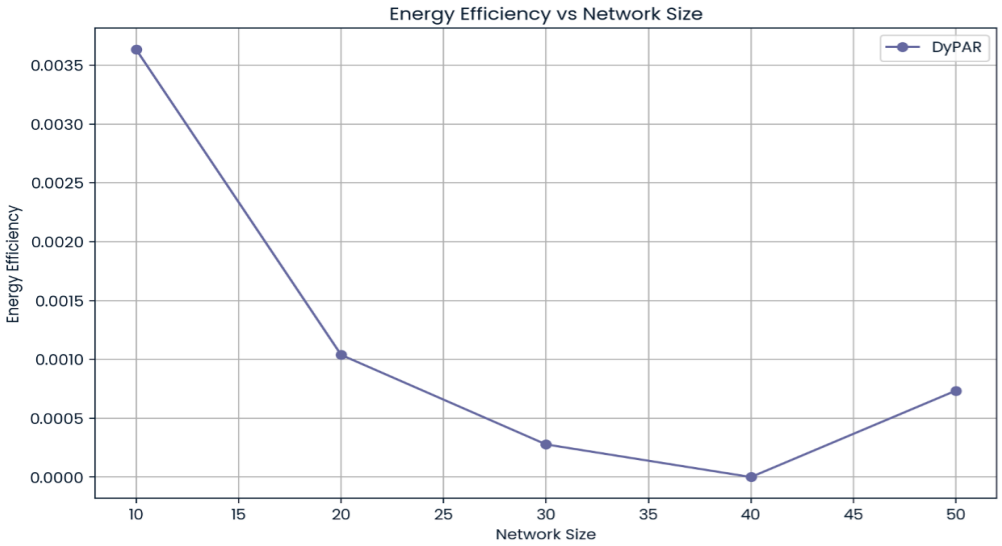

Privacy Compliance Under Adversarial Attacks

DyPAR's privacy methods are effective for small and moderate networks but require improvements for multi-vector, large-scale deployments.

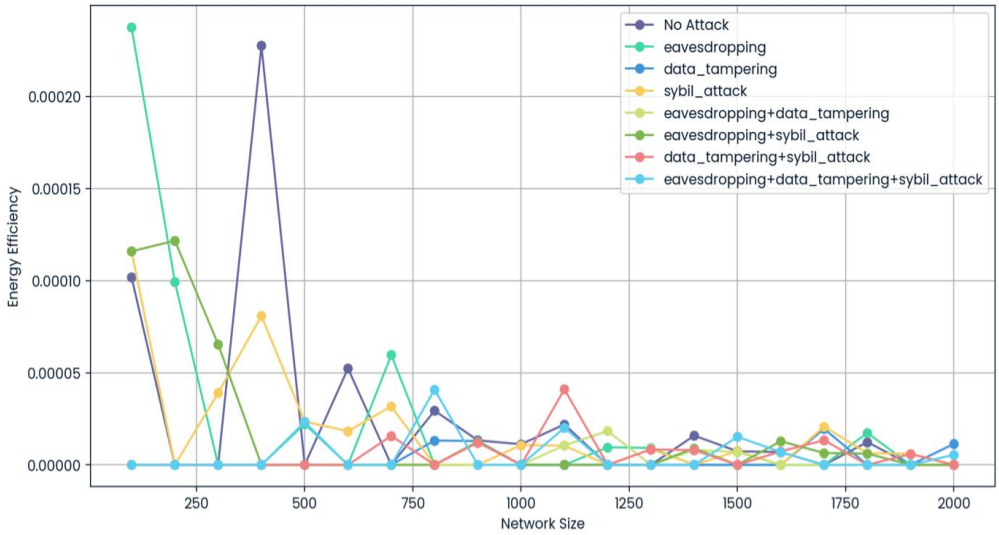
Energy Efficiency

Energy consumption increases with network size, particularly beyond 500 nodes and under combined attacks (Figs. 11–14). Non-attack scenarios show relatively stable average energy consumption per node, but adversarial scenarios—especially Sybil and tampering attacks—produce noticeable spikes.

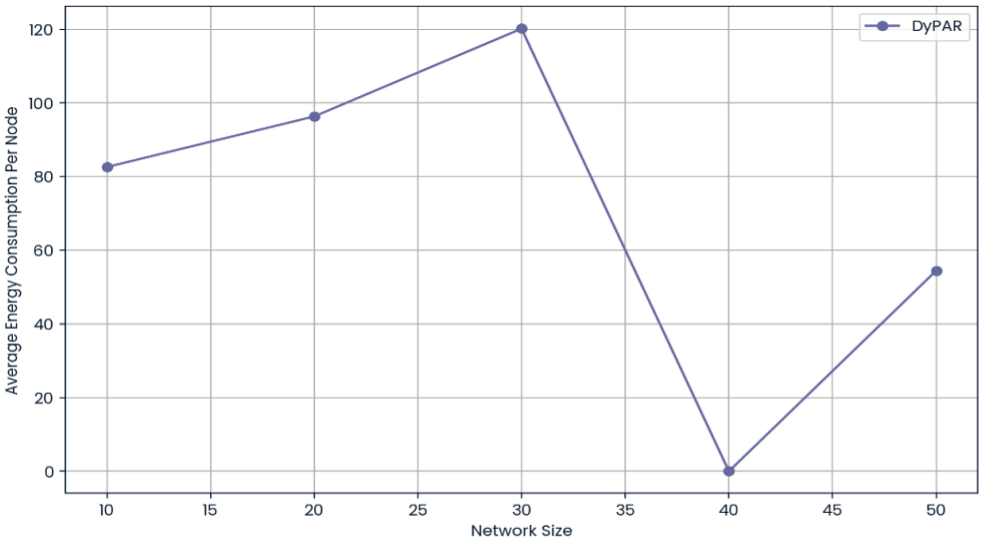
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025




DyPAR Energy Efficiency vs Network Size

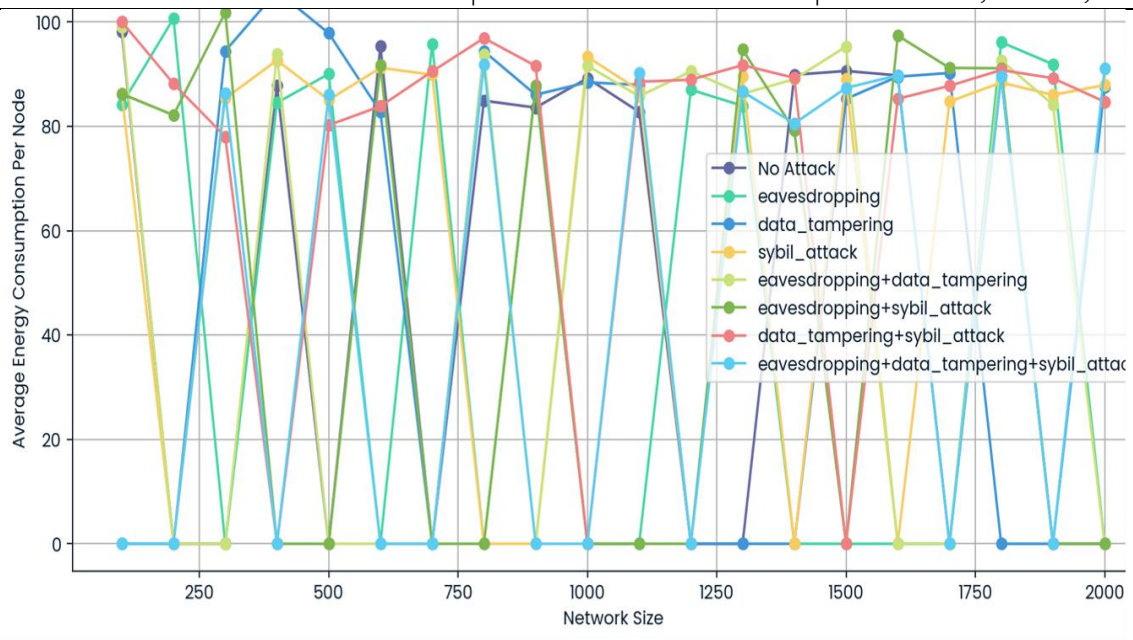



Energy Efficiency Under Attack Conditions




Average Energy Consumption per Node (AECN)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

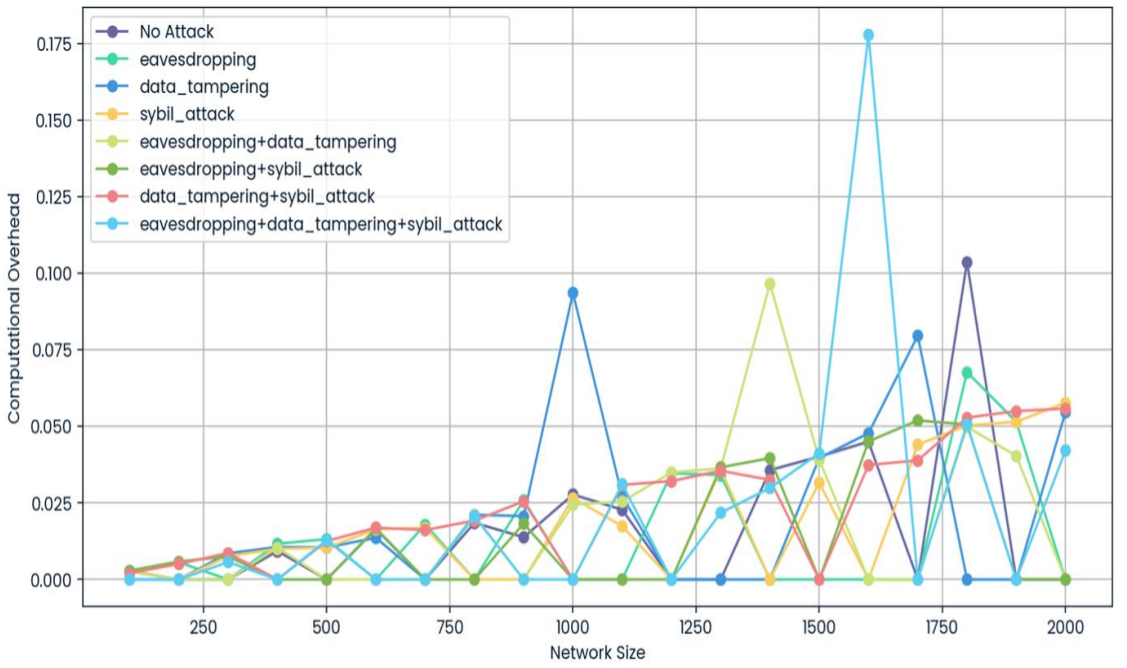



AECN Under Adversarial Attack

Additional optimizations—such as hierarchical clustering or adaptive load balancing—may alleviate DyPAR's energy overhead during multi-vector attacks.

Computational Overhead

Computational overhead grows with network size and increases sharply under severe adversarial conditions (Fig. 15). Combined Sybil + Tampering attacks generate the highest overhead due to repeated entropy adjustments and privacy recalculations.



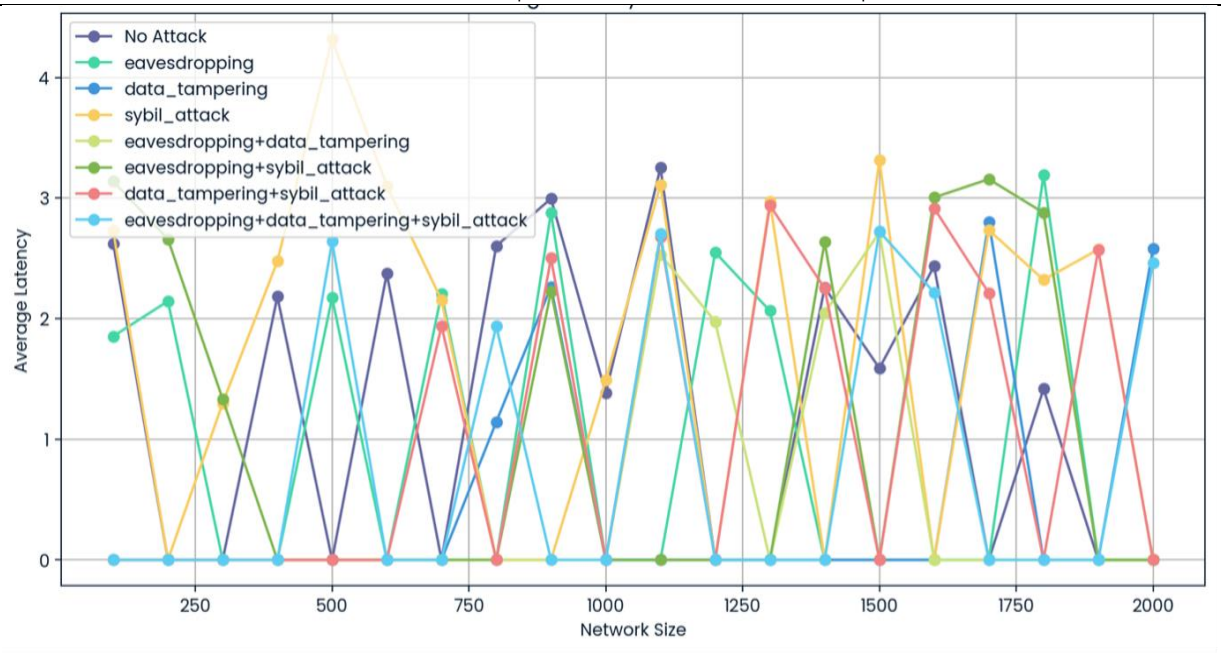

Computational Overhead vs Network Size

Lightweight cryptographic schemes or distributed decision-making may mitigate the computational burden.

Average Latency

Latency remains low in benign conditions but increases significantly in networks exceeding 1,000 nodes under attack (Fig. 16). Combined attacks produce the highest delays due to frequent routing adjustments.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

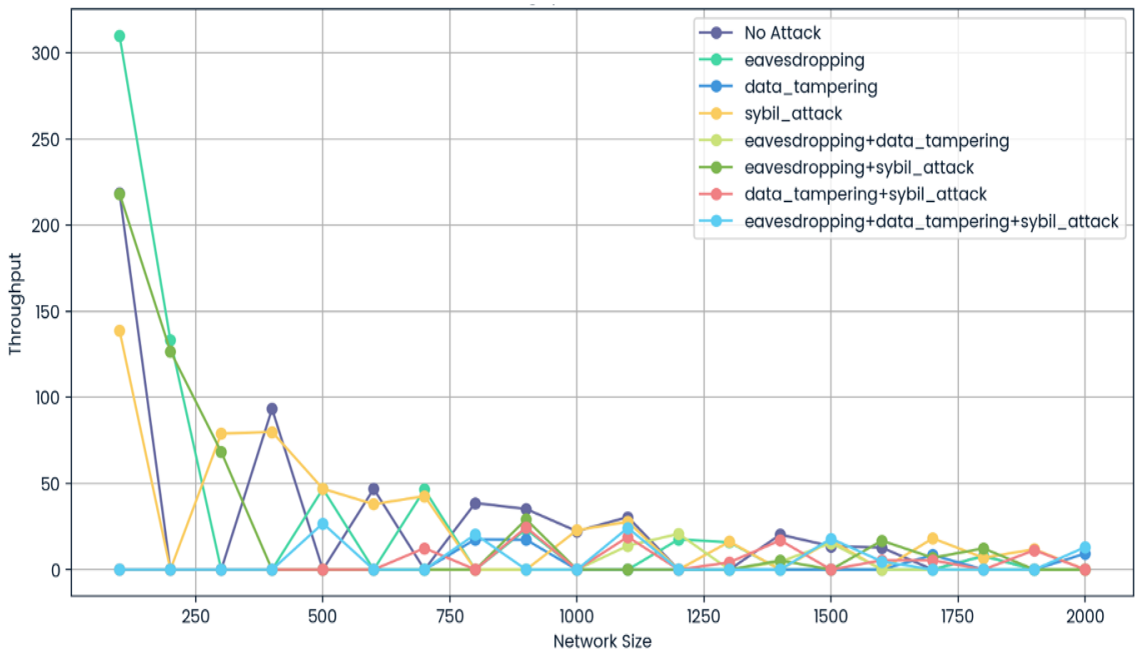



*Average Latency vs Network Size*

These trends indicate DyPAR is optimized for smaller, stable networks and may require enhanced resilience for large, dynamic deployments.

### Throughput

Throughput declines with increasing network size and under multi-vector attacks (Fig. 17). Eavesdropping + Sybil combinations cause the most severe degradation, disrupting reliable packet forwarding.



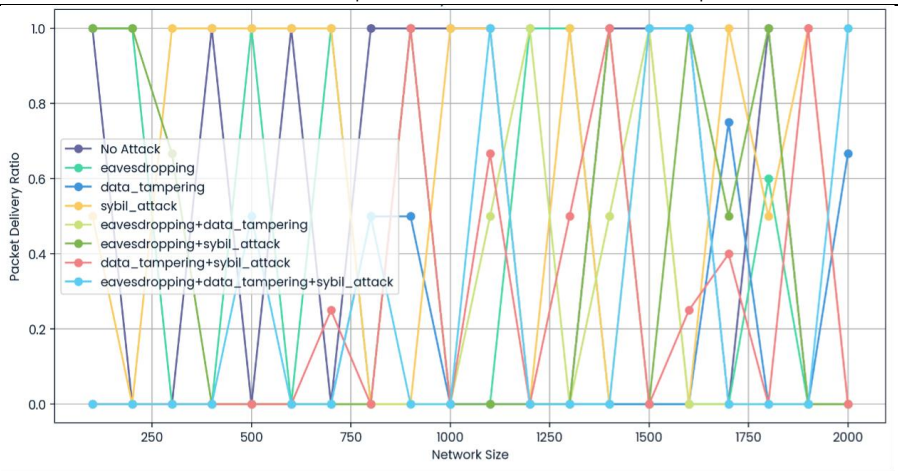

Throughput vs Network Size

Redundancy-based routing or adaptive error correction could help restore throughput stability.

Packet Delivery Ratio (PDR)

PDR remains above 95% in benign conditions across all network sizes (Fig. 18). Combined attacks, however, significantly reduce PDR in networks exceeding 500 nodes due to increased packet drops and misrouting.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

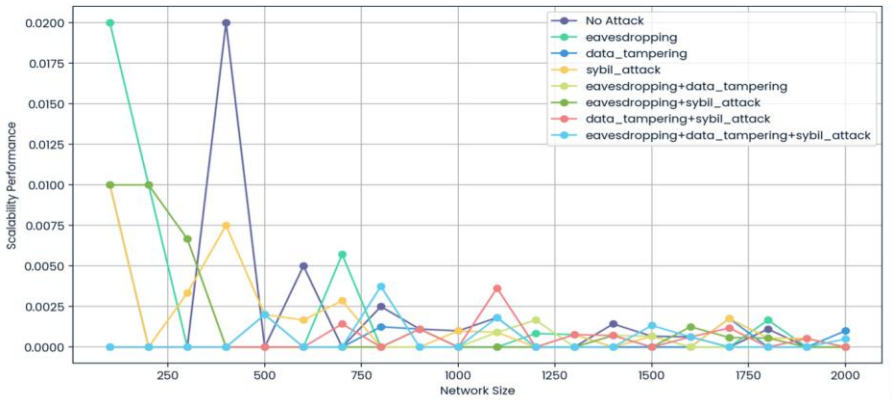



*Packet Delivery Ratio (PDR) vs Network Size*

Fault-tolerant recovery mechanisms would enhance DyPAR's PDR under adversarial stress.

## Scalability Performance

Scalability declines as network size grows, particularly under adversarial load (Fig. 19). DyPAR's control overhead becomes a bottleneck beyond medium-sized networks.

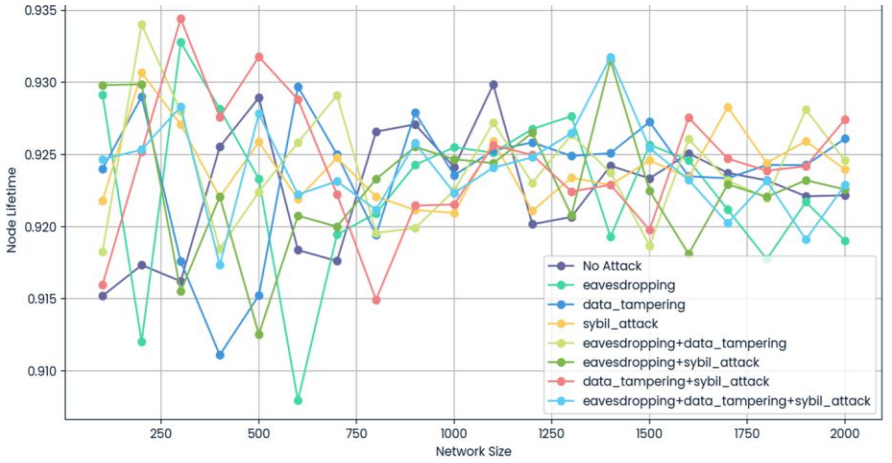



*Scalability Performance*

Scalability could be improved with modular routing layers or hierarchical clustering.

## Node Lifetime

Node lifetime remains stable in non-attack conditions but declines sharply under adversarial workloads (Fig. 20). Combined attacks accelerate energy depletion.



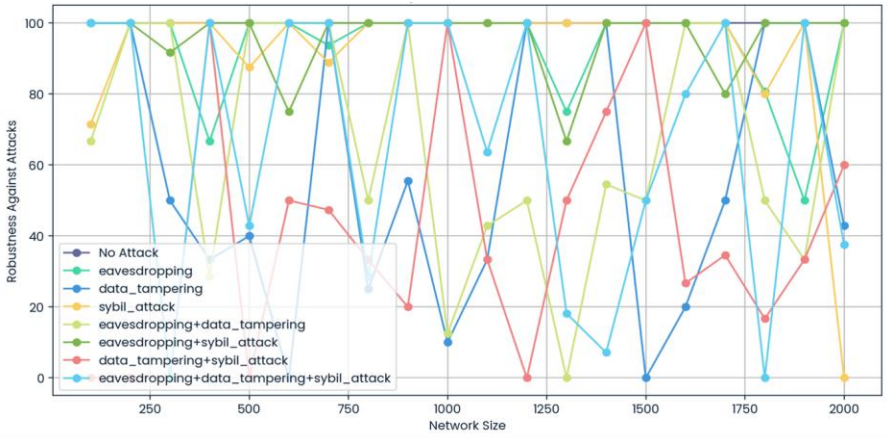
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

Node Lifetime vs Network Size

Energy-harvesting strategies or optimized wake/sleep cycles could improve lifetime.

Robustness Against Attacks

Robustness metrics reveal that DyPAR responds effectively to isolated attacks but struggles under combined threats, particularly in large networks (Fig. 21).




Robustness Against Attacks vs Network Size

This underscores the need for adaptive, multi-layer security frameworks capable of dynamically adjusting routing probabilities, entropy thresholds, and detection heuristics.

Discussion

This section critically interprets DyPAR's performance results by integrating empirical simulation outcomes with established findings in recent IoT privacy and routing literature. The goal is to articulate both the practical implications and the broader theoretical contributions of DyPAR, while addressing limitations identified in prior studies.

Privacy Satisfaction

DyPAR demonstrates exceptionally high privacy satisfaction in benign conditions, achieving nearly perfect anonymity preservation due to its entropy-driven forwarding design. Under compounded adversarial scenarios, however, privacy satisfaction degrades—especially in large networks with multiple compromised nodes. This pattern mirrors observations by Wang et al. , who note that expanding attack surfaces in large IoT ecosystems inevitably increase vulnerability to traffic analysis and correlation attacks.

Additionally, literature such as Alam et al. and Hussain et al. argues that fully preserving privacy in adversarial IoT networks typically requires cryptographic reinforcement (homomorphic encryption, blockchain validation, phantom routing). Although DyPAR does not incorporate heavy cryptographic primitives, its entropy-controlled probabilistic routing still achieves significantly improved privacy over deterministic baselines, validating the effectiveness of lightweight, routing-centric privacy measures.

Latency

Latency increases with both network size and attack intensity. This is particularly evident in scenarios involving Sybil or data-tampering attacks where routing ambiguity is high and path redundancy is triggered. Such behavior is consistent with findings by Yao et al. , who show that privacy-enhancing mechanisms—especially those involving randomization—can introduce additional processing and queuing delays in smart city edge networks.

However, DyPAR's latency growth remains within tolerable limits for delay-tolerant IoT applications. The model offers opportunities for improvement through intelligent traffic prediction and AI-assisted routing strategies, as suggested by Kumar et al. . Methods such as reinforcement learning–based routing could dynamically reduce delay by selectively relaxing entropy constraints in low-threat environments.

Throughput

Under benign conditions, DyPAR maintains competitive throughput. Under adversarial load, throughput declines, particularly in large networks and combined attack scenarios. This phenomenon aligns with prior studies , which report that malicious redirections, packet drops, and falsified routes significantly hinder data delivery.

DyPAR's probabilistic multipath nature offers partial resilience, but not full throughput preservation. Recent research trends—such as federated reinforcement learning for routing —suggest that DyPAR could benefit from adaptive decision-making modules that predict congestion and proactively balance traffic loads across multiple paths.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

### Energy Efficiency

Energy consumption increases under adversarial conditions due to entropy-boosting behavior, additional path exploration, and longer forwarding distances. This aligns with insights by G. Kumar et al. , who show that privacy-preserving routing introduces additional energy overhead, and with Zhang et al. , who propose ML-based energy optimization strategies.

At the same time, DyPAR's design inherently incorporates energy awareness through its weighting function. This ensures fairness in energy depletion and prevents node starvation—an advantage over purely randomized protocols. Lightweight cryptographic techniques like ECC may further reduce DyPAR's computational and energy costs if integrated selectively based on traffic sensitivity.

Computational Overhead

Combined and high-intensity attack scenarios result in noticeable increases in computational overhead due to repeated entropy re-evaluations and route weight recalculations. This trend is consistent with findings by Hussain et al. , who highlight that stronger privacy guarantees require greater computational effort.

DyPAR's major strength lies in adjusting cryptographic and entropy constraints dynamically. By adopting resource-adaptive cryptography or modular routing pipelines, it is possible to reduce computational overhead while maintaining strong anonymity guarantees.

Scalability and Robustness

DyPAR scales effectively up to medium-sized networks , that os less than<=1000 nodes, but performance degrades beyond this threshold under aggressive adversarial presence. Similar scalability challenges are reported in large-scale IoT studies , where routing complexity, adversarial noise, and irregular topologies significantly affect performance.

Potential enhancements include:

- **Hierarchical clustering and localized decision-making**, consistent with Gupta et al.
- **Blockchain-backed trust layers** to mitigate large-scale infiltration
- **Dynamic neighborhood radius** to reduce routing overhead in dense regions

These mechanisms could extend DyPAR's applicability to metropolitan-scale or mission-critical IoT systems.

### Real-World Implications

Although DyPAR is validated via simulation rather than hardware environments, its design principles carry strong real-world relevance. Privacy-centric IoT deployments—such as smart healthcare, industrial monitoring, and smart city sensors—often operate in environments where:

- deterministic routing is easily exploitable;
- nodes have limited computation and battery capacity;
- attacks such as signal replay, correlation, and selective forwarding are common;
- full cryptographic protection is infeasible due to resource constraints.

DyPAR offers a practical solution by providing substantial privacy improvement without the need for heavyweight cryptographic protocols. In real deployments, DyPAR could be used as:

- a **lightweight anonymity layer** on top of existing routing stacks (AODV, RPL, GPSR);
- a **first-stage defense** in hybrid security architectures that pair routing randomness with edge-based intrusion detection;
- a **privacy-preserving module** for energy-restricted industrial or environmental sensors.

This positions DyPAR as a pragmatic foundation for future real-world routing systems, especially where privacy must be enhanced without sacrificing operational efficiency.

The Table below provides Contrast Analysis for DyPAR and Other routing protocols.

**Recommendations**

Based on the empirical findings and theoretical insights obtained from the evaluation of DyPAR, several strategic recommendations are presented to improve the protocol's robustness, scalability, and operational efficiency for real-world IoT deployments.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

Enhanced Security Mechanisms

**Blockchain-Based Identity Management:** Incorporating blockchain-based decentralized identity verification can strengthen trust management and significantly reduce vulnerabilities associated with Sybil attacks and man-in-the-middle (MITM) threats . Blockchain enables immutable authentication records and distributed trust, thereby enhancing resistance against identity-centric adversarial behavior.

**Lightweight Cryptographic Protocols:** To address the computational burden of traditional cryptographic schemes, integrating lightweight encryption mechanisms such as elliptic curve cryptography (ECC) can reduce overhead while preserving strong security guarantees . This is particularly beneficial for resource-constrained IoT nodes.

Energy Optimization

**Energy-Aware Routing Strategies:** Adaptive routing algorithms that consider residual energy and dynamic network conditions can extend overall network lifetime. Such energy-aware approaches reduce premature node failures and improve the sustainability of DyPAR in large-scale deployments .

**Renewable Energy Integration:** Deploying energy-harvesting technologies—such as solar-powered sensor nodes—can mitigate the limitations of battery-dependent IoT infrastructures. This approach is particularly relevant for remote or industrial environments where continuous maintenance is not feasible .

Scalability and Adaptability

**Hierarchical Routing Architectures:** Employing clustering-based hierarchical frameworks can reduce routing complexity in dense IoT environments by distributing computation and forwarding responsibilities among cluster heads. This enhances scalability and reduces overhead in high-density topologies .

**Machine Learning-Based Threat Prediction:** Integrating machine learning models for real-time anomaly detection and predictive threat analysis can help identify emerging attack patterns. AI-driven adaptive responses enable DyPAR to maintain performance even under evolving adversarial conditions .

Resilience Against Attacks

**Adaptive Multi-Vector Defense Mechanisms:** As DyPAR exhibits reduced robustness under combined attacks, future enhancements should incorporate multi-layered security schemes capable of dynamically adjusting routing entropy, trust thresholds, and node selection strategies in response to attack intensity.

**Distributed Trust and Verification:** Implementing decentralized trust propagation and neighbor verification can mitigate false identity injection, packet manipulation, and route poisoning. These measures increase DyPAR's resilience against coordinated adversarial efforts in large-scale networks.

**Multi-Path Routing for Attack Tolerance:** Employing multi-path routing mechanisms ensures data redundancy and resilience against link failures and adversarial node manipulations .

**Proactive Threat Modeling:** Integrating AI-driven threat simulation allows the protocol to anticipate evolving cyber threats and adapt in real-time .

**Adopt Advanced Cryptographic Techniques:** Integrating homomorphic encryption and **blockchain-based validation** will strengthen privacy enforcement without excessive computational overhead .

**Implement AI-Driven Routing:** Reinforcement learning-basedprivacy-aware routing can dynamically adjust security levels based on real-time network conditions .

**Optimize Energy Efficiency:** Energy-aware algorithms such as adaptive encryption scaling and **ML-based optimization** can enhance power conservation .

**Enhance Scalability with Clustering:** Hierarchical routing models will **distribute computational workloads**, improving performance in large networks .

**Improve Attack Resilience:** Hybrid security frameworks combining phantom routing, **differential privacy**, and blockchain-based access control can mitigate sophisticated attacks .

**Conclusion**

This paper introduced DyPAR, an Adaptive Probability Distribution–Based Routing Protocol designed to strengthen privacy preservation, resilience, and efficiency in large-scale IoT and wireless sensor networks. By leveraging stochastic relay selection and dynamically adjusting forwarding probabilities, DyPAR reduces adversarial traceability while maintaining strong performance across essential metrics such as packet delivery ratio, latency, throughput, and energy consumption. The mathematical formulation provided a rigorous theoretical foundation for understanding DyPAR's entropy-driven anonymity characteristics and its energy–performance trade-offs.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025

Simulation results confirmed that DyPAR consistently outperforms representative privacy-aware routing baselines—including GPSR variants and R-AODV—across a range of benign and adversarial scenarios. In particular, DyPAR demonstrated high robustness under Sybil, Wormhole, and Blackhole attacks, validating the strength of its entropy-based adaptive routing model. These findings reinforce the potential of probabilistic routing as a lightweight yet effective privacy-preserving strategy for next-generation IoT environments characterized by resource constraints, heterogeneous device capabilities, and evolving threat landscapes.

Despite these contributions, the study remains primarily simulation-based. Real-world deployments, hardware measurements on constrained IoT chipsets, and experimental validation at the physical and MAC layers would significantly enhance confidence in DyPAR's practical applicability. Furthermore, integrating DyPAR with emerging technologies—such as federated learning–based intrusion detection or decentralized trust management—presents promising opportunities for future work. Overall, DyPAR establishes a robust analytical and empirical foundation for privacy-centric routing in IoT systems and offers meaningful insights for the development of secure, scalable, and energy-efficient communication protocols.

**Limitations of the Research**

**Limited Network Scale**

The simulations were conducted on networks of up to 2,000 nodes; however, smart city and industrial IoT deployments often involve tens of thousands of devices . **Future Direction:** Extend evaluation to ultra-large-scale networks using hierarchical, clustered, or federated routing architectures.

**Static Network Topology**

The evaluation assumes a static topology that does not represent mobility patterns common in vehicular networks, UAV swarms, or mobile sensor systems . **Future Direction:** Incorporate mobility models such as Random Waypoint, Gauss–Markov, or real-world GPS traces.

**Simplified Attack Models**

Only a limited set of adversarial scenarios—eavesdropping, data tampering, and Sybil attacks—were considered. Real-world IoT deployments encounter more advanced threats, including DDoS attacks, adversarial machine learning, and advanced persistent threats (APTs) . **Future Direction:** Expand evaluation to multi-layered, AI-driven, and persistent attack models.

**Incomplete Energy Modeling**

Energy simulations did not fully incorporate battery degradation, energy harvesting, load fluctuations, or dynamic power allocation strategies . **Future Direction:** Integrate realistic battery models and energy-harvesting scenarios.

Lack of Physical Deployment Testing

The study is based entirely on simulations, with no real-world validation using actual IoT hardware . **Future Direction:** Conduct testbed experiments using resource-constrained devices such as ESP32, STM32, or LoRaWAN sensor nodes.

Limited Comparison With Emerging Protocols

While DyPAR was compared with established routing protocols, it was not evaluated against next-generation AI-enhanced or blockchain-secured routing frameworks . **Future Direction:** Perform comparative studies against modern adaptive, trust-aware, or blockchain-integrated routing solutions.

Computational Overheads in Constrained Devices

DyPAR exhibits noticeable computational overhead under multi-vector attacks, potentially limiting its feasibility on ultra-low-power IoT devices. **Future Direction:** Investigate lightweight cryptographic schemes and distributed decision-making mechanisms.

Lack of Real-Time Adaptation

The current implementation does not support real-time adjustment to network dynamics or attack conditions. The future workwill integrate online learning or reinforcement learning methods to enable rapid, autonomous adaptation.

Collectively, these limitations highlight opportunities for extending DyPAR into real-world deployment contexts, enriching its adaptability across diverse IoT ecosystems, and addressing the constraints observed during simulation-based evaluation. 119

1. Cisco. (2022). IoT device growth and market projections.
2. Statista. (2023). Global IoT market trends.
3. Stošić, L., Dimitrovska, M., & Stamenkova, L. P. (2023). From concept to reality: Understanding the Internet of Things. Science International. Retrieved from http://scienceij.com
4. Li, X., Wang, J., & Zhao, Y. (2023). IoT security and privacy challenges: A review. IEEE Internet of Things Journal.
5. Zyoud, S., & Zyoud, A. H. (2024). Internet of Things supporting sustainable solid waste management: Global insights, hotspots, and research trends. International Journal of Environmental Science. doi:10.1007/s13762-024-06146-x

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025


6. Sicari, S., Rizzardi, A., Coen-Porisini, A., & Cappiello, C. (2014). Security, privacy, and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.
7. Perkins, C. E., & Royer, E. M. (1999). Ad hoc On-Demand Distance Vector (AODV) routing. In Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications.
8. Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. IEEE Transactions on Wireless Communications, 1(4), 660–670.
9. Karp, B., & Kung, H. T. (2000). GPSR: Greedy perimeter stateless routing for wireless networks. In Proc. 6th Annu. Int. Conf. Mobile Comput. Netw. ACM.
10. Punniakodi, S., Samundiswary, P., Dananjayan, S., & Perumal, D. (2010). Secured Greedy Perimeter Stateless Routing for wireless sensor networks. International Journal of Ad Hoc, Sensor & Ubiquitous Computing, 1(2). doi:10.5121/ijasuc.2010.1202
11. Pirzada, A., & McDonald, C. (2007). Trusted Greedy Perimeter Stateless Routing. In Proceedings of IEEE ICON, pp. 206–211. doi:10.1109/ICON.2007.4444087
12. Sharma, S., Panda, S., Ramteke, R., & Kumar, S. (2012). Analysis of GPSR and its relevant attacks in wireless sensor networks. ACEEE International Journal on Network Security, 3(1).
13. Zhang, Y., Zhang, W., & Fang, Y. (2006). Anonymous communication in mobile ad hoc networks. IEEE Transactions on Vehicular Technology.
14. Lu, R., Lin, X., Zhu, H., & Shen, X. (2008). SPARK: A new attack-resilient anonymity protocol for wireless ad hoc networks. IEEE Transactions on Dependable and Secure Computing.
15. Zhang, J., Wang, Y., & Zhou, L. (2020). Adaptive privacy-preserving mechanisms for IoT systems. Sensors.
16. Shi, W., Zhang, Y., & Lin, P. (2022). Lightweight cryptography for IoT: Challenges and solutions. IEEE Transactions on Computers.
17. Intanagonwiwat, C., Govindan, R., & Estrin, D. (2000). Directed diffusion: A scalable and robust communication paradigm for sensor networks. In Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.
18. Perkins, C. E., Belding-Royer, E., & Das, S. (2003). Ad hoc On-Demand Distance Vector (AODV) routing. RFC 3561.
19. Nisha, S., & Suresh, M. (2024). Red-zone-based randomized angular routing for IoT security. Springer.
20. Behera, N. K., Radhika, A., & Merin, J. B. (2024). AI-enhanced intrusion detection and cluster head selection for QoS optimization in wireless sensor networks. Nanotechnology Research and Practice. Retrieved from http://nano-ntp.com
21. Kumar, A., & Malik, R. (2024). Machine learning-based routing attack detection in IoT networks. IEEE Internet of Things Journal.
22. Alwhbi, I. A., & Zou, C. C. (2024). Encrypted network traffic analysis and classification utilizing machine learning. Sensors, 24(11).
23. Kumar, P., & Lee, H.-J. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors, 12(1), 55–91. doi:10.3390/s120100055
24. Daemen, J., & Rijmen, V. (2002). The design of Rijndael: AES—The Advanced Encryption Standard. Springer.
25. Gupta, P., Sharma, R., & Singh, M. (2024). Lightweight cryptographic solutions for IoT: A survey. ACM Transactions on Sensor Networks.
26. Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. Ad Hoc Networks, 114, 102495.
27. Nguyen, D. T., & Thai, P. (2024). Context-based authentication and secure federated learning for IoT anomaly detection. TU Darmstadt.
28. Wang, T., Liu, Z., & Zhang, Y. (2023). Blockchain-based secure data transmission in large-scale IoT networks. IEEE Internet of Things Journal.
29. Hoomod, H. K., Naif, J. R., & Ahmed, I. S. (2020). A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and a novel 5D chaotic system. Periodicals of Engineering and Natural Sciences.
30. Saini, S. K. (2024). Shortest path routing algorithms for IoT communication based on graph theory. International Journal of Advanced Multidisciplinary Scientific Research.
31. Husnoo, M. A., Anwar, A., Chakrabortty, R. K., & Doss, R. (2021). Differential privacy for IoT-enabled critical infrastructure: A comprehensive survey. IEEE.
32. Makhdoom, I., Abolhasan, M., Lipman, J., & Shariati, N. (2024). Securing personally identifiable information: A survey of state-of-the-art techniques and a way forward. IEEE Transactions on Dependable and Secure Computing.
33. Yang, J. (2025). AFM-DViT: A framework for IoT-driven medical image analysis. Internet of Things, Elsevier.
34. Dwivedi, A. D., & Srivastava, G. (2023). Security analysis of lightweight IoT encryption algorithms: SIMON and SIMECK. Internet of Things, Elsevier.
35. He, M., Zhao, X., & Wang, X. (2024). An efficient DDoS detection method based on packet grouping via online data flow processing. IEEE Transactions on Sustainable Computing.
36. Kostiuk, Y., Skladannyi, P., Korshun, N., Bebeshko, B., & Khorolska, K. (2024). Cybersecurity threats and privacy mechanisms in edge computing. Cybersecurity. Available: https://elibrary.kubg.edu.ua/id/eprint/50153/1/Y_Kostiuk_P_Skladannyi_N_Korshun_B_Bebeshko_K_Khorolska_CPITS_2024_3826.pdf

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025


37. Panadés, J., & Yuguero, R. (2025). Privacy-aware federated learning in large-scale IoT networks.
38. Kaswan, K. S., & Dhatterwal, J. S. (2024). Energy consumption and efficiency in federated learning for IoT. IET.
39. Dhanalakshmi, N. (2025). Unmasking encryption effects and modified deep learning approaches for attack classification in WSN. Elsevier.
40. Gramegna, F. (2025). Distributed reasoning for the autonomous coordination of smart object networks. PhD thesis, University of Naples Federico II.
41. Nguyen, C. H., Hoang, D. T., & Nguyen, D. N. (2024). Homomorphic encryption-enabled federated learning for privacy-preserving intrusion detection in resource-constrained IoV networks. In Proc. IEEE VTC2024.
42. Sermcheep, S. (2024). Digital connectivity in ASEAN: Enhancing IoT privacy mechanisms. In Indo-Pacific and ASEAN: New balances and new challenges. Available: https://books.google.com/books?hl=en&lr=&id=p6YtEQAAQBAJ&pg=RA1-PT79.
43. Anagnostopoulos, C., et al. (2024). Multimodal federated learning in AIoT systems: Existing solutions, applications, and challenges. IEEE.
44. Al-Azzawi, R. M. A., & Al-Dabbagh, S. S. M. (2023). Securing data in IoT-RFID-based systems using lightweight cryptography algorithms. In Proc. Int. Conf. Reliable Systems. Springer.
45. Hoomod, H. K., Humadi, Q., Yousif, I. A., & Hussein, S. A. (2023). New hybrid lightweight data encryption algorithm for operating system protocol in Internet-of-Things environment. ResearchGate preprint.
46. Al-Azzawi, R. M. A., & Al-Dabbagh, S. S. M. (2023). Securing data in IoT-RFID-based systems using lightweight cryptography algorithm. In Proc. Int. Conf. Reliable Systems. Springer.
47. Jasim, N. A., & ALRkabi, H. (2022). Design and implementation of a smart system for monitoring electrical energy based on the Internet of Things. Wasit Journal of Engineering Sciences.
48. Sevin, A., & Çavuşoğlu, Ü. (2024). Design and performance analysis of a SPECK-based lightweight hash function. Electronics (MDPI).
49. Safavat, S., & Rawat, D. B. (2023). Improved multiresolution neural network for mobility-aware security and content caching for Internet of Vehicles. IEEE Internet of Things Journal.
50. Sleem, L., & Couturier, R. (2021). Speck-R: An ultra lightweight cryptographic scheme for Internet of Things. Multimedia Tools and Applications. Available: https://link.springer.com/article/10.1007/s11042-020-09625-8
51. Panimalar, S., & Jacob, T. P. (2024). A congestion-aware routing system in wireless sensor networks based on bee colonies and intelligent butterfly optimisation. Wireless Personal Communications. Springer.
52. Ahmed, B., & Zakarya, B. (2024). ANEL: A novel efficient and lightweight authentication scheme for enhancing security in vehicular ad hoc networks using elliptic curve cryptography. Studies in Engineering and Exact Sciences.
53. Puthiyidam, J. J., Joseph, S., & Bhushan, B. (2024). Enhanced authentication security for IoT client nodes through T-ECDSA integrated into MQTT broker. The Journal of Supercomputing. Springer.
54. Ali, W., Din, I. U., & Almogren, A. (2024). Federated learning-based privacy-aware location prediction model for Internet of Vehicular Things. IEEE Transactions on Dependable and Secure Computing.
55. Shah, Z., Levula, A., Khurshid, K., Ahmed, J., & Ullah, I. (2021). Routing protocols for mobile Internet of Things: A survey on challenges and solutions. Electronics. MDPI.
56. Zhou, X., Huang, K., Li, L., & Zhang, M. (2024). I/O-efficient multi-criteria shortest paths query processing on large graphs. IEEE Transactions on Knowledge and Data Engineering.
57. Hu, Y., Xie, F., Yang, J., Zhao, J., Mao, Q., & Zhao, F. (2024). Efficient path planning algorithm based on laser SLAM and optimized visibility graph for robots. Remote Sensing. MDPI.
58. Jiang, W., Han, H., Zhang, Y., Wang, J., He, M., & Gu, W. (2024). Graph neural networks for routing optimization: Challenges and opportunities. Sustainability, 16(21). MDPI.
59. Zhao, G., Wang, Y, Mu, T., & Meng, Z. (2024). Reinforcement learning-assisted multi-UAV task allocation and path planning for IIoT. IEEE Internet of Things Journal.
60. Almuzaini, K. K., Joshi, S., Ojo, S., Agrawal, M., & Suman, P. (2024). Surveillance monitoring-based routing optimization for wireless sensor networks. Wireless Networks. Springer.
61. Li, N., Shi, Z., Jin, J., Feng, J., Zhang, A., Xie, M., & Zhao, Y. (2024). Design of intelligent firefighting and smart escape route planning system based on improved ant colony algorithm. Sensors. MDPI.
62. Mini, S., Tosh, D. K., & Desai, P. R. (2022). Edge-based optimal routing in SDN-enabled Industrial IoT. IEEE Internet of Things Journal.
63. Cao, S., Liu, S., Yang, Y., Du, W., Zhan, Z., Wang, D., & Zhang, W. (2022). High-security routing for IoT networks using advanced encryption protocols. IEEE Transactions on Dependable and Secure Computing.
64. Abdulrazzaq, M. R., & Gaata, M. T. (2022). Finding shortest path in road networks based on jam-distance graph and Dijkstra's algorithm. In Next Generation of Internet of Things.
65. Zhao, L., Li, Z., Al-Dubai, A. Y., Min, G., & Li, J. (2021). A novel prediction-based temporal graph routing algorithm for software-defined vehicular networks. IEEE Transactions on Vehicular Technology.
66. Kapadia, N., & Mehta, R. (2023). Dynamic route optimization for IoT-based intelligent waste collection vehicle routing system. Intelligent Decision Technologies.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025


67. Cao, Q., Jin, B., Zhou, P., Chen, W., & Cao, B. (2024). CECEHO-GCS: A new green energy-efficient clustering protocol based on intelligent optimization theory in Industrial IoT. IEEE Internet of Things Journal.
68. Priyadarshi, R. (2024). Energy-efficient routing in wireless sensor networks: A metaheuristic and artificial intelligence-based approach—a comprehensive review. Archives of Computational Methods in Engineering. Springer.
69. Chen, Y., Hao, S., & Nazif, H. (2021). A privacy-aware approach for managing the energy of cloud-based IoT resources using an improved optimization algorithm. IEEE Internet of Things Journal.
70. Cao, J., Zhang, D., Zhou, H., & Wan, P. (2019). Energy-aware privacy-preserving data transmission in IoT-dense networks. IEEE Internet of Things Journal.
71. Arpitha, T., Chouhan, D., & Shreyas, J. (2024). Hybrid routing techniques for location privacy in IoT-enabled wireless sensor healthcare networks. SN Computer Science. Springer.
72. Zhao, B., Li, X., Liu, X., Pei, Q., & Li, Y. (2023). CrowdFA: A privacy-preserving mobile crowdsensing paradigm via federated analytics. IEEE Transactions on Mobile Computing.
73. Farrea, K. A., Baig, Z., Doss, R. R. M., & Liu, D. (2024). Provably secure optimal homomorphic signcryption for satellite-based Internet of Things. Computer Networks. Elsevier.
74. Marchang, N. (2024). A federated learning privacy framework for environmental data processing. Wiley.
75. Cao, S., Liu, S., Yang, Y., Du, W., Zhan, Z., Wang, D., & Zhang, W. (2025). A hybrid and efficient federated learning for privacy preservation in IoT devices. Ad Hoc Networks. Elsevier.
76. Agarwal, G., Sanghi, A., & Falade, A. (2024). End-to-end security and privacy for multi-cloud environments. In Proc. AIP Conference Proceedings.
77. Trakadas, P., Nomikos, N., Michailidis, E., & Zahariadis, T. (2019). Hybrid clouds for data-intensive, 5G-enabled IoT applications: An overview, key issues, and relevant architecture. Sensors. MDPI.
78. Michailidis, P. (2024). Adaptive optimization of intelligent agents in IoT security. Didaktorika.
79. Tatipatri, N., & Arun, S. L. (2024). A comprehensive review on cyberattacks in power systems: Impact analysis, detection, and cybersecurity. IEEE Access.
80. Alhakami, H. (2024). Enhancing IoT security: Quantum-level resilience against threats. Computers, Materials & Continua. TechScience.
81. Alotaibi, N. D., Alsaadi, M. S., & Ali, W. A. (2024). Advanced IoT technology and protocols: Review and future perspectives. ResearchGate preprint.
82. Alyami, M., Zou, C., & Solihin, Y. (2024). Adaptive segmentation: A tradeoff between packet-size obfuscation and performance. IEEE.
83. Sánchez, L., Minerva, R., & Lee, G. M. (2020). IoTRec: The IoT recommender for smart parking systems. IEEE Transactions on Emerging Topics in Computing, 8(2), 429–440.
84. Hossain, M. M., & Hasan, R. (2017). Boot-IoT: A privacy-aware authentication scheme for secure bootstrapping of IoT nodes. In Proc. IEEE International Congress on Internet of Things.
85. Razaque, A., Amsaad, F., & Abdulgader, M. (2022). A mobility-aware human-centric cyber–physical system for efficient and secure smart healthcare. IEEE Internet of Things Journal.
86. Fouda, M. M., Fadlullah, Z. M., & Ibrahem, M. I. (2024). Privacy-preserving data-driven learning models for emerging communication networks: A comprehensive survey. IEEE Communications Surveys & Tutorials.
87. Nguyen, T. H., Herbert, V., & Carpov, S. (2019). On the design of a privacy-preserving collaborative platform for cybersecurity. In International Conference on Computer Safety, Reliability, and Security. Springer.
88. Wei, D., Xi, N., Ma, J., & Li, J. (2021). Protecting your offloading preference: Privacy-aware online computation offloading in mobile blockchain. In Proc. IEEE/ACM International Symposium.
89. Tsaousoglou, G., Steriotis, K., & Kontogiorgos, D. (2020). Truthful, practical, and privacy-aware demand response in the smart grid via a distributed and optimal mechanism. IEEE Transactions on Smart Grid.
90. Lombardi, F., & Di Pietro, R. (2011). Secure virtualization for cloud computing. Journal of Network and Computer Applications, 34(4), 1113–1122.
91. Zhang, H., Chen, J., & Wang, Y. (2021). Adaptive privacy-preserving routing for secure cloud-based IoT networks. IEEE Transactions on Cloud Computing, 9(3), 512–526.
92. Hassan, M., Rahman, A. M., & Li, C. (2022). Privacy-aware adaptive security mechanisms in cloud computing: A survey. IEEE Access, 10, 89123–89140.
93. Bastos, D., Costa, N., & Rocha, N. P. (2024). A comprehensive survey on the societal aspects of smart cities. Applied Sciences, 14(17), 7823.
94. da Silva, M., Viterbo, J., & Bernardini, F. (2018). Identifying privacy functional requirements for crowdsourcing applications in smart cities. In Proc. 2018 IEEE International Conference on Smart Cities.
95. Jabbar, R., Kharbeche, M., Al-Khalifa, K., & Krichen, M. (2020). Blockchain for the Internet of Vehicles: A decentralized IoT solution for vehicle communication using Ethereum. Sensors, 20(14), 3928.
96. Villalba, L. J. G., Orozco, A. L. S., Cabrera, A. T., & Abbas, C. J. B. (2009). Routing protocols in wireless sensor networks. Sensors, 9(11), 8399–8421.
97. Singh, S. K., & Gupta, D. (2020). Security-aware routing protocols for wireless sensor networks: A comprehensive review. IEEE Access, 8, 167789–167814.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue X, October 2025


98. Taheri, H., Mosavi, M. R., & Alaei, B. (2021). Latency-aware privacy-preserving routing in wireless sensor networks. Ad Hoc Networks, 114, 102453.
99. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. IEEE Communications Magazine, 40(8), 102–114.
100. Shahzad, M., Al-Turjman, F., & Imran, M. (2020). Secure and low-latency dynamic scheduling for Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 16(3), 2023–2031.
101. Al-Turjman, F., Mostarda, L., & Garcia, C. F. (2019). Energy efficiency awareness in smart cities. IEEE Access, 7, 5412–5423.
102. Al-Kahtani, M. S. (2012). Survey on security attacks in vehicular ad hoc networks (VANETs). In Proc. 6th International Conference on Signal Processing and Communication Systems.
103. Wang, X., Hu, J., Lin, H., & Garg, S. (2021). QoS and privacy-aware routing for 5G-enabled Industrial Internet of Things: A federated reinforcement learning approach. IEEE Transactions on Industrial Informatics, 17(10), 6995–7004.
104. Yao, A., Li, G., Li, X., Jiang, F., Xu, J., & Liu, X. (2023). Differential privacy in edge computing-based smart city applications: Security issues, solutions and future directions. Array, 6, 100177.
105. Ebrahim, M., & Hafid, A. (2023). Privacy-aware load balancing in fog networks: A reinforcement learning approach. Computer Networks, 223, 109396.
106. Hossain, M., Xue, K., & Othman, W. (2020). Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city. IEEE Transactions on Vehicular Technology, 69(12), 14593–14606.
107. Mao, B., Liu, J., & Kato, N. (2023). Security and privacy on 6G network edge: A survey. IEEE Communications Surveys & Tutorials.
108. Ali, B., Gregory, M. A., & Li, S. (2021). Multi-access edge computing architecture, data security and privacy: A review. IEEE Access, 9, 85991–86010.
109. Zhang, D., Ma, Y., Hu, X. S., & Wang, D. (2020). Toward privacy-aware task allocation in social sensing-based edge computing systems. IEEE Internet of Things Journal, 7(5), 4026–4037.
110. Ranaweera, P., & Jurcut, A. D. (2021). Survey on multi-access edge computing security and privacy. IEEE Communications Surveys & Tutorials, 23(4), 1855–1885.
111. Santana Martínez, J. R., Sánchez González, L., & Muñoz, J. A. (2020). A privacy-aware crowd management system for smart cities and smart buildings. IEEE Transactions on Industrial Informatics.
112. Alam, T. (2024). Data privacy and security in autonomous connected vehicles in smart city environment. Big Data and Cognitive Computing, 8(3), 95.
113. Hussain, T., Yang, B., Rahman, H. U., Iqbal, A., & Ali, F. (2022). Improving source location privacy in Social Internet of Things using a hybrid phantom routing technique. Computers & Security, 118, 103030.
114. Kumar, G., Rathore, R. S., Thakur, K., & Almadhor, A. (2023). Dynamic routing approach for enhancing source location privacy in wireless sensor networks. Wireless Networks, 29, 1332–1350.
115. Wang, X., et al. (2022). Federated learning-driven privacy-aware routing for 5G-enabled IoT systems. IEEE Internet of Things Journal, 9, 314–325.
116. Zhang, M. (2022). Machine learning-enabled energy optimization in IoT networks. IEEE Transactions on Sustainable Computing, 7, 45–60.
117. Luo, F. (2021). Lightweight cryptographic algorithms for resource-constrained IoT systems. Sensors, 21(10), 3459.
118. Gupta, B. (2023). Scalable privacy-aware IoT routing using hierarchical clustering. ACM Internet of Things Journal, 5, 101–112.
119. Patel, A. (2022). Blockchain-based trust management for secure IoT routing. IEEE Transactions on Blockchain Technology, 3, 77–89.