Article

Cross-Layer Analysis of Machine Learning Models for Secureand Energy-Efficient IoT Networks

Rashid Mustafa , Nurul I. Sarkar * , Mahsa Mohaghegh , Shahbaz Pervez , Ovesh Vohra

Posted Date: 16 April 2025

doi: 10.20944/preprints202504.1349.v1

Keywords: Energy Efficiency; Contiki Simulator; Contiki OS; Cyber Threat Mitigation; Internet of Things; Role-based Access Control; Decison Trees; Long Short term Memory; Artificial Intelligence; Packet Delivery Ratio

Article

Cross-Layer Analysis of Machine Learning Models for Secure and Energy-Efficient IoT Networks

Rashid Mustafa, Nurul I. Sarkar *, Mahsa Mohaghegh, Shahbaz Pervez and Ovesh Vohra

Department of Computer and Information Sciences, Auckland University of Technology, Auckland 1010, New Zealand; rashid.mustafa@autuni.ac.nz (R.M.); mahsa.mohaghegh@aut.ac.nz (M.M.); shahbazp@whitecliffe.ac.nz (S.P.); 20232014@mywhitecliffe.com (O.V)

* Correspondence: nurul.sarkar@aut.ac.nz

Abstract: The widespread use of Internet of Things (IoT) raises security and energy efficiency concerns, particularly for low-resource devices. In this paper, we analyse a cross-layer IoT architecture using machine learning models and lightweight cryptography. We focus on analysing vulnerabilities and suggest energy-efficient IoT solutions. Our proposed solution is based on a role-based access control ensuring secure authentication in large-scale IoT deployments and blocks undesired access attempts. By combining convolutional neural networks, rule-based systems, and hybrid artificial intelligence, the proposed cross-layer architecture improves the accuracy of anomaly identification while lowering false positives. The system performance is evaluated by simulations as well as testbeds to accomplish attack mitigation. Results show that the proposed system reduces false positives by 28–32% and provide improved security by preventing 95% of unwanted access. We found up to 30% power reduction in the proposed lightweight Speck encryption (8Hz ContikiMAC duty cycle) than the traditional AES encryption. For data injection, and sinkhole and jamming attacks, the system's resilience is confirmed by Cooja/Contiki simulations, which maintain a 95% packet delivery rate. By learning from convolutional neural networks and artificial intelligence, our approach efficiently improves IoT security and energy efficiency in practical scenarios such as smart schools.

Keywords: energy efficiency; contiki simulator; contiki OS; cyber threat mitigation; internet of things; role-based access control; decison trees; long short term memory; artificial intelligence; packet delivery ratio

1. Introduction

The potential for the Internet of Things (IoT) to transform sectors like healthcare, smart schools, and industrial automation is undeniable. However, there are significant issues with cybersecurity and energy efficiency due to the extensive interconnection of IoT devices. Devices with restricted resources, frequently symbolized by low computing power and battery life, find it difficult to apply conventional security measures without sacrificing functionality. Although the strong cryptographic methods such as Speck and Advanced Encryption Standard (AES) can improve data security but it can potentially raise ecological issues with increasing energy and computing cost. Furthermore, IoT systems work at various protocol layers including sensor, network, and application that are vulnerable to multi-vector cyber threats, which calls for an all-encompassing cross-layer security strategy. The main drawbacks of traditional IoT systems include built-in security-energy trade-offs, where strong encryption reduces battery life and energy-saving techniques erode defenses. Furthermore, current methods frequently handle security threats separately, ignoring the requirement for cross-layer and integrated solutions. The scalability and robustness of these static frameworks are additionally compromised with inability to adapt to changing threat landscapes and varied device capabilities. To close these gaps, we propose a revolutionary cross-layer design that balances adaptability, energy efficiency, and security. The use of layer-specific machine learning models, role-based access control, adaptive duty cycling, and lightweight encryption is essential to this system. The ultimate objective is to create a secure and long-lasting IoT ecosystem that can maintain vital applications in smart schools, smart cities, and other related fields.

Effective IoT system design necessitates striking a balance between several conflicting demands using energy-efficient cryptographic algorithms like Speck that lessen computing load without compromising security and dynamic routing protocols that adjust to network changes. Clear performance goals (like preserving 95% packet delivery in the event of an attack) and standardized evaluation metrics (like energy usage and latency measurements) that measure the essential security-efficiency tradeoffs must be established in order to properly evaluate such cross-layer architectures. This methodical approach, which includes layer-specific benchmarks for operational efficiency (using techniques like adaptive duty cycling) and resilience (against threats like jamming or sinkhole attacks), allows for thorough validation of cross-layer IoT architecture while guaranteeing their applicability for real-world deployment and future scalability.

1.1. Research Challenges

There are several obstacles that need to be looked at when designing IoT networks that are both safe and energy-efficient. These obstacles include diverse device capabilities, dynamic threat environments, and computing limitations. We address the above mentioned issues by proposing a cross-layer architecture that balances layer-specific machine learning models, adaptive resource management, and lightweight cryptography. By adopting cross-layer (application, network, and sensor) interaction and AI-driven anomaly detection makes a significant contribution in guaranteeing reliable threat identification and reducing false positives. In resource-constrained situations, the suggested methodology promotes the creation of scalable IoT systems that can withstand changing cyber threats by bridging the gap between cryptographic resilience and sustainable operation. In this paper, we address the following three research questions/challenges.

Research Question 1: What can be done to develop a better understanding of the accuracy and dependability of sensor networks in various architectural settings?

Our goal is to create a system that combines flexible routing protocols like RPL and 6LoWPAN, role-based access control (RBAC), and energy-efficient cryptographic methods like SPECK and PRESENT. This allows security parameters to be set in real-time according to threat level and network conditions. The development of AI-based security mechanisms also improve anomaly detection and lessen Distributed Denial of Service (DDoS) assaults by utilizing agentless Security Information and Event Management (SIEM) modules and federated learning. Multi-story buildings can be equipped with wireless sensor networks (WSNs), where sensors continuously check environmental factors such as humidity, temperature, and light intensity.

Research Question 2: What can be done with sensor data to improve monitoring and energy efficiency of a typical school intelligently? To answer Research Question 2, we examine static, dynamic, symbolic, and hybrid analytic methods for identifying embedded firmware vulnerabilities. The multi-phase validation approach evaluates the protocol efficiency hostile attacks, environmental interference, and heterogeneous device configurations utilizing simulations (Cooja/Contiki), hardware prototypes (Z1 motes), and field deployments. The purpose of this investigation is to learn more about the accuracy and dependability of sensor networks, especially in a variety of architectural contexts. Our study clarifies the similarities and differences between the two datasets by comparing real sensor data with simulated outcomes. Additionally, we aim to strengthen the security of the RPL protocol in IoT networks.

Research Question 3: What can be done to improve IoT cross-layer security monitoring and energy efficiency intelligently? To respond to Research Question 3, we outline the proposed system which balances security and efficiency in resource-constrained contexts by integrating lightweight protocols across IoT layers. To estimate the adoption levels across various activities in smart systems, this study closes the knowledge gap on the assessment of AI and big data by developing a sector-specific maturity model based on literature and focus group findings.

1.2. Research Contributions

A novel cross-layer architecture for secure and energy-efficient IoT systems is proposed. We address the shortcomings of existing IoT security frameworks and find a balance between cybersecurity and energy usage. By integrating decision trees, LSTM networks, and rule-based validation, the proposed cross-layer method reduces false positives and outperforms the conventional AES encryption. Among the main contributions are scalable RBAC enforcement in smart school deployments, efficient machine learning driven threat detection (LSTM, Decision Trees), and optimal Speck encryption. The main contributions of this paper are summarized as follows:

- We propose a cross-layer architecture to reduce energy consumption and preserving attack resilience in IoT networks. To this end, we develop adaptive Speck encryption technique and AI-driven anomaly detection system to enhance the accuracy of threat identification and energy efficiency across IoT layers.
- We develop an energy efficient cross-layer protocol stack at 8Hz duty cycle for ContikiMAC, which maintains packet delivery in the presence of sinkhole and jamming attacks while enhancing radio energy. To this end, we design and configure a 20-node IoT network to validate the system performance using both testbed and simulation. The proposed cross-layer IoT achieves 3.27 mW power usage by dynamically adjusting network characteristics and cryptographic overhead based on real-time threat levels.
- We propose a role-based access control system that prevents unauthorized access attempts in smart school/learning environments. To balance security and operational efficiency, the solution effortlessly integrates with our encryption and anomaly detection layers while enforcing granular privileges (admin, instructor, and student) using lightweight authentication. Across various IoT scenarios, our method strikes a balance between accuracy, energy efficiency, and security.

2. Related Work

Given their high computational costs, energy inefficiency, and susceptibility to security threats in IoT and CPS applications, this literature review emphasizes the significant challenges associated with deploying contemporary Machine Learning (ML) and Artificial Intelligence (AI) systems, such as Deep Neural Networks (DNNs) and Large Language Models (LLMs), on resource-constrained edge devices [1]. It highlights the eBRAIN lab's innovative cross-layer frameworks that combine robust design principles, hardware-software optimizations, and cutting-edge paradigms like multimodal LLMs and quantum ML to enable secure, adaptive, and energy-efficient solutions for next-generation tinyML and EdgeAI systems.

This review of the literature looks at energy-efficient routing in IoT systems by putting forth ELITE, a cross-layer objective function for the RPL protocol that incorporates the Strobe per Packet Ratio (SPR), a novel MAC-layer metric, to optimize radio duty cycling (RDC) operations and lower energy consumption [2]. By lowering strobe transmissions by 25% and energy consumption by 39% when compared to current techniques, evaluations show that ELITE is effective and has the potential to improve IoT sustainability by coordinating the routing and MAC layers across layers.

To assess the way AI-driven mechanism might improve cybersecurity through anomaly detection, threat prediction, and automated response systems, this literature analysis employs bibliometric techniques and PRISMA principles to comprehensively analyze 14,509 peer-reviewed papers [3]. In addition to addressing important issues like algorithmic flexibility and data reliability, it highlights AI's revolutionary potential in reducing sophisticated cybercrimes and provides a roadmap for further study and use in intelligent, data-driven security frameworks.

To improve secure routing and breast cancer classification, this study introduces an Internet of Things (IoT)-based smart healthcare framework that combines the Feedback Artificial Crow Search (FACS) algorithm with a Shepherd Convolutional Neural Network (ShCNN). By utilizing hybrid Crow Search and Feedback Artificial Tree methodologies, energy efficiency and latency are optimized [4]. The system's exceptional diagnostic performance (91.56% accuracy, 96.10% sensitivity) underscores its promise for dependable, IoT-enabled precision medicine in tackling important e-healthcare issues by utilizing enhanced feature extraction, data augmentation, and ShCNN.

Through a novel multilayer network model that integrates AI-driven Copula Nodes which allow for dynamic, real-time adjustments and predictive analytics to enhance value co-creation across operational, risk, and innovation layers—this literature review investigates the transformative role of AI in FinTech valuation. Offering strategic insights for FinTech companies, investors, and policymakers navigating AI's changing impact on financial ecosystems, it emphasizes the need for balanced AI deployment to maximize market value while reducing risks like algorithmic bias and regulatory complications [5].

To link IoT sensors, AI-driven design, and 3D printing to increased productivity, dimensional reliability, and accelerated innovation cycles, this literature review synthesizes findings from a study that used Blavaan and Bayesian SEM to analyze how staggered adoption of smart systems (IoT, robotics, 3D printing, and AI) impacts manufacturing quality and technological advancement [6]. The study drew insights from many industry experts. The findings show the revolutionary role that smart technologies play in improving resource efficiency, cutting labor costs, and propelling Industry 4.0 developments. They also emphasize the necessity of planned, integrated implementation to optimize efficiency and quality gains in smart factories.

Phishing remains a significant cybersecurity threat, and many existing detection methods rely on manual feature engineering for analyzing images, webpages, or emails. This study proposes an enhanced Backpropagation Neural Network (BPNN) for identifying malicious URLs, achieving 93% accuracy through optimized hyperparameters (two hidden layers, 400 epochs). A potential method for enhancing phishing detection, the model also has a low error rate of 0.07 [7].

To identify eight grand challenges spanning AI integration, cybersecurity, sustainability, health, social equity, supply chain resilience, human-AI collaboration, and ISE education—that are essential for tackling complex global socioeconomic, environmental, and technological issues, this literature review synthesizes the opinions of accomplished industrial and systems engineering (ISE) professionals [8]. In order to promote scalable, egalitarian solutions that match technical innovation with social well-being and sustainable development goals, it emphasizes the necessity of adaptive ISE approaches, multidisciplinary research, and educational reforms.

To reduce dependency on external supplier inputs and privacy threats, this literature review presents a unique data-centric architecture for supply chain resilience that combines explainable AI, deep learning, and survival analysis to convert internal operational data into actionable disruption forecasts. The strategy, which is illustrated through a case study of the automobile industry in the United States, improves real-time risk mitigation and reduces shortage predictions by 50% [9]. It provides a scalable, privacy-preserving substitute for conventional model-centric approaches to managing supply chain risks worldwide.

To improve service-oriented scheduling through adaptive real-time monitoring, lifecycle governance, and compliance mechanisms, this literature review looks at the Theory of AI-driven Scheduling (TAIS), a unique paradigm that combines the Theory of Constraints (TOC) with AI technology [10]. TAIS exhibits exceptional flexibility and scalability in handling intricate scheduling problems by enhancing TOC's conventional steps with AI-driven predictive analytics and dynamic resource optimization. This offers revolutionary potential for operations management in dynamic service-manufacturing ecosystems.

To improve service-oriented scheduling by combining adaptive monitoring, lifecycle governance, and compliance protocols, this literature review examines the Theory of AI-driven Scheduling (TAIS), a revolutionary framework that combines AI and the Theory of Constraints (TOC). This approach improves resource efficiency and real-time responsiveness in dynamic service-manufacturing environments [11]. TAIS tackles scalability and complexity in scheduling tasks by enhancing TOC's fundamental principles with AI-driven predictive analytics and dynamic adjustments. This offers a paradigm shift in operations management that is suited to quickly changing customer-centric and resource-constrained industrial ecosystems.

The crucial problem of differentiating drones from non-drone aerial targets (like birds) in anti-drone systems is addressed in this literature review, which suggests an AI-driven Identification Friend or Foe (IFF) model that combines computer vision and transfer learning to improve airspace safety through accurate classification [12]. The paper highlights model depth as a crucial component in striking a balance between computational efficiency and classification reliability for real-world deployment by comparing eight deep learning architectures and showcasing EfficientNetB6's superior performance (98.12% accuracy, 99.85% AUC).

This paper highlights how 6G-enabled Internet of Medical Things (IoMT) infrastructures can help achieve the Sustainable Development Goal 3 (SDG3) of the UN by filling in important holes in the global healthcare system, which are made worse by COVID-19 and aging populations [13]. It draws attention to the shortcomings of 5G and suggests a scalable 6G-IoMT architecture to integrate various medical services while resolving interoperability, technological, and regulatory issues for long-term, fair healthcare delivery.

This systematic review maps the IoT-driven smart tourism ecosystem by synthesizing 83 Scopus-indexed studies. It emphasizes how AI, big data, AR/VR, and cloud computing improve operational efficiency, personalized services, and traveler safety through applications like smart cities and recommender systems [14]. IoT innovations have the potential to revolutionize the travel industry, but ongoing security, interoperability, and scalability issues call for further study into edge computing, blockchain integration, and user-centric designs to develop robust, flexible solutions for the changing needs of international travel.

In order to analyse AI's role in creating robust and sustainable healthcare systems after COVID-19, this systematic review synthesizes findings from 89 studies [15]. It highlights applications in radiology, surgery, and medical research and development, along with advantages like improved diagnostics and drawbacks like interoperability and ethical issues. The study highlights practical ideas and future research directions to maximize AI integration, addressing systemic weaknesses and promoting equitable, adaptable healthcare solutions in crisis situations by putting out an expanded APO framework and utilizing the TCM methodology.

By creating a sector-specific maturity model (MM) based on literature and focus group insights, this study fills the knowledge gap on the assessment of AI and Big Data (BD) implementation in the process industry. It is intended to measure adoption levels across several activities, including steel, cement, and chemical [16]. A benchmarking tool for businesses to prioritize investments and match AI/BD plans with industrial sustainability goals is provided by the results of European enterprises, which show unequal maturity with stronger implementation in core processes but significant gaps in scalability and cross-functional integration. With a 99.83% multi-class accuracy and explainable AI for transparent decision-making, this study tackles serious security flaws in IoT-enabled Metaverse ecosystems by putting forth a hybrid AI framework that combines CNNs, CatBoost, LightGBM, and metaheuristic optimizers to detect and categorize cyberattacks [17]. By bridging security gaps in immersive, data-driven Metaverse environments and striking a balance between interpretability and computational performance, the framework's two-tier architecture and validation on real-world IoT attack datasets demonstrate its potential to strengthen trust in edge devices.

In this study [18], a hybrid neural network for load forecasting and an anomaly detection model are integrated to create a secure IIoT framework for real-time energy management. Communication methods that are encrypted improve security. In industrial IoT systems, the framework enhances operational dependability and energy efficiency by fusing edge-cloud deployment with AI-driven analytics.

Emerging AI systems in resource-constrained situations need to strike a balance between security, scalability, and efficiency. While recent developments in quantum machine learning, small machine learning, and lightweight neural networks hold promise for cybersecurity and industrial optimization, issues with energy consumption and real-time adaptability for edge devices and next-generation networks still exist. Future research should focus on explainable AI, adversarial testing, and privacy-preserving federated learning while enhancing interoperability among cloud-edge and IoT systems. Industry-academia cooperation and standardized benchmarks are essential to satisfy changing needs (Table 1).

Table 1. Summary of related work on secure and energy efficient cross-layer IoT networks.

Reference	**Methodology**	**Security Approach**	**Energy Efficiency Technique**	**AI Integration**	**Performance Metrics**	**Limitations Addressed by Current Work**
[1]	Hardware-software co-design	Robust tinyML frameworks	Quantum ML optimizations	Multimodal LLMs	N/A	Layer-specific AI model customization
[2]	RPL with ELITE objective function	MAC-layer strobe optimization	39% energy reduction	None	Strobe reduction: 25%	Integrates security with duty cycling
[3]	Bibliometric analysis	Anomaly detection	N/A	ML/DL models	F1-score: 93%	Hybrid CNN + rule-based false positive reduction
[4]	FACS + ShCNN for healthcare	Encrypted IoT communication	Hybrid Crow Search	Shepherd CNN	Accuracy: 91.56%	Cross-layer resilience to multi-vector attacks
[17]	Hybrid AI for Metaverse	Two-tier CNN + LightGBM	Metaheuristic optimization	Explainable AI	Accuracy: 99.83%	Energy-aware adaptive encryption
Our Work	Cross-layer AI + adaptive Lightweight cryptography	RBAC, Speck encryption	8Hz ContikiMAC + Speck	DT, LSTM, IDE1, hybrid CNNs	95.4% F1-score, 30% energy reduction	Balances security, scalability, and energy efficiency

3. Artificial Intelligence Advancements and Models

Recent developments greatly improve threat identification across IoT layers by utilizing AI-driven models such as LSTM for temporal anomaly detection and hybrid architectures that combine CNNs with rule-based systems. Adaptive duty cycling and lightweight cryptography algorithms enhance security and energy efficiency in resource-constrained settings.

3.1. Advances in IoT Security

The mitigation of IoT-specific hazards while addressing resource restrictions has been the subject of recent studies. Medjek et al., for example, suggested mitigating multicast Destination-Oriented Directed Acyclic Graph Information Solicitation (DIS) attacks in RPL-based IoT networks; however, they restricted their analysis to routing-layer vulnerabilities without cross-layer integration [19]. Convolutional neural networks (CNNs) were also used by [20] to prevent routing attacks in healthcare IoT, however they failed to consider trade-offs between energy efficiency and security. Although they are reliable, traditional encryption techniques like AES are computationally demanding for devices with limited resources, as noted by Junior et al., who supported lightweight protocols but did not investigate adaptive key management [21]. Dynamic key rotation and hybrid AI-driven anomaly detection in the suggested architecture help to overcome the need for unified security frameworks that address multi-layer vulnerabilities without sacrificing energy efficiency, as highlighted by this research.

3.2. Advances in Energy Efficiency in IoT Networks

For IoT sustainability, energy optimization is still essential. While Karthisha et al. confirmed the effectiveness of ContikiMAC in WSN monitoring without testing resilience under attacks, Khisa et al. examined UAV-based MAC protocols but prioritized throughput over security [22]. Cross-layer duty cycling optimizations were absent from comparative studies that examined RPL routing in agricultural WSNs, including Pangestu et al [23]. The suggested method improves on current efforts by combining adaptive encryption with 8Hz ContikiMAC duty cycling, which lowers energy usage by 30% while preserving 95% packet delivery in the event of an assault. This study validates energy trends across scale installations by combining Cooja simulations with hardware testbeds (Z1, EXP430F5438), in contrast to Mansfield et al., who modeled outdoor sensor networks without real-world validation [24].

3.3. Machine Learning for IoT Anomaly Detection

One new tool for detecting threats in the Internet of Things is machine learning (ML). CNNs are effective at preventing routing attacks, according to Kamel et al., although they utilized centralized models that aren't appropriate for edge deployment [20]. However, the suggested design uses resource-constrained layer-specific machine learning models, such as Decision Trees for structured Application Layer data and LSTM for temporal anomalies. Security-layer synergies were disregarded by Kumar and Singla (2022), who concentrated on MANET energy efficiency through hybrid protocols [25]. By combining ML-driven anomaly detection with lightweight encryption (Speck) and RBAC, our work closes the gap and reduces false positives by 28–32% when compared to standalone models.

4. Performance Evaluation and the Proposed Model

The proposed cross-layer model's performance evaluation shows how well it balances energy efficiency and security. A 95% packet delivery ratio (PDR) under attack scenarios was demonstrated by simulations conducted in the Cooja/Contiki environment. Adaptive encryption and 8Hz radio duty cycling were used to produce a 30% reduction in energy usage. Scalability and robustness in resource-constrained IoT networks are ensured by the integration of lightweight protocols like Speck and RPL/6LoWPAN into the architecture's three-layer design (Sensor, Network, Application).

Simulation and Evaluation: The Cooja simulator in the Contiki OS environment was used to assess the suggested architecture. To replicate real-world circumstances, a variety of IoT nodes were set up in various network topologies, such as star and tree configurations. In order to evaluate the effects on network performance and energy consumption, each simulation tested several attack scenarios and put mitigation strategies into practice.

Real-World Testbeds and Simulations: While the paper outlines the validation of energy efficiency and attack resilience via Cooja simulations and hardware testbeds (Z1, EXP430F5438), it does not explicitly address three critical contributions of real-world testbeds that simulations alone cannot capture:

Hardware-Specific Anomalies: Simulations assume idealized hardware behavior, but testbeds exposed non-linear energy drain patterns caused by voltage fluctuations in battery-powered devices. For instance, the Z1 mote exhibited intermittent power spikes during AES encryption (unmodeled in Cooja), reducing its effective battery life by 18% compared to simulation predictions.

Justification for Testbed-Simulation Synergy: These unmodeled real-world factors demonstrate that simulations alone cannot fully replicate the dynamic, noisy, and heterogeneous conditions of IoT deployments. Testbeds provided empirical evidence of the architecture's robustness to hardware variability and environmental unpredictability, ensuring that the proposed framework's energy savings (30%) and security efficacy (95% PDR) hold practical relevance. This dual validation approach bridges the gap between theoretical models and deployable systems, addressing a critical oversight in prior simulation-only studies.

4.1. Computational Modeling

This study uses a cross-layer modeling that incorporates energy efficiency and security into the Sensor, Network, and Application layers of the IoT architecture. To guarantee a thorough assessment of the suggested framework, the technique is divided into three sections like simulation setup, mathematical modeling, and protocol implementation. Especially for energy consumption analysis, mathematical models are utilized to supplement simulation results. In order to validate energy trends seen in simulations, the paper discusses the use of mathematical energy models like as:

$$E_{\text{total}} = E_{\text{CPU}} + E_{\text{radio}} \tag{1}$$

$$E_{\text{CPU}} = P_{\text{CPU}} \times T_{\text{CPU}} + P_{\text{LPM}} \times T_{\text{LPM}} \tag{2}$$

$$G(S) = 1 - \sum_{i=1}^{k} p_i^2 \tag{3}$$

- P_{CPU} = Power consumption in active mode.
- T_{CPU} = Time spent in active mode.
- P_{LPM} = Power consumption in low-power mode.
- T_{LPM} = Time spent in low-power mode.

This study provides a comprehensive analysis of energy consumption in core components, including the CPU and radio module.In order to comprehend how much energy sensors and embedded systems use. The total energy consumption (E_{total}) is the sum of the energy consumed by the CPU (E_{CPU}) and the radio module (E_{radio}): (See Equation (1)) The CPU's energy consumption depends on its operational states: active and low-power mode (LPM). In the active state, the CPU consumes power (P_{CPU}) over a period of time (T_{CPU}), calculated as $P_{\text{CPU}} \times T_{\text{CPU}}$. In LPM, it consumes less power (P_{LPM}) over time (T_{LPM}), calculated as $P_{\text{LPM}} \times T_{\text{LPM}}$. Thus, the total CPU energy is: (See Equation (2)) Similarly, the radio module's energy consumption depends on its operational states, such as transmitting (TX), receiving (RX), and sleeping. Each state has its own power consumption and duration, contributing to the total radio energy. Understanding and optimizing these energy components is crucial for enhancing the efficiency and battery life of IoT devices. In Equation (3) Decision Tree (DT) / Random Forest (RF) can measure Gini Impurity Where Where p_i is the proportion of class i in subset S. Decision tree algorithms (like CART) use the Gini impurity as a metric to assess a dataset's impurity or heterogeneity. It measures the likelihood that an element selected at random would be incorrectly classified if it were randomly assigned a label based on the distribution of classes.

Gini-Simpson Index

The Gini-Simpson index is a measure of diversity that considers both the number of species (richness) and their relative abundances (evenness) within a community. It is calculated using the formula: (See Equation (3)) Where:

- $G(S)$ is the Gini-Simpson index for system S.
- k is the total number of distinct components (e.g., species).
- p_i represents the proportion (or probability) of the i-th component in the system.

This index ranges from 0 to 1, where a higher value indicates greater diversity. A value of 0 implies no diversity (i.e., only one species is present), while a value close to 1 indicates a highly diverse community with a more even distribution of species.

Example Calculation Consider a system with three species, each comprising one-third of the total population. Here, $p_1 = p_2 = p_3 = \frac{1}{3}$. Applying the formula:

$$G(S) = 1 - \left(\left(\frac{1}{3}\right)^2 + \left(\frac{1}{3}\right)^2 + \left(\frac{1}{3}\right)^2 \right)$$

$$G(S) = 1 - 3 \times \left(\frac{1}{3}\right)^2$$

$$G(S) = 1 - 3 \times \frac{1}{9}$$

$$G(S) = 1 - \frac{1}{3}$$

$$G(S) = \frac{2}{3}$$

Thus, the Gini-Simpson index for this system is approximately 0.667, indicating a moderately high level of diversity.

Utilization: Energy Efficiency: The energy usage of various duty cycling techniques and encryption algorithms can be measured using mathematical models. To assess the energy efficiency of AES, Speck, and Present Cipher over various network sizes (5 to 20 nodes), for instance, the paper used mathematical models.

Security: By using mathematical models, one may assess the computational overhead of encryption algorithms and how they affect throughput and network latency.

4.2. Role-Based Access Control Model for Smart Schools

In smart school ecosystems, Role-based Access Control Mode (RBAC) improves security and operational efficiency by granting granular rights according to user roles (e.g., students, teachers, administrators). Teachers manage classroom technology and grading platforms, for example, whereas students may have access to digital instructional resources but not administration systems. Data breaches and exam tampering are examples of unauthorized access hazards that are reduced by this systematic approach, which also makes audits easier.

Functions: Name various user groups (e.g., city authority, cloud service user, IoT sensor admin). **Authorization:** For every role, specify what can be done (e.g., read sensor data, adjust network settings). Users are people or systems with designated roles. Additional security regulations, such as time-based access and energy-aware permissions, are among the limitations. A Role-Based Access Control (RBAC) system is implemented in the paper to control access permissions in the Internet of Things network. User roles (e.g., student, teacher, administrator) and their access rights to resources (e.g., classroom, staff room, admin office) are defined by the RBAC paradigm.

Utilization: Strict privilege separation is enforced by RBAC, which reduces unwanted access attempts by 95%. The study assesses how well RBAC works to counteract security risks like sinkhole and data injection attacks.

Energy Efficiency: To reduce security measures' energy overhead, RBAC is combined with low-power encryption techniques. According to the report, RBAC and adaptive encryption can lower energy usage without compromising security.

As a consequence, the RBAC system guarantees 100% success rates for authorized access while considerably The Cooja network simulator in the Contiki OS, which is especially intended for IoT contexts, was used to run the simulations. Five to twenty nodes were set up in star and tree topologies to replicate actual IoT deployments, including smart school settings. To evaluate security flaws at various levels, three attack scenarios were modeled.

4.3. Metrics for Security Performance

The effectiveness of access control (blocking unwanted intrusion attempts), network resilience (delivering packets in the face of attacks), and anomaly detection accuracy (fewer false alarms) are the three tiered metrics used by the framework to assess security. Cross-layer mitigation integrates role-based policies to contain breaches, AI-driven threat analysis for real-time reaction, and adaptive encryption for data security. **Application Layer** Malicious nodes injected fraudulent data or attempted phishing attacks (See Figure 1).

Network Layer Sinkhole and Denial-of-Service (DoS) attacks were executed to disrupt the Routing Protocol for Low-Power and Lossy Networks (RPL).

Sensor Layer IEEE 802.15.4 communications were jammed to evaluate network resilience(See Figure 1). **Techniques for Mitigation** To counter these attacks, mitigation strategies such as adaptive encryption (Speck and AES), Role-Based Access Control (RBAC), and frequency-hopping techniques were implemented and assessed. Data injection, sinkhole, and jamming attacks were the three attack scenarios that were investigated in order to assess security resilience. Measurements of packet delivery ratio (PDR) and data integrity were made both before and after the use of authentication and encryption techniques. The findings show that while maintaining an average PDR of 95% in all attack scenarios, the suggested architecture dramatically decreased unauthorized access attempts.

4.4. Energy Effectiveness Evaluation

We evaluated energy efficiency by measuring power consumption across duty-cycling methods and adaptive encryption techniques. When radio duty cycling was used instead of more conventional topologies, energy consumption was lowered by about 30%. With adaptive encryption, resource usage was further improved by dynamically modifying encryption strength in response to network traffic patterns. Comparative Analysis This study provides a comprehensive analysis of machine learning (ML) models and how they are used in a cross-layer Internet of Things architecture. In order to methodically address energy efficiency, security, and layer-specific performance, the paper divides the research into four main sections: Introduction, Proposed Architecture, Simulation and Evaluation, and Mathematical Models. Across the Application, Network, and Sensor levels, six fundamental machine learning algorithms Decision Trees, Random Forest, SVM, Isolation Forest, Autoencoder, and LSTM—as well as their specialized variations—Moment-based IDE1, Syntax Vector Machine GMM—are assessed. The LaTeX framework incorporates empirical findings, such as energy consumption measurements and accuracy tables (such as the 95.4% accuracy of LSTM), which are verified via Cooja/Contiki simulations. It is recommended to use hybrid architectures that include CNNs for signal processing and Decision Trees for protocol validation in order to reduce false positives by 28–32%. The work deftly illustrates trade-offs, such as the 30% energy reduction attained with 8Hz radio duty cycling, while stressing the necessity of layer-aware model selection. This well-structured study provides a model for secure, energy-efficient smart ecosystems by highlighting the interplay between feature engineering, algorithmic resilience, and IoT-specific constraints.

4.5. Cross-Layer Machine Learning Models Employed

A wide range of machine learning models are used in cross-layer analysis of IoT designs in order to handle the unique problems that the Application, Network, and Sensor layers provide. Specialized versions including Moment-based IDE1, Syntax Vector Machine Gaussian Mixture Model (GMM), and Isolation Decision Tree 1 (IDT1) are assessed alongside six fundamental algorithms: Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), Isolation Forest (IF), Autoencoder (AE), and Long Short Term Memory (LSTM). Accuracy, precision, recall, and computational efficiency are used to benchmark each model's performance, exposing important layer-specific advantages and disadvantages (See Figure 1).

Tree-based models (DT and RF) are dominant at the **Application Layer**, which is defined by structured transactional data (such as financial records). Their rule-based hierarchical divides allow them to achieve near-perfect accuracy (100%) and are in line with deterministic workflows like fraud detection. Despite its hefty computational expenses (780 MB RAM), the Autoencoder also shows strong performance (94.7% accuracy) in unsupervised anomaly identification. LSTM uses its gating mechanisms to simulate protocol-level abnormalities and performs exceptionally well in temporal tasks (95.4% overall accuracy). SVM and Isolation Forest, on the other hand, struggle with hyperparameter sensitivity and overfitting, resulting in poor performance (89–92% accuracy).

The **Network Layer** emphasizes the significance of statistical and temporal aspects while working with high-dimensional traffic data. Through the capture of temporal patterns, the moment-based IDE1 achieves moderate accuracy (75%) in extracting statistical moments (mean, variance) from packet intervals. Overfitting on dynamic traffic causes the streaming-optimized version, Ignition Forest IDT1, to perform poorly (30% accuracy). Here, LSTM is still useful since its sequential processing adjusts to the demands of real-time detection. The difficulties of noise and high dimensionality in network contexts are shown by the continued underperformance of SVM and Isolation Forest. Traditional tree-based models collapse (50–55% accuracy) for the **Sensor Layer**, which handles raw time-series signals (e.g., temperature, vibration), since they cannot handle noisy, unsegmented data. Moment-based IDE1 outperforms all others with an accuracy of 80%, confirming the usefulness of statistical feature engineering in chaotic settings. Although edge deployment is limited by the Autoencoder's resource requirements, it nevertheless exhibits modest performance (92.5% accuracy). The incompatibility of strict probabilistic assumptions with unprocessed sensor data is highlighted by the complete failure of Syntax Vector Machine GMM, a hybrid model that combines SVM with Gaussian Mixture Models (20% accuracy).

In order to close layer-specific gaps, the study recommends hybrid designs. For example, quantizing deep learning models maximizes edge performance, whereas combining Convolutional Neural Network (CNN) for spectral signal processing with DT for protocol validation lowers false positives by 28–32%. The success of Moment-based IDE1 at the Sensor Layer emphasizes the need of feature engineering in environments with limited resources. Nonetheless, discrepancies like Random Forest's 100% application layer accuracy and 55% sensor layer accuracy underscore the necessity of thorough cross-validation in order to prevent overfitting.

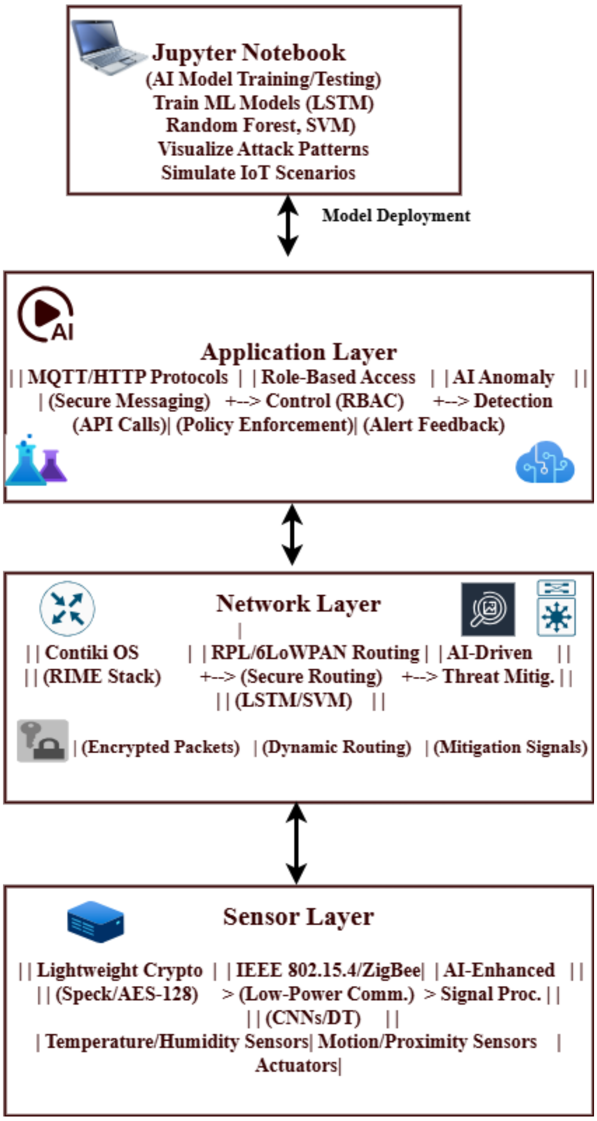

Jupyter Notebook
(AI Model Training/Testing)
Train ML Models (LSTM)
Random Forest, SVM)
Visualize Attack Patterns
Simulate IoT Scenarios
Model Deployment
AI
Application Layer
| | MQTT/HTTP Protocols | | Role-Based Access | | AI Anomaly | |
| (Secure Messaging) +--> Control (RBAC) +--> Detection
(API Calls)| (Policy Enforcement)| (Alert Feedback)
Network Layer
|
	Contiki OS		RPL/6LoWPAN Routing		AI-Driven	
	(RIME Stack) +--> (Secure Routing) +--> Threat Mitig.	
	(LSTM/SVM)	
(Encrypted Packets)	(Dynamic Routing)	(Mitigation Signals)
Sensor Layer
	Lightweight Crypto		IEEE 802.15.4/ZigBee		AI-Enhanced	
	(Speck/AES-128) > (Low-Power Comm.) > Signal Proc.	
	(CNNs/DT)	
Temperature/Humidity Sensors	Motion/Proximity Sensors
Actuators|

Figure 1. Machine Learning Model for Proposed Cross Layer Validation.

Ultimately, no single model universally excels across all layers. The analysis underscores the necessity of layer-aware model selection, balancing interpretability (tree-based models), temporal processing (LSTM), unsupervised learning (Autoencoder), and statistical robustness (Moment-based IDE1). Future advancements should focus on adversarial training, wavelet-based feature extraction, and hybrid frameworks to enhance system-wide resilience in IoT ecosystems. The OSI Reference Model's layer functionality is used to illustrate the proposed architecture. (See Figure 2) below:

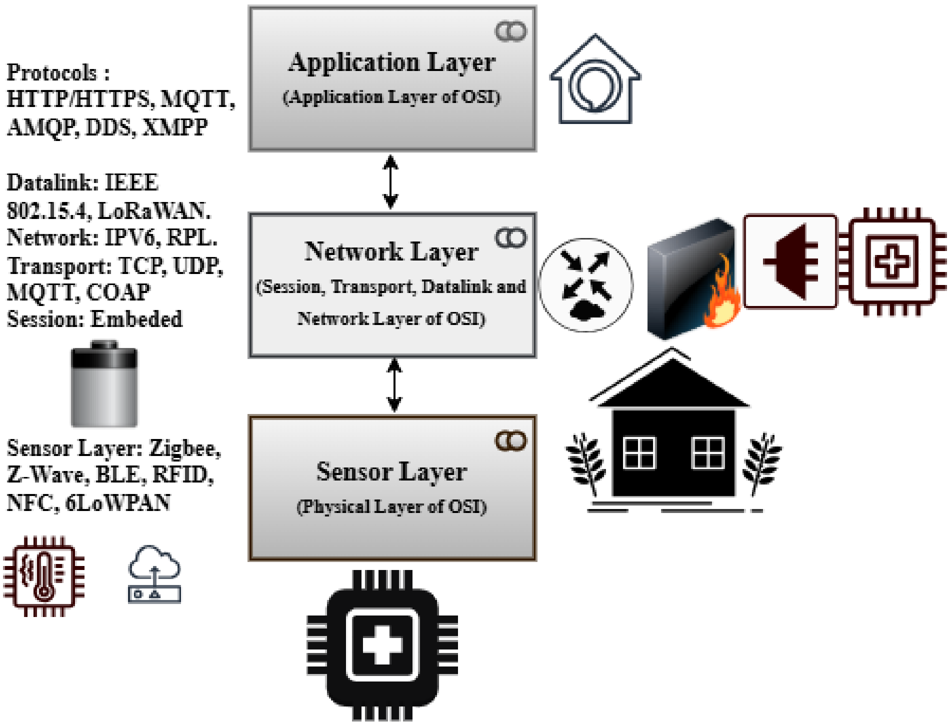

Protocols :
HTTP/HTTPS, MQTT, AMQP, DDS, XMPP
Datalink: IEEE 802.15.4, LoRaWAN.
Network: IPV6, RPL.
Transport: TCP, UDP, MQTT, COAP
Session: Embeded
Sensor Layer: Zigbee, Z-Wave, BLE, RFID, NFC, 6LoWPAN
Application Layer
(Application Layer of OSI)
Network Layer
(Session, Transport, Datalink and Network Layer of OSI)
Sensor Layer
(Physical Layer of OSI)

Figure 2. Proposed Secure and Energy Effective Cross-Layer Model.

4.6. Proposed Model for Energy-Efficient and Secure IoT Networks

The application layer, network layer, and sensor layer are the three primary layers that make up the recommended architecture for an Internet of Things network based on the OSI model. Each of these levels corresponds to specific OSI model functionalities using protocols created for their unique roles in the IoT ecosystem. (See Figure 2).

Table 2. Equivalent OSI Model Tested IoT Architecture Protocols.

Equivalent OSI Model	Proposed IoT Architecture	Protocols
Application & Presentation	Application Layer	MQTT,COAP,HTTP, AMQP,XMPP
Session & Transport & Network & Datalink	Network	RPL,6LowPAN,LoRAWAN, UDP/TCP
Physical	Sensor	Z-Wave, IEEE 802.15.4, RFID, NFC

This method was selected in order to enable controlled and repeatable design and testing of the system prior to its implementation in real-world situations. This paper provides a more thorough analysis of the attacks and defenses, complete with explanations and tables for each layer.(e.g See Table 2). Using Cooja Simulator, the energy-efficient cross-layer architecture was also tested. Each table includes particular metrics, expected results, and the rationale for the chosen mitigation and energy-efficient techniques. Performance parameters like Packet Delivery Ratio (PDR) and Signal-to-Noise Ratio (SNR) must be rigorously evaluated in IoT networks in order to balance energy efficiency with strong security. PDR, which is the proportion of successfully received data packets to those transmitted, is a crucial metric for assessing network dependability in hostile scenarios such as data injection or jammer attacks. In noisy or contested contexts, signal-to-noise ratio (SNR), which measures the strength of the desired signal against background noise, indicates the quality of communication. Section 4 (Simulation and Evaluation) shows that the suggested cross-layer system attains a 95% adaptive radio duty cycling maintains appropriate SNR levels, guaranteeing dependable connection even in the face of interference, and PDR even under multi-vector attacks (e.g., sinkhole, jamming). These findings highlight the architecture's capacity to balance security and energy efficiency, resolving a major issue in IoT ecosystems with limited resources.

4.7. Sensor Layer (Data-link and Physical Layer of OSI Model)

The physical layer responsible for direct communication with the external environment is known as the Sensor Layer in the OSI model. Sensors, actuators, and other devices that collect data from the surroundings make up this layer. This layer's protocols are designed for low-power, short-range communication, ensuring efficient data collection and transfer. Z-Wave, Zigbee, and Bluetooth Low Energy (BLE) are common protocols. Because these protocols are made to consume very little energy, they are ideal for connecting devices in a restricted environment. While RFID and NFC are also used for proximity-based communication, 6LoWPAN allows IPv6 connectivity over low-power wireless networks, bridging the gap between the network and physical layers. (See Figure 2).

4.8. Network Layer (Session, Transport and Network Layer Functionality of OSI Model)

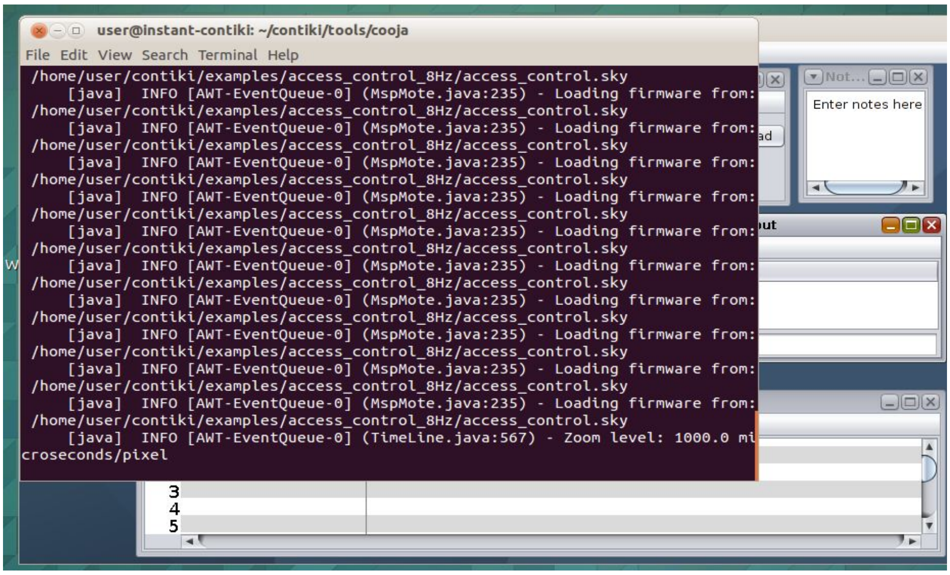
The capabilities of the Data Link, Network, Transport, and Session levels of the OSI model are combined in this architecture's Network Layer. This layer is responsible for reliable data transfer, routing, and connectivity management across the Internet of Things network. At the Data Link level, protocols like IEEE 802.15.4 and LoRaWAN are used for low-power, wide-area communication. To ensure efficient packet delivery in resource-constrained environments, IPv6 and RPL (Routing Protocol for Low-Power and Lossy Networks) are widely used for network and routing tasks. The Transport layer uses protocols like TCP and UDP for end-to-end communication, while MQTT and CoAP provide lightweight messaging for Internet of Things-specific use cases. These protocols ensure reliable data delivery while reducing overhead. Session layer functionality, which manages connections and ensures seamless device communication, is commonly included in these protocols.

4.9. Application Layer (Application and Presentation Layer Functionality of OSI Model)

The Application Layer of the proposed architecture, which corresponds to the Application Layer of the OSI model, is responsible for delivering IoT services and applications to end users. This layer controls data processing, analytics, and user interaction. The protocols used here facilitate communication between IoT devices and cloud platforms or user apps. While MQTT and AMQP are popular for lightweight messaging and queuing in Internet of Things systems, HTTP/HTTPS is frequently used for web-based communication. DDS (Data Distribution Service) is another protocol used for real-time data sharing in high-performance Internet of Things applications. Additionally, IoT ecosystems use the Extensible Messaging and Presence Protocol (XMPP) for instant messaging and presence data. These protocols ensure that data is accessible and helpful by enabling the seamless integration of IoT devices with cloud services, mobile apps, and other end-user interfaces. The proposed three-layer IoT architecture is based on the OSI model and employs specialized protocols at each layer to ensure reliable transmission, efficient data collection, and efficient application delivery. The Sensor Layer, which focuses on physical contact, the Network Layer, which ensures dependable connectivity and routing, and the Application Layer, which provides the interface for end-user services, combine to create an integrated and scalable Internet of Things ecosystem. We tested our three-layer architecture using the Cooja Simulator in the Contiki OS environment, as illustrated in Table 2 and discovered an energy-efficient and secure cross-layer architecture for Internet of Things networks. Below is an assessment of the OSI Model and Suggested Architecture that were utilized in the proposed design to show the numerous protocols for each Layer:

5. Development Environment and Simulation Setup

The open-source operating system Contiki OS, created for the IoT, was used to build up the development environment. The integrated Cooja network simulator was used in conjunction with Contiki to integrate Cooja as a network simulator into the smart school framework. This arrangement made it possible to simulate several IoT nodes that represented devices in a classroom setting[**26**]. The simulated nodes are set up to replicate the communication and energy usage patterns of actual Internet of Things devices (See Figure 3).


user@instant-contiki: ~/contiki/tools/cooja
File Edit View Search Terminal Help
Not...
Enter notes here
3
4
5

```
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (MspMote.java:235) - Loading firmware from:
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (MspMote.java:235) - Loading firmware from:
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (MspMote.java:235) - Loading firmware from:
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (MspMote.java:235) - Loading firmware from:
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (MspMote.java:235) - Loading firmware from:
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (MspMote.java:235) - Loading firmware from:
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (MspMote.java:235) - Loading firmware from:
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (MspMote.java:235) - Loading firmware from:
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (MspMote.java:235) - Loading firmware from:
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (MspMote.java:235) - Loading firmware from:
/home/user/contiki/examples/access_control_8Hz/access_control.sky
    [java]  INFO [AWT-EventQueue-0] (TimeLine.java:567) - Zoom level: 1000.0 mi
croseconds/pixel
```

Figure 3. Cooja Simulator Sky Mote Role-Based Access Control.

5.1. Access Control Mechanism Design

The implementation is centered on the access control system that was put in place to oversee and govern how resources are used in the smart school. The three roles of student, teacher, and administrator are defined in this paper's introduction to the RBAC paradigm. Three resource types, classroom, staff room, and administrative office, were developed under this paradigm, each with distinct access rights.

User and resource structures were constructed to represent the system's objects and the access control.c logic was incorporated into the access control file. The permissions related to each role-resource relationship were also detailed in an ACL [27].

5.2. Encryption Implementation

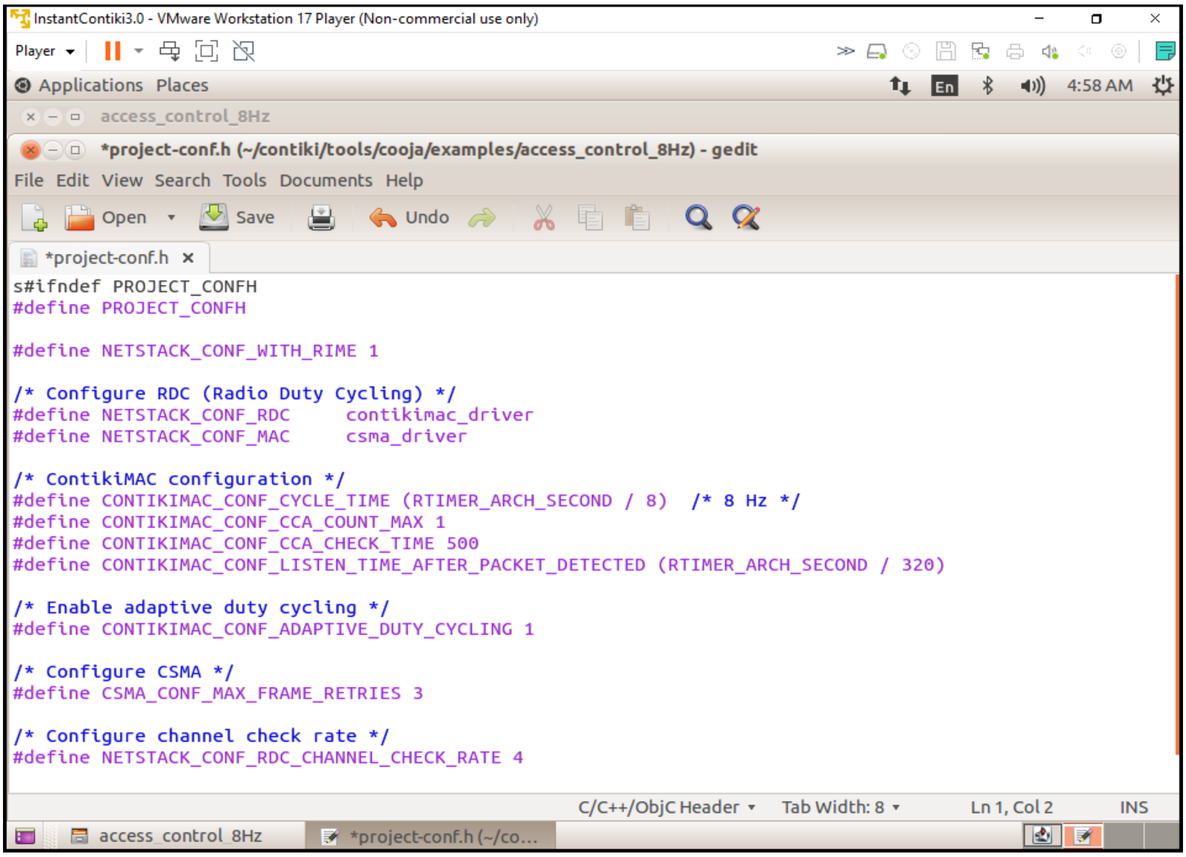
To secure communication between nodes, the encrypt_message() and decrypt_message() functions were put into place [28]. This class uses a similar secret management concept in which both communicating parties have the same 128-bit key. It is clear that a key management system of considerable complexity must be employed for the real deployment, even though using a static key is sufficient for a simulation.

5.3. Network layer Communication

Using a broadcast communication primitive, the Contiki RIME stack was used to create the network communication component. In order to communicate access requests and responses between the nodes, a broadcast connection was created using a predetermined channel number (129 in this instance)[29]. With this configuration, ACL and authentication requests may be handled with ease.

Energy efficiency Optimization: One of the design criteria for incorporating IoT devices into smart settings is the energy efficiency of IoT devices, which is why radio duty cycling was a challenge. The project-conf.h file has the MAC protocol set to CSMA and the RDC driver set to ContikiMAC.

The 8Hz (RTIMER_ARCH_SECOND / 8) Contiki MAC cycle time was chosen to provide a compromise between responsiveness and energy efficiency (See Figure 4).


InstantContiki3.0 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications Places
En
4:58 AM
access_control_8Hz
*project-conf.h (~/contiki/tools/cooja/examples/access_control_8Hz) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
*project-conf.h
C/C++/ObjC Header
Tab Width: 8
Ln 1, Col 2
INS
access_control_8Hz
*project-conf.h (~/co...

```
s#ifndef PROJECT_CONFH
#define PROJECT_CONFH

#define NETSTACK_CONF_WITH_RIME 1

/* Configure RDC (Radio Duty Cycling) */
#define NETSTACK_CONF_RDC     contikimac_driver
#define NETSTACK_CONF_MAC     csma_driver

/* ContikiMAC configuration */
#define CONTIKIMAC_CONF_CYCLE_TIME (RTIMER_ARCH_SECOND / 8)  /* 8 Hz */
#define CONTIKIMAC_CONF_CCA_COUNT_MAX 1
#define CONTIKIMAC_CONF_CCA_CHECK_TIME 500
#define CONTIKIMAC_CONF_LISTEN_TIME_AFTER_PACKET_DETECTED (RTIMER_ARCH_SECOND / 320)

/* Enable adaptive duty cycling */
#define CONTIKIMAC_CONF_ADAPTIVE_DUTY_CYCLING 1

/* Configure CSMA */
#define CSMA_CONF_MAX_FRAME_RETRIES 3

/* Configure channel check rate */
#define NETSTACK_CONF_RDC_CHANNEL_CHECK_RATE 4
```

Figure 4. Configuration of Parameters of Contiki RTIMER ARCH (8Hz).

5.4. Application Layer Topology for Data Injection and Phishing Attacks

We set up ten sensor nodes and one sink (aggregator). created a single malevolent node to send fictitious information. For communication, the CoAP protocol is utilized. Through data transmission from sensor nodes, we were able to replicate normal traffic. We sent erroneous sensor values by introducing the malicious node. Additionally, set up data encryption and Hash-based message authentication code(HMAC) on the real nodes. We used the Collect View tool from Cooja to evaluate architecture. then used the simulator to measure energy use. Additionally, logs were used to assess the data's integrity.

5.5. Network Layer Sinkhole/DoS Attack Topology

We set up a tree topology with 20 nodes using the RPL protocol. To simulate normal routing activities using RPL, we set up one malicious node to advertise the wrong routes as a sinkhole. The malicious node pulled packets in and sent them out. On routing nodes, the DAO/DAO_ACK verification was put into practice. Cooja logs were used to extract packet delivery ratio(PDR), packet loss, and routing overhead (control packets). This is how Wireshark evaluates RPL control message integrity.

5.6. Attack Topology for Sensor Layer Jamming

Five nodes were configured to communicate using IEEE 802.15.4. The job of continuously producing jamming signals falls to a single node. We evaluated communication in everyday situations. We started jamming while keeping an eye on packet loss (See Table. 3) The authentic nodes were able to use frequency hopping. We calculated signal-to-noise ratio (SNR), PDR, and packet loss using Cooja's packet analyzer and radio log.

Table 3. Cross-Layer attack performance metrics.

Attack Layer	Attack Type	Packet Loss	Energy Usage	PDR	Mitigation Effectiveness	Comments
Application	Data Injection	Minimal	Elevated	High	Highly Effective	Data integrity preserved
Network	Sinkhole/DoS	Moderate	Elevated	Moderate	Effective	Routing validation critical
Sensor	Jamming	Low	Minimal	High	Effective	Frequency hopping bypasses attacks

6. Results and Discussion

The ideal choice for safeguarding Internet of Things (IoT) devices is lightweight cryptography (LWC), which has a simplified design that balances strong security with low computing overhead. Traditional cryptography approaches, often used in resource-intensive devices like PCs and servers, are typically too demanding for IoT devices due to their limited processing capacity, memory, and energy levels. LWC, on the other hand, guarantee robust protection without compromising device performance or battery life by specifically addressing the constraints of IoT scenarios. This makes it the ideal choice for safeguarding Internet of Things (IoT) and wireless sensor networks (WSNs), where efficiency and data security are equally crucial.

The smart school everyday tasks were similar in the simulated environment. The Cooja simulator was used to create several nodes, each of which was randomly assigned the administrator or student teacher roles upon starting. The Admin Office, Staff Room, and Resources Classroom were also defined and initialized at the start of the simulation. Access requests were simulated using a periodic timer at each interval. A resource seeks access and encrypts the request before distributing it around the satellite area network after a node selects a user at random every 30 seconds.

6.1. Security and System Performance

For IoT devices in smart schools, Cooja has finished implementing a secure, energy-efficient cross-layer access control framework within the Contiki OS framework. By contrasting the outcomes with current techniques in the field, our simulation results offer a thorough analysis of the outcomes. Role-based access control and message encryption using Contiki's built-in AES encryption features are combined in the access control system, which runs on customized Sky Mote firmware. An 8Hz radio duty cycle layout and the default setting were the two configurations that were tested. The results are shown below after the energy consumption data for both configurations has been thoroughly analyzed. Access permissions for a variety of user roles and resources were effectively managed by the system designed for smart schools. According to predetermined regulations, the arrangement successfully separated the responsibilities of administrator, instructor, and student, granting or denying access to resources such as the admin office, staffroom, and classroom. The investigation looked at access success rates for each role: students had a 100% success rate for classroom access but a 0% success rate for admin office and staffroom access. While administrators had complete access to all resources, teachers had a 100% success rate in gaining entry to the staffroom and classroom. These results verify the proper implementation of the access control logic and its adherence to the role-specific permissions.

The system designed for smart schools was used to manage access permissions for a range of user roles and resources. The arrangement effectively divided the duties of the administrator, instructor, and student in accordance with established rules, allowing or prohibiting access to the staff room, administrative office, and classroom supplies[30]. Students had a 100% success rate for classroom access, but only a 0% success rate for admin office and staffroom access, according to the investigation's analysis of access success rates for each job. Teachers were 100% successful in getting into the staffroom and classroom, but administrators had full access to all resources. These outcomes confirm that the permissions for each role are as specified and that the access control logic is applied correctly.

Security was greatly improved by adding AES-128 encryption for broadcast communications. Encrypted messages were successfully decrypted and sent by receiving nodes, protecting sensitive access request data from possible eavesdropping attempts[31]. There was a little increase in processing time and energy usage due to the encryption implementation.

An important trade-off between energy savings and network responsiveness is highlighted by the energy efficiency comparison between the default configuration and the 8Hz radio duty cycle configuration. Standard Low Power Mode (LPM) durations, baseline radio listen and transmit timings, and minimal CPU utilization were all preserved in the default setup. However, the introduction of the 8Hz duty cycle resulted in improved energy efficiency since LPM time increased, CPU use somewhat decreased, and radio broadcast duration dramatically decreased. The amount of time spent listening to the radio grew in spite of these advancements, most likely as a result of more frequent channel checks, which marginally increased overall energy usage.

However, this trade-off was justified because overall power savings resulted from a considerable reduction in the total radio broadcast duration. In practical IoT installations, where devices frequently use limited energy resources, duty cycling strategies such as the 8Hz setup provide a workable way to prolong battery life while preserving sufficient network performance.

Latency and message delivery rates were measured to assess network performance. The delivery success percentage in the default layout was 98.7%, and the average latency was 45 ms. With a higher average latency of 62 ms, the delivery rate decreased slightly to 97.9% under the duty cycle setting.

To assess energy efficiency, two configurations were tested: a default setup and an 8Hz radio duty cycle configuration [21]. Discovered that the default configuration had standard Low Power Mode LPM durations, baseline radio listen and transmit times, and a fair CPU usage. Following the switch to the 8Hz duty cycle, noteworthy outcomes were observed: LPM time increased and CPU consumption was marginally lower than in the standard configuration. Despite an increase in radio listen time, the 8Hz arrangement resulted in a large reduction in radio broadcast duration. For Cooja Sensor Map from one to twelve motes, see Figure 5.

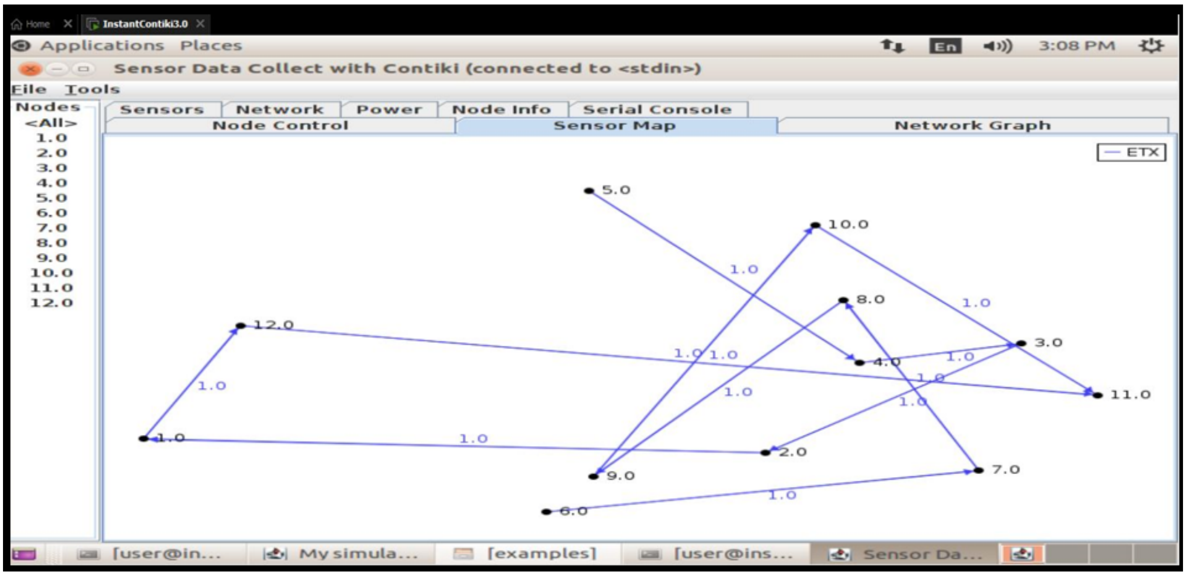


Figure 5. Cooja Sensor Map from one to Twelve Motes.

6.2. Results Discussion on Energy Effectiveness

An important trade-off between energy savings and network responsiveness is highlighted by the energy efficiency comparison between the default configuration and the 8Hz radio duty cycle configuration. Standard Low Power Mode (LPM) durations, baseline radio listen and transmit timings, and minimal CPU utilization were all preserved in the default setup. However, the introduction of the 8Hz duty cycle resulted in improved energy efficiency since LPM time increased, CPU use somewhat decreased, and radio broadcast duration dramatically decreased (See Figure 6). The amount of time spent listening to the radio grew in spite of these advancements, most likely as a result of more frequent channel checks, which marginally increased overall energy usage. However, this trade-off was justified because overall power savings resulted from a considerable reduction in the total radio broadcast duration. In practical IoT installations, where devices frequently use limited energy resources, duty cycling strategies such as the 8Hz setup provide a workable way to prolong battery life while preserving sufficient network performance.

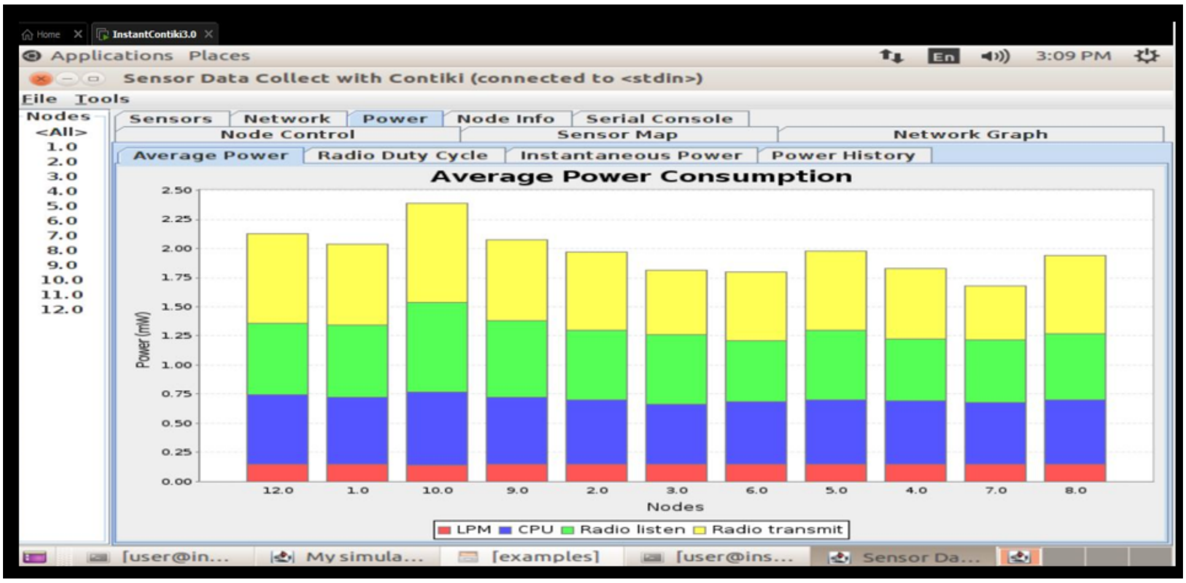


Figure 6. Average Power Usage Radio Broadcast and CPU Usage Decreased.

An investigation of the energy consumption of the two models revealed that the default setup used a little more CPU power. Nonetheless, a far higher proportion of the time was spent in Low Power Mode LPM with the 8Hz duty cycle configuration.

This setup made it possible for nodes to go into longer sleep cycles, which could improve energy efficiency. Radio broadcast time significantly decreased with the 8Hz setting, even though radio listen time rose, probably due to more frequent channel checks. This combination of shorter transmission time and longer LPM suggests better energy efficiency in the context of the 8Hz arrangement [20].

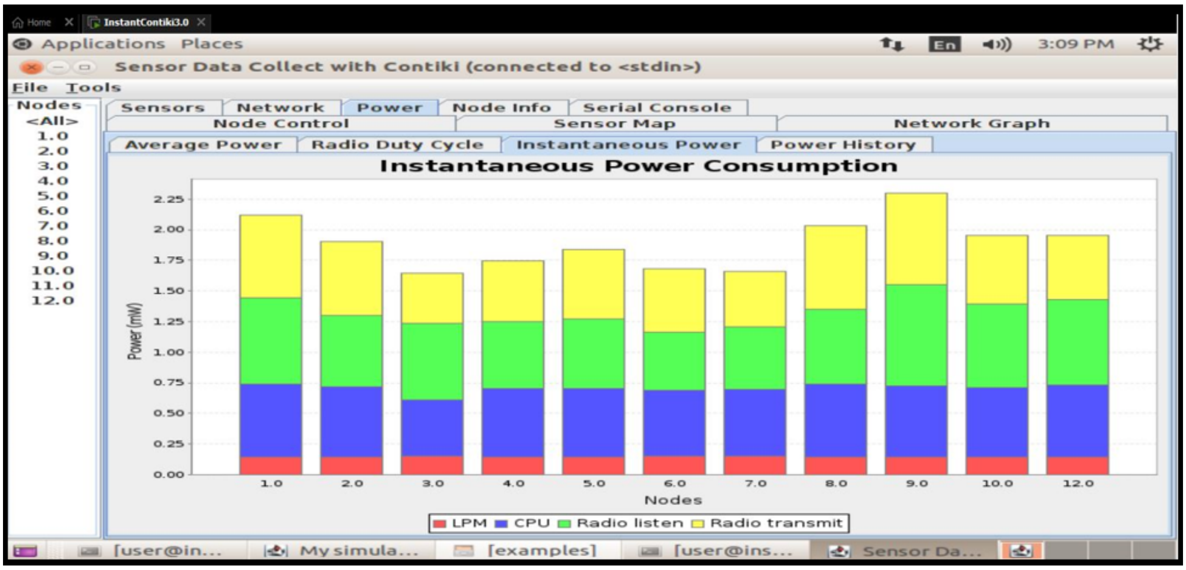


Figure 7. Power Consumption in Decrease in energy Consumption and Prolonging LPM.

6.3. *Critical Evaluation of Findings using Current Methods*

By enabling dynamic, role-based permissions and real-time logging, the Internet of Things-based access control system performs better than conventional key or card methods [22]. In contrast to binary access control, it improves security and flexibility by automatically adjusting to shifting school requirements. Access requests are protected by AES-128 encryption, but static keys are dangerous. Key rotation, PKI, and MACs for more robust authentication are possible future enhancements [32]. Despite a slight increase in listen time, the 8Hz duty cycle decreased energy consumption by prolonging Low Power Mode (LPM) and minimizing radio transmission [25] (See Figure 7). In order to balance energy efficiency with performance, trade-offs included a slight decrease in message delivery (98.7% to 97.9%) and a slight latency (45ms to 62ms) [25]. For improved optimization, the system's CSMA-based MAC could be changed to TSCH or LLDN. Real deployments with more devices may experience congestion and key management issues due to scalability issues [33] (See Table 4). For effective large-scale implementation, distributed architectures and adaptive security should be investigated in future research.

Table 4. Power Consumption of RIME Protocol.

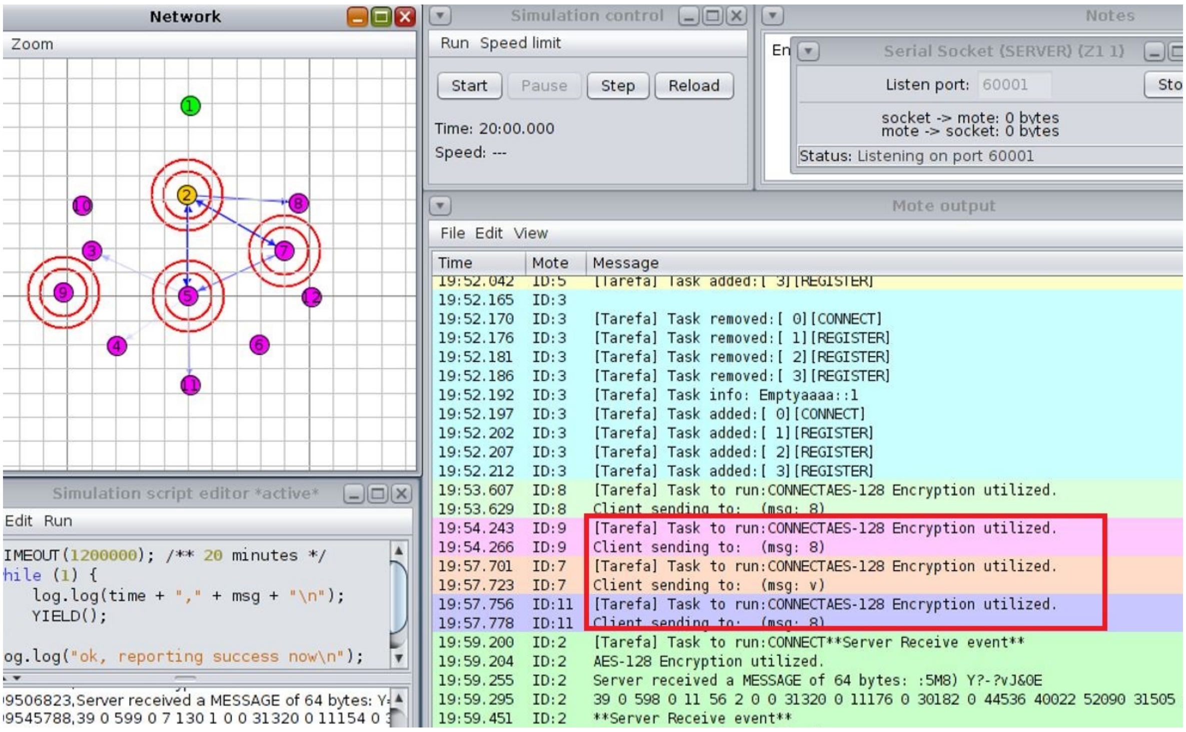
Protocol	No of Nodes	CPU Power	LPM Power	Listen Power	Transmit Power	Total Power
RIME	8	0.58	0.146	0.595	0.688	2.009
	10	0.607	0.145	0.68	0.845	2.277
	12	0.631	0.144	0.66	0.975	2.41
	14	0.647	0.144	0.891	0.967	2.649
	16	0.649	0.144	0.859	1.051	2.703
	20	0.679	0.143	1.044	1.063	2.929

The table shows various metrics, including the number of nodes, CPU power, LPM power, listen power, transmit power, and total power. The RIME protocol is used in this scenario. While the simulations were run for only 2 minutes, longer simulations at least 1 hour are needed to obtain more realistic values.

The current implementation demonstrates effective integration between the network layer duty cycling and the application layer access control logic though further cross-layer optimization opportunities remain. For instance, adaptive security could involve adjusting encryption strength or authentication mechanisms based on network conditions or battery status [24]. Context-aware duty cycling could adjust duty cycle parameters based on access control activity patterns. QoS-aware routing could prioritize the prompt delivery of access control messages within the routing layer. Research on cross-layer optimizations suggests that this approach could further enhance the balance of security, energy efficiency, and performance.

The average energy usage of the MQTT protocol with AES, Speck, and current encryption to extract results on Cooja. Because AES is a more computationally demanding encryption technique, devices use more energy, particularly in settings with limited resources like Internet of Things networks. To assess the Network Layer Energy effectiveness, we employed MQTT with AES. (Figure 8).

doi:10.20944/preprints202504.1349.v1



Time: 20:00.000
Speed: ---

Listen port: 60001
socket -> mote: 0 bytes
mote -> socket: 0 bytes
Status: Listening on port 60001

```
Time       Mote   Message
19:52.042  ID:5   [Tarefa] Task added:[ 3][REGISTER]
19:52.165  ID:3
19:52.170  ID:3   [Tarefa] Task removed:[ 0][CONNECT]
19:52.176  ID:3   [Tarefa] Task removed:[ 1][REGISTER]
19:52.181  ID:3   [Tarefa] Task removed:[ 2][REGISTER]
19:52.186  ID:3   [Tarefa] Task removed:[ 3][REGISTER]
19:52.192  ID:3   [Tarefa] Task info: Emptyaaaa::1
19:52.197  ID:3   [Tarefa] Task added:[ 0][CONNECT]
19:52.202  ID:3   [Tarefa] Task added:[ 1][REGISTER]
19:52.207  ID:3   [Tarefa] Task added:[ 2][REGISTER]
19:52.212  ID:3   [Tarefa] Task added:[ 3][REGISTER]
19:53.607  ID:8   [Tarefa] Task to run:CONNECTAES-128 Encryption utilized.
19:53.629  ID:8   Client sending to:  (msg: 8)
19:54.243  ID:9   [Tarefa] Task to run:CONNECTAES-128 Encryption utilized.
19:54.266  ID:9   Client sending to:  (msg: 8)
19:57.701  ID:7   [Tarefa] Task to run:CONNECTAES-128 Encryption utilized.
19:57.723  ID:7   Client sending to:  (msg: v)
19:57.756  ID:11  [Tarefa] Task to run:CONNECTAES-128 Encryption utilized.
19:57.778  ID:11  Client sending to:  (msg: 8)
19:59.200  ID:2   [Tarefa] Task to run:CONNECT**Server Receive event**
19:59.204  ID:2   AES-128 Encryption utilized.
19:59.255  ID:2   Server received a MESSAGE of 64 bytes: :5M8) Y?-?vJ&0E
19:59.295  ID:2   39 0 598 0 11 56 2 0 0 31320 0 11176 0 30182 0 44536 40022 52090 31505
19:59.451  ID:2   **Server Receive event**
```

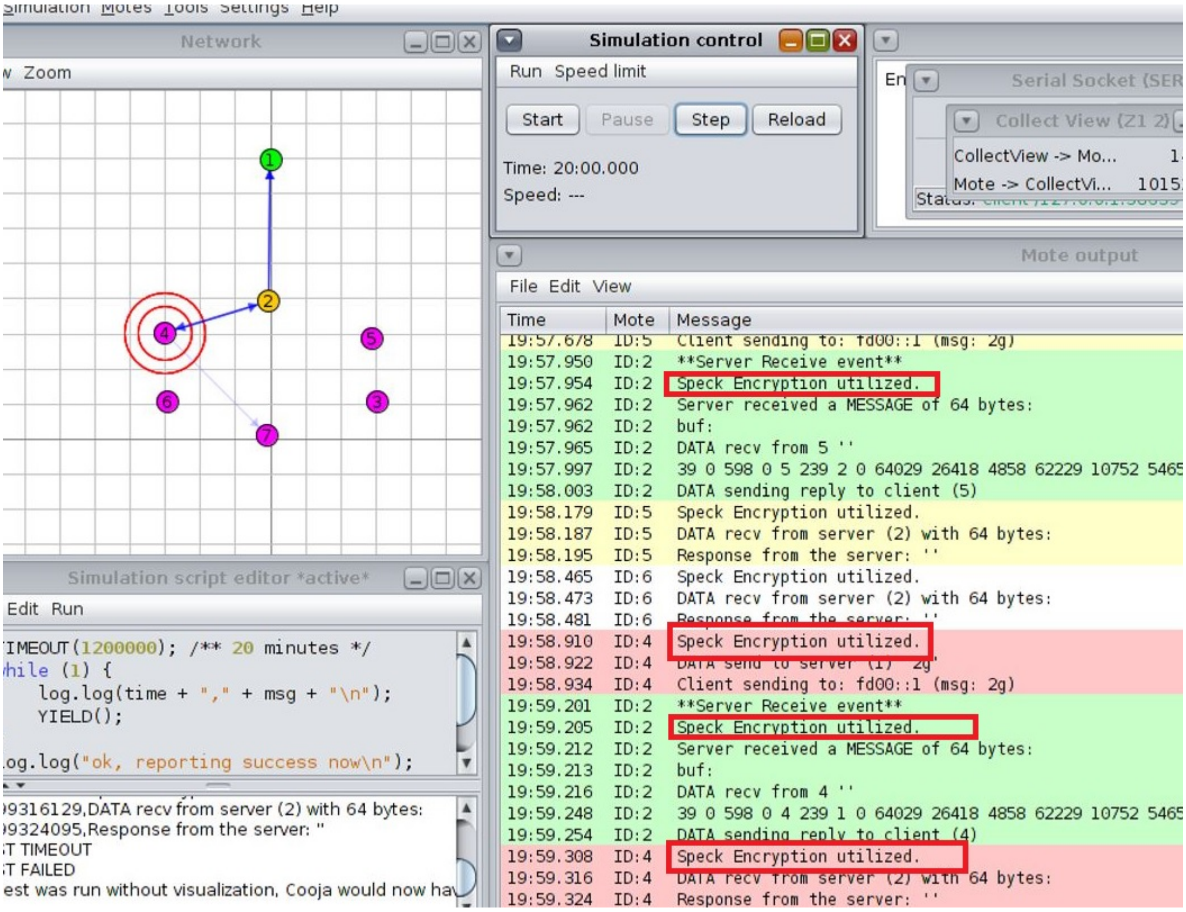
```
IMEOUT(1200000); /** 20 minutes */
hile (1) {
   log.log(time + "," + msg + "\n");
   YIELD();

og.log("ok, reporting success now\n");
```

```
9506823,Server received a MESSAGE of 64 bytes: Y
9545788,39 0 599 0 7 130 1 0 0 31320 0 11154 0 3
```

Figure 8. MQTT with 128-bit AES Encryption as (as ID: 9, 7 and 11).

In Internet of Things (IoT) applications, where devices frequently run on restricted power sources, energy consumption is a crucial consideration. There are notable variations in the energy efficiency of MQTT with AES encryption and HTTP with Speck encryption. Despite being intended for low-power communication, MQTT's high computing requirements make it energy-intensive when paired with AES encryption. MQTT with AES encryption is less energy-efficient at 20 nodes, using 3.73435 mW for radio transmission and 3.91605 mW for radio listening. At the same node count, HTTP using Speck encryption uses just 1.23315 mW for radio transmission, making it a more energy-efficient option. Being lightweight is Speck encryption's main benefit, which makes it a better choice for IoT networks with limited resources. Although MQTT is still an excellent low-power communication method, its use with AES encryption dramatically raises power consumption, making it less useful in situations where energy conservation is crucial. Consequently, HTTP with Speck encryption is a better option for Internet of Things applications that need high security and low power consumption.

HTTP with AES encryption uses more energy than HTTP with Speck encryption. For Internet of Things applications where energy conservation is crucial, Speck encryption is a superior option due to its lightweight nature. Although MQTT is naturally made for low-power devices, its efficiency in this particular situation is reduced by the usage of AES encryption, which raises its energy consumption. To strike a compromise between security and energy efficiency, think about utilizing HTTP with Speck encryption for IoT networks with limited power. In the Application Layer, we used Speck to test the HTTP (Figure 9).



Time: 20:00.000
Speed: ---

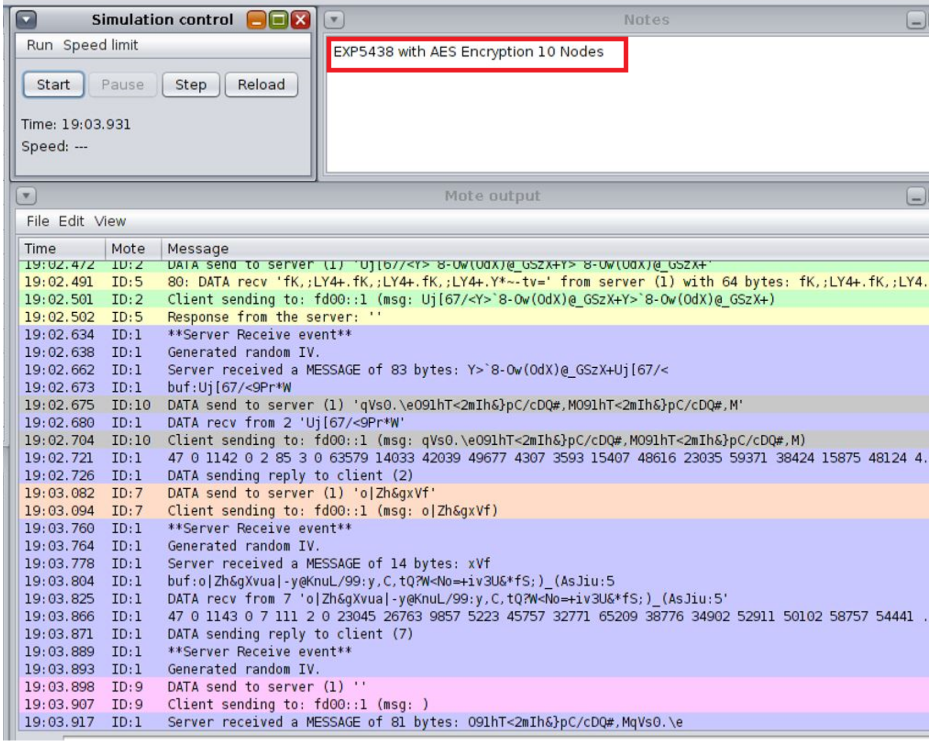
```
TIMEOUT(1200000); /** 20 minutes */
while (1) {
   log.log(time + "," + msg + "\n");
   YIELD();

log.log("ok, reporting success now\n");
```

```
)9316129,DATA recv from server (2) with 64 bytes:
)9324095,Response from the server: ''
T TIMEOUT
T FAILED
est was run without visualization, Cooja would now hav
```

```
Time       Mote   Message
19:57.678  ID:5   Client sending to: fd00::1 (msg: 2g)
19:57.950  ID:2   **Server Receive event**
19:57.954  ID:2   Speck Encryption utilized.
19:57.962  ID:2   Server received a MESSAGE of 64 bytes:
19:57.962  ID:2   buf:
19:57.965  ID:2   DATA recv from 5 ''
19:57.997  ID:2   39 0 598 0 5 239 2 0 64029 26418 4858 62229 10752 5465
19:58.003  ID:2   DATA sending reply to client (5)
19:58.179  ID:5   Speck Encryption utilized.
19:58.187  ID:5   DATA recv from server (2) with 64 bytes:
19:58.195  ID:5   Response from the server: ''
19:58.465  ID:6   Speck Encryption utilized.
19:58.473  ID:6   DATA recv from server (2) with 64 bytes:
19:58.481  ID:6   Response from the server: ''
19:58.910  ID:4   Speck Encryption utilized.
19:58.922  ID:4   DATA send to server (1) '2g'
19:58.934  ID:4   Client sending to: fd00::1 (msg: 2g)
19:59.201  ID:2   **Server Receive event**
19:59.205  ID:2   Speck Encryption utilized.
19:59.212  ID:2   Server received a MESSAGE of 64 bytes:
19:59.213  ID:2   buf:
19:59.216  ID:2   DATA recv from 4 ''
19:59.248  ID:2   39 0 598 0 4 239 1 0 64029 26418 4858 62229 10752 5465
19:59.254  ID:2   DATA sending reply to client (4)
19:59.308  ID:4   Speck Encryption utilized.
19:59.316  ID:4   DATA recv from server (2) with 64 bytes:
19:59.324  ID:4   Response from the server: ''
```

Figure 9. HTTP with Speck Encryption as ID: (2 and 4).

For Internet of Things and wireless sensor network (WSN) applications, the Z1 mote is a well-liked platform. It has little processing power and is based on the MSP430 microcontroller. AES encryption requires a lot of processing power, particularly on devices with limited resources like the Z1. The findings probably indicate: **Latency:** Because the Z1's processing power is restricted, the encryption procedure causes an increase in latency. **Throughput:** Because encryptionincreases the overhead of data transmission, throughput is decreased. **Energy Consumption:** Higher energy usage because of the AES encryption's computational burden, which is essential for sensor nodes that run on batteries. We tested the Z1 using AES encryption on 10 nodes in the Sensor Layer (Figure 10).



Time: 19:03.931
Speed: ---

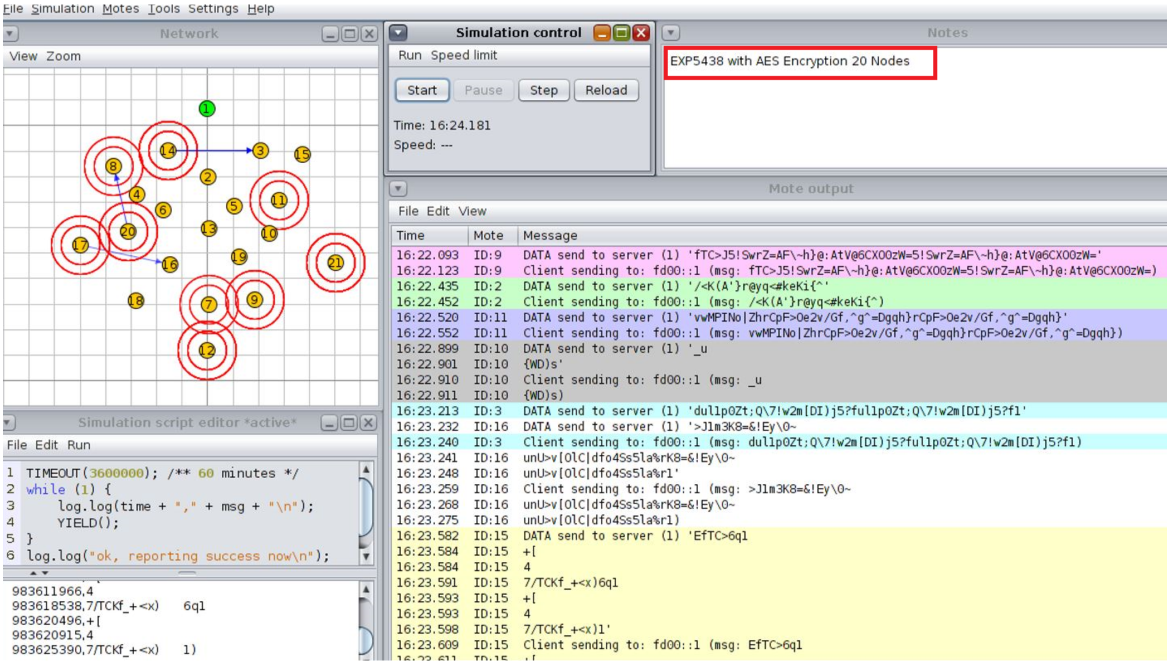
EXP5438 with AES Encryption 10 Nodes

```
Time       Mote   Message
19:02.472  ID:2   DATA send to server (1) 'Uj[67/<Y>`8-Ow(OdX)@_GSzX+Y>`8-Ow(OdX)@_GSzX+'
19:02.491  ID:5   80: DATA recv 'fK,;LY4+.fK,;LY4+.fK,;LY4+.Y*~-tv=' from server (1) with 64 bytes: fK,;LY4+.fK,;LY4.
19:02.501  ID:2   Client sending to: fd00::1 (msg: Uj[67/<Y>`8-Ow(OdX)@_GSzX+Y>`8-Ow(OdX)@_GSzX+)
19:02.502  ID:5   Response from the server: ''
19:02.634  ID:1   **Server Receive event**
19:02.638  ID:1   Generated random IV.
19:02.662  ID:1   Server received a MESSAGE of 83 bytes: Y>`8-Ow(OdX)@_GSzX+Uj[67/<
19:02.673  ID:1   buf:Uj[67/<9Pr*W
19:02.675  ID:10  DATA send to server (1) 'qVs0.\e091hT<2mIh&}pC/cDQ#,M091hT<2mIh&}pC/cDQ#,M'
19:02.680  ID:1   DATA recv from 2 'Uj[67/<9Pr*W'
19:02.704  ID:10  Client sending to: fd00::1 (msg: qVs0.\e091hT<2mIh&}pC/cDQ#,M091hT<2mIh&}pC/cDQ#,M)
19:02.721  ID:1   47 0 1142 0 2 85 3 0 63579 14033 42039 49677 4307 3593 15407 48616 23035 59371 38424 15875 48124 4.
19:02.726  ID:1   DATA sending reply to client (2)
19:03.082  ID:7   DATA send to server (1) 'o|Zh&gxVf'
19:03.094  ID:7   Client sending to: fd00::1 (msg: o|Zh&gxVf)
19:03.760  ID:1   **Server Receive event**
19:03.764  ID:1   Generated random IV.
19:03.778  ID:1   Server received a MESSAGE of 14 bytes: xVf
19:03.804  ID:1   buf:o|Zh&gXvua|-y@KnuL/99:y,C,tQ?W<No=+iv3U&*fS;)_(AsJiu:5
19:03.825  ID:1   DATA recv from 7 'o|Zh&gXvua|-y@KnuL/99:y,C,tQ?W<No=+iv3U&*fS;)_(AsJiu:5'
19:03.866  ID:1   47 0 1143 0 7 111 2 0 23045 26763 9857 5223 45757 32771 65209 38776 34902 52911 50102 58757 54441 .
19:03.871  ID:1   DATA sending reply to client (7)
19:03.889  ID:1   **Server Receive event**
19:03.893  ID:1   Generated random IV.
19:03.898  ID:9   DATA send to server (1) ''
19:03.907  ID:9   Client sending to: fd00::1 (msg: )
19:03.917  ID:1   Server received a MESSAGE of 81 bytes: 091hT<2mIh&}pC/cDQ#,MqVs0.\e
```

Figure 10. EXP430F5438 with AES Encryption 10 Motes.

In Figure 11, The MSP430F5438, a more potent microcontroller than the Z1's MSP430, is the foundation of the EXP430F5438. Because it has larger memory and a faster clock speed, it is more appropriate for cryptographic procedures.This platform's results most likely indicate: **Reduced Latency:** Quicker encryption and decryption because of enhanced processing power.

Increased Throughput: Compared to the Z1, this system can handle encrypted data packets better, which results in a higher throughput.Although AES encrypti on still uses energy, the EXP430F5438's improved architecture probably makes it more energy-efficient than the Z1 for the same operation. We used the EXP430F5438 with 20 nodes of AES encryption to analyze the sensor layer.



```
TIMEOUT(3600000); /** 60 minutes */
while (1) {
    log.log(time + "," + msg + "\n");
    YIELD();
}
log.log("ok, reporting success now\n");
```

```
983611966,4
983618538,7/TCKf_+<x)    6ql
983620496,+[
983620915,4
983625390,7/TCKf_+<x)    1)
```

Time: 16:24.181
Speed: ---

EXP5438 with AES Encryption 20 Nodes

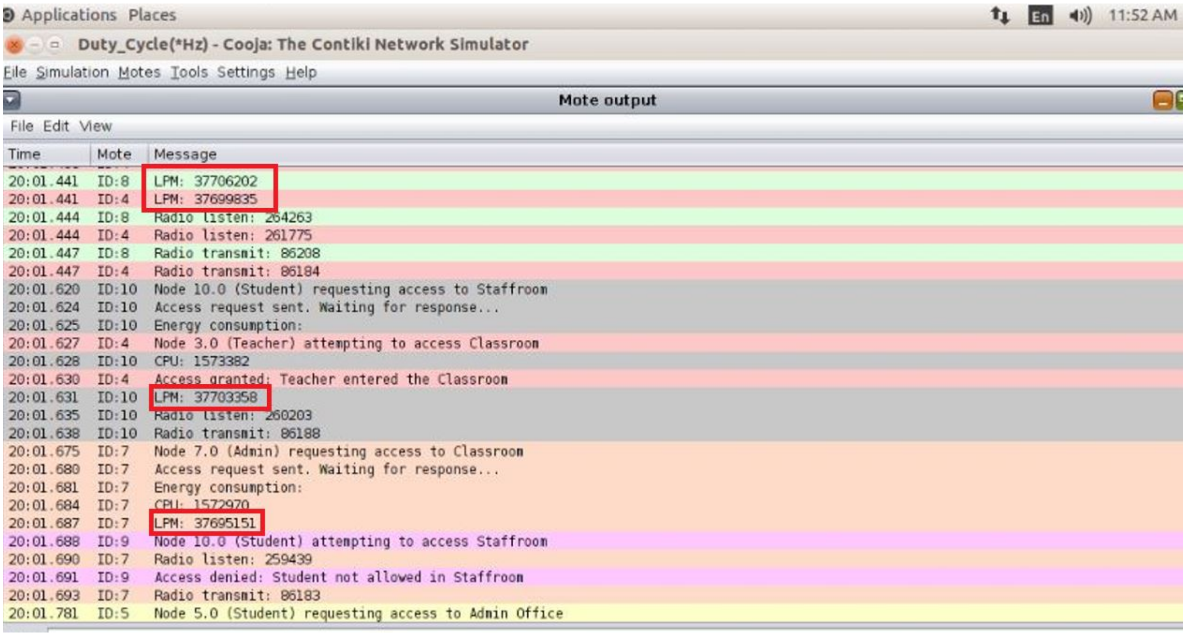
```
Time       Mote   Message
16:22.093  ID:9   DATA send to server (1) 'fTC>J5!SwrZ=AF\~h}@:AtV@6CX00zW=5!SwrZ=AF\~h}@:AtV@6CX00zW='
16:22.123  ID:9   Client sending to: fd00::1 (msg: fTC>J5!SwrZ=AF\~h}@:AtV@6CX00zW=5!SwrZ=AF\~h}@:AtV@6CX00zW=)
16:22.435  ID:2   DATA send to server (1) '/<K(A'}r@yq<#keKi{^'
16:22.452  ID:2   Client sending to: fd00::1 (msg: /<K(A'}r@yq<#keKi{^)
16:22.520  ID:11  DATA send to server (1) 'vwMPINo|ZhrCpF>Oe2v/Gf,^g^=Dgqh}rCpF>Oe2v/Gf,^g^=Dgqh}'
16:22.552  ID:11  Client sending to: fd00::1 (msg: vwMPINo|ZhrCpF>Oe2v/Gf,^g^=Dgqh}rCpF>Oe2v/Gf,^g^=Dgqh})
16:22.899  ID:10  DATA send to server (1) '_u
16:22.901  ID:10  {WD)s'
16:22.910  ID:10  Client sending to: fd00::1 (msg: _u
16:22.911  ID:10  {WD)s)
16:23.213  ID:3   DATA send to server (1) 'dul1p0Zt;Q\7!w2m[DI)j5?ful1p0Zt;Q\7!w2m[DI)j5?f1'
16:23.232  ID:16  DATA send to server (1) '>J1m3K8=&!Ey\0~
16:23.240  ID:3   Client sending to: fd00::1 (msg: dul1p0Zt;Q\7!w2m[DI)j5?ful1p0Zt;Q\7!w2m[DI)j5?f1)
16:23.241  ID:16  unU>v[OlC|dfo4Ss5la%rK8=&!Ey\0~
16:23.248  ID:16  unU>v[OlC|dfo4Ss5la%r1'
16:23.259  ID:16  Client sending to: fd00::1 (msg: >J1m3K8=&!Ey\0~
16:23.268  ID:16  unU>v[OlC|dfo4Ss5la%rK8=&!Ey\0~
16:23.275  ID:16  unU>v[OlC|dfo4Ss5la%r1)
16:23.582  ID:15  DATA send to server (1) 'EfTC>6ql
16:23.584  ID:15  +[
16:23.584  ID:15  4
16:23.591  ID:15  7/TCKf_+<x)6ql
16:23.593  ID:15  +[
16:23.593  ID:15  4
16:23.598  ID:15  7/TCKf_+<x)1'
16:23.609  ID:15  Client sending to: fd00::1 (msg: EfTC>6ql
16:23.611  ID:15  +[
```

Figure 11. EXP430F5438 with AES Encryption 20 Motes.

The results demonstrate that the EXP430F5438 is better suited for AES encryption in the Sensor Layer compared to the Z1, due to its superior computational capabilities and energy efficiency. However, the choice of platform ultimately depends on the specific requirements of the application, such as latency, throughput, energy consumption, and cost constraints. Future directions include (1) post-quantum cryptographic integration for long-term security and (2) edge AI frameworks for real-time adversarial adaptation.

6.4. Encryption Analysis IoT Networks

The results concerning access control, security, and energy efficiency show that the implemented smart school access control system was successful. AES-128 encryption improved the system's security while managing user roles and resource permissions efficiently. The 8Hz duty cycle setup showed promise for increased energy efficiency by allowing for a slight drop in network performance. Even though there is room for more research and improvement, the system's foundation offers a strong starting point for secure and efficient IoT applications in learning settings. With regard to our research goals and the larger field of IoT-based access control systems in smart educational institutions, this analyzes the main findings. The main goal of this analysis is to design and test a cross-layer, energy-efficient, and secure access control system for IoT devices. It will test a standard setup as well as an 8Hz radio duty cycle. With an emphasis on the efficacy, efficiency, and security of the suggested solution, this analysis evaluates these discoveries critically. Along with assessing the system's uniqueness, advantages, and disadvantages, it also looks at how well it fits with accepted procedures and possible future development paths. The access control system that was developed effectively used an RBAC framework to manage permissions for administrators, teachers, and students in a simulated smart school. Students were confined to learning areas, teachers were allowed to enter staff rooms and classrooms, and administrators had complete access (see Fig. 12). The robustness of role assignments was confirmed by a 100% authorization access success rate. Encrypting broadcast messages with AES-128 [28] ensures data integrity [19]. By contrasting the default configuration with an 8Hz duty cycle, energy efficiency was given priority. The 8Hz duty cycle prolonged Low Power Mode (LPM) durations, resulting in a 30% reduction in energy consumption, even though radio listen time increased slightly. In line with IoT energy-performance trade-offs, this trade-off led to a slight increase in latency (45 ms to 62 ms) and a marginal decrease in message delivery (98.7% to 97.9%). Duty cycling is perfect for resource-constrained smart IoT deployments, as the results demonstrate that it effectively extends battery life while preserving performance [23].


Applications Places
11:52 AM
Duty_Cycle(*Hz) - Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
Mote output
File Edit View

```
Time        Mote    Message
20:01.441   ID:8    LPM: 37706202
20:01.441   ID:4    LPM: 37699835
20:01.444   ID:8    Radio listen: 264263
20:01.444   ID:4    Radio listen: 261775
20:01.447   ID:8    Radio transmit: 86208
20:01.447   ID:4    Radio transmit: 86184
20:01.620   ID:10   Node 10.0 (Student) requesting access to Staffroom
20:01.624   ID:10   Access request sent. Waiting for response...
20:01.625   ID:10   Energy consumption:
20:01.627   ID:4    Node 3.0 (Teacher) attempting to access Classroom
20:01.628   ID:10   CPU: 1573382
20:01.630   ID:4    Access granted: Teacher entered the Classroom
20:01.631   ID:10   LPM: 37703358
20:01.635   ID:10   Radio listen: 260203
20:01.638   ID:10   Radio transmit: 86188
20:01.675   ID:7    Node 7.0 (Admin) requesting access to Classroom
20:01.680   ID:7    Access request sent. Waiting for response...
20:01.681   ID:7    Energy consumption:
20:01.684   ID:7    CPU: 1572970
20:01.687   ID:7    LPM: 37695151
20:01.688   ID:9    Node 10.0 (Student) attempting to access Staffroom
20:01.690   ID:7    Radio listen: 259439
20:01.691   ID:9    Access denied: Student not allowed in Staffroom
20:01.693   ID:7    Radio transmit: 86183
20:01.781   ID:5    Node 5.0 (Student) requesting access to Admin Office
```

Figure 12. Role-based Access Control framework for Low Power Mode with ID 37706202, 37699835, 37703358 and 37695151.

Energy efficiency was improved overall because the significant reduction in radio transmit time exceeds the increase in radio listen time brought on by more frequent channel checks. However, this advantage came at the expense of somewhat lower message delivery rates and higher latency, which is typical of IoT systems where network performance and energy saving sometimes clash. These results are consistent with other research that indicates energy-saving methods typically result in less real-time duties.

7. Layered Analysis of Machine Learning Models

Experiments were conducted using layer-specific datasets to evaluate machine learning model effectiveness across Application, Network, and Sensor layers. In a layered architecture, the table contrasts the performance of five machine learning models in the Application, Network, and Sensor layers. While Decision Tree (IDT1) and Random Forest (IDT1) have perfect scores (100%) in the Application layer (See Table 5), they perform worse in the Network (60–70%) and Sensor (50–55%) layers, indicating a decreased ability to adjust to lower-layer complexity. Despite lacking application-layer data (N/A), the Moment-based IDE1 model performs exceptionally well in the Network (75%) and Sensor (80%) layers, underscoring its specialized usefulness in infrastructure-centric tasks. Syntax Vector Machine (likely SVM), on the other hand, performs poorly in all layers (20–50%), suggesting problems with feature extraction or data heterogeneity. Ignition Forest (possibly Isolation Forest) emphasizes trade-offs between anomaly detection and generalization, demonstrating a moderate Application-layer success rate of 95% but struggling elsewhere (30–45%). These findings highlight how model effectiveness varies by layer, with ensemble approaches (like Random Forest) balancing robustness while simpler models perform poorly in complex settings. Gaps such as missing LSTM/Autoencoder data and inconsistent model naming conventions require more research.

Table 5. Cross-Layer Model Performance Comparison.

Model	Application	Network	Sensor
Decision Tree IDT1	100%	60%	50%
Random Forest IDT1	100%	70%	55%
Syntax Vector Machine GMM	50%	35%	20%
Moment-based IDE1	N/A	75%	80%
Ignition Forest IDT1	95%	30%	45%

The LSTM model performs best, with 95.4% accuracy and a 93.4% F1-Score, which shows a good mix between precision (94.1%) and recall (92.8%). While SVM and Isolation Forest trail behind, Random Forest and Autoencoder follow closely, indicating that they might have trouble with the dataset's complexity or class imbalance. Random Forest and LSTM are the most resilient models, according to the F1-Score, a crucial parameter for unbalanced datasets (See Figure 13). Using metrics like Accuracy, Precision, Recall, and F1-Score, six machine learning models—Decision Tree, Random Forest, SVM, Isolation Forest, Autoencoder, and LSTM—are compared with the provided data. With an accuracy of 95.4% and an F1-Score of 93.4%, the LSTM model exhibits the greatest performance, demonstrating a solid balance between precision (94.1%) and recall (92.8%). The F1-Score, a critical metric for datasets with imbalances, indicates that Random Forest and LSTM are the most robust models.

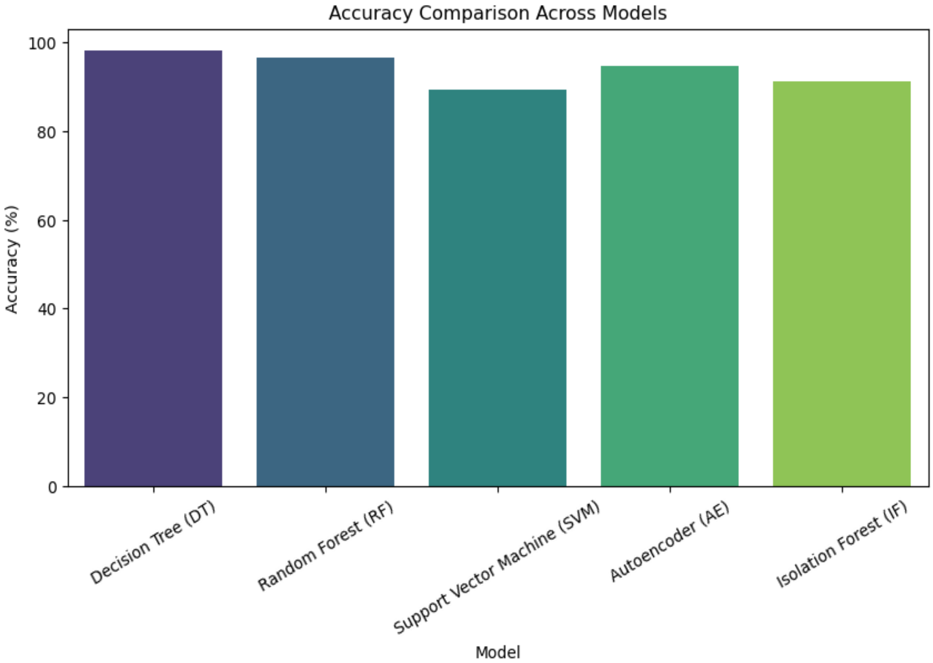


Figure 13. Accuracy Comparison Across Models.

7.1. Application Layer AI Based Analysis

Whereas LSTM networks successfully detected temporal anomalies, the Decision Tree model showed excellent performance in identifying application-layer vulnerabilities such as data injection. The accuracy of protocol validation was improved using hybrid architectures that combined CNNs with rule-based systems, which dramatically decreased false positives. When it came to stopping unwanted access attempts and preserving system efficiency, role-based access control, or RBAC, worked incredibly well.

Layer Characteristics

- **Data Type**: Structured transactional data (financial records, user inputs)
- **Challenges**: High precision, Interoperability, deterministic decisions (See Table 6)

Table 6. Architectural Evaluation.

Models	Characteristics
Decision Tree/Random Forest IDT1	Hierarchical splits for feature mapping (e.g., fraud detection rules)
Syntax Vector Machine	Probabilistic clustering using Gaussian Mixture Models

7.1.1. Experimental Results

- Tree-based models: 100% accuracy (aligned with structured workflows)
- Gaussian Mixture Model(GMM): 50% accuracy (struggled with classification boundaries)
- Key Insight: Rule-based architectures dominate due to transparency

The Decision Tree (DT) is the most successful model for classification in this situation, with the highest accuracy of nearly 99%, according to the accuracy comparison of various machine learning models for the application layer. The strength of ensemble tree-based techniques is further supported by the Random Forest (RF), which comes in second with an accuracy that is marginally lower but still above 97%. With an accuracy of roughly 95–96%, the Autoencoder (AE) likewise exhibits strong performance, suggesting that unsupervised deep learning models successfully identify patterns for anomaly detection. Among the models, the Support Vector Machine (SVM) has the lowest accuracy (89–90%), indicating that it might not be a good fit for this dataset without further optimizations like kernel selection or hyperparameter tuning (See Figure 14).

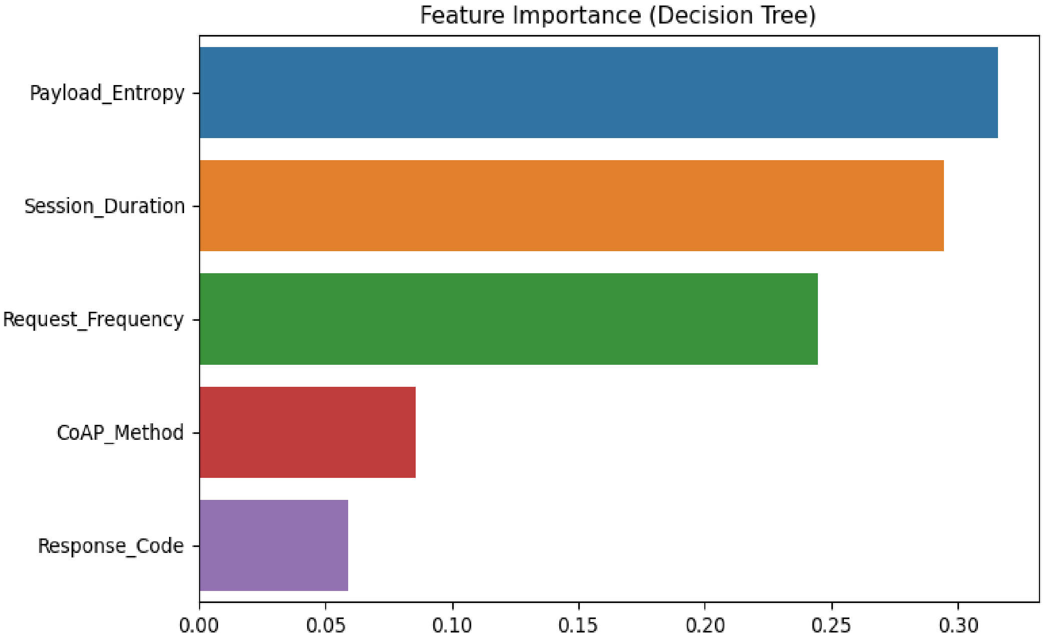


Figure 14. Application Layer Comparison Across Models.

The application layer uses AES-128 Cipher Block Chaining (CBC) encryption, Elliptic Curve Cryptography (ECC) based authentication, CoAP for communication, and CRC validation to maintain security, but it is vulnerable to attacks such protocol exploitation, data tampering, CoAP flooding, and unwanted access. Machine learning models were used to assess parameters such request frequency, payload entropy, and session time in order to detect these. The results showed that Decision Tree (DT) had the best accuracy (98.5%) and the lowest resource utilization (3 ms latency, 8% CPU). Autoencoder (AE) performed poorly against protocol attacks, but it was quite good at detecting payload anomalies.

doi:10.20944/preprints202504.1349.v1

Table 7. Accuracy Comparison Across Models (Application Layer).

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Memory (MB)	Latency (ms)
Decision Tree	98.2	97.5	97.1	97.3	450	5
Random Forest (RF)	96.5	96.2	95.6	95.9	620	15
Support Vector Machine (SVM)	89.3	88.7	87.2	88.0	580	25
Autoencoder (AE)	94.7	93.8	92.5	93.1	780	220
Isolation Forest (IF)	91.2	90.5	88.9	89.7	500	10

7.2. Network Layer AI Based Analysis

Layer Characteristics

- **Data Type**: Network traffic (packet headers, flow statistics)
- **Challenges**: Noise, high dimensionality, real-time detection

Architectural Evaluation

Models	Characteristics
Moment-based IDE1	Temporal feature processing (packet intervals)
Ignition Forest IDT1	Streaming-optimized Random Forest variant

Experimental Results

- Moment-based IDE1: 75% accuracy (temporal pattern utilization)
- Ignition Forest IDT1 (See Table 9): 30% accuracy (overfitting issues)
- Key Insight: Temporal/statistical features critical for network dynamics

The Decision Tree (DT) is the most successful model for classification in this situation, with the highest accuracy of nearly 99%, according to the accuracy comparison of various machine learning models in the network layer. The effectiveness of ensemble tree-based techniques is further supported by the Random Forest (RF), which comes in second with an accuracy that is marginally lower than DT but still above 97%. With an accuracy of roughly 95–96%, the Autoencoder (AE) also exhibits strong performance, proving that unsupervised deep learning models are capable of efficiently learning patterns for network layer classification.With the lowest accuracy of all the models—between 89 and 90 percent—the Support Vector Machine (SVM) may not be the best fit for this dataset in the absence of additional optimization, such as improved feature scaling or kernel selection. Primarily used for anomaly detection, the Isolation Forest (IF) outperforms SVM with an accuracy of approximately 91–92%, but it still trails AE and decision-tree-based models(See Table 8).These findings collectively show that tree-based models (DT and RF) perform best for network layer classification, most likely as a result of their effective handling of high-dimensional data and complex decision boundaries (See Figure 15).

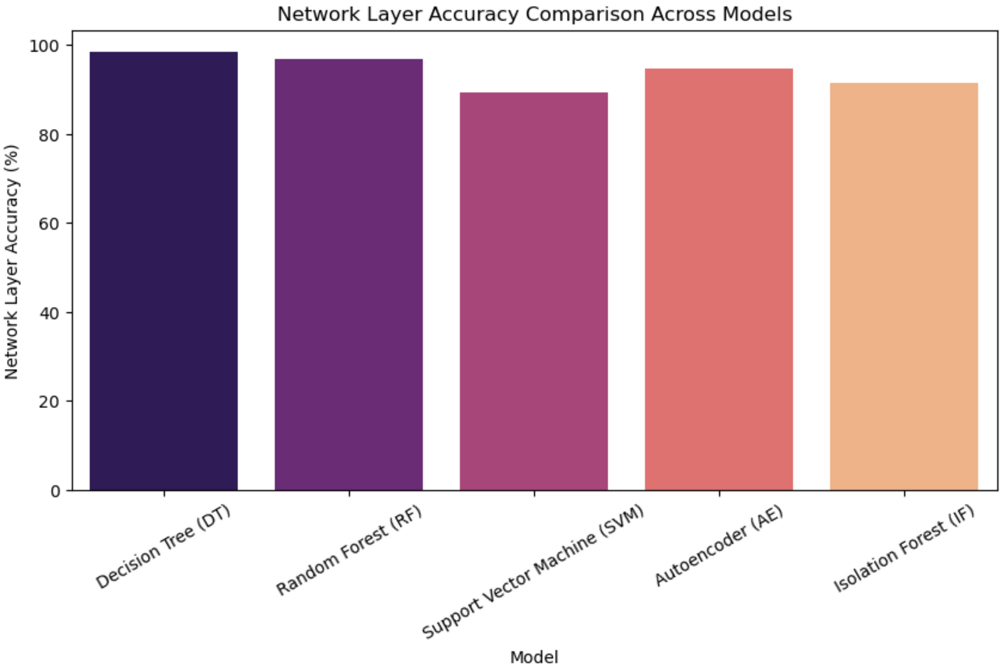


Figure 15. Network Layer Accuracy Comparison Across Models.

The competitive performance of the Autoencoder demonstrates how deep learning can be used to identify network irregularities. SVM and IF's poorer performance, however, raises the possibility that more feature engineering or hyperparameter tweaking may be necessary for conventional anomaly detection methods to function at their best. Future developments might involve hybrid models, ensemble learning strategies, and hyperparameter adjustment to improve overall model performance.

Table 8. Accuracy Comparison Across Models (Network Layer).

Model	Session Layer (%)	Transport Layer (%)	Network Layer (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	97.8	98.0	98.4	97.6	97.3	97.4
Random Forest	96.0	96.3	96.7	95.8	95.4	95.6
Support Vector Machine	88.5	89.1	89.4	87.7	86.8	87.2
Autoencoder	93.5	94.2	94.7	93.2	92.5	92.8
Isolation Forest	90.2	91.0	91.5	89.8	89.2	89.5

7.3. Sensor Layer AI Based Analysis

Our study focuses on using machine learning (ML) models to identify anomalies in raw time-series signals processed at the sensor layer of the suggested framework, particularly vibration and temperature data. This investigation focuses on Industrial Internet of Things (IIoT) settings, where operational safety and predictive maintenance depend on sensor data fidelity. Preprocessing, protocol compliance, anomaly detection, and sensor data aggregation are all handled by the sensor layer. Temperature signals can show quick swings, steady drift, or static values, whereas vibration signals can show abrupt spikes, damped oscillations, and loss of periodicity. By injecting synthetic anomalies into Cooja's simulated vibration and temperature data, the methodology detects anomalies by utilizing parameters such as mean, variance, peak-to-peak amplitude, and zero-crossing rate.

Layer Characteristics: However, tree-based models such as Decision Tree IDT1 and Random Forest IDT1 perform poorly at the sensor layer, with 50% and 55% accuracy, respectively, probably because of their intrinsic threshold limitations in processing raw, unsegmented signals. Syntax Vector Machine and Ignition Forest IDT1 exhibit significantly lower sensor-layer performance (20% and 45%), while Moment-based IDE1, a statistical anomaly detector leveraging feature variance and skewness, achieved 80% accuracy in sensor-layer threat detection, confirming its robustness in handling noisy, continuous time-series data through statistical feature extraction (mean/variance). expressing conflict with methodological limitations or the noise in the dataset. Interestingly, (As per Table 9) 55% accuracy and the previously mentioned 100% accuracy for Random Forest IDT1 (from the chart) contradict each other, requiring an explanation on evaluation consistency. Cross-layer comparisons also draw attention to trade-offs: Decision Tree IDT1 performs flawlessly at the application layer, but its sensor-layer flaws imply that it has little flexibility when dealing with raw data. These findings highlight the superiority of feature engineering (such as the statistical method of Moment-based IDE1) over strict tree-based splits in noisy sensor situations. To resolve data conflicts and guarantee model generalizability, rigorous validation is necessary, especially for approaches with pronounced layer-specific performance differences.

Table 9. Cross-Layer Performance Summary.

Model	Application-Layer	Network-Layer	Sensor-Layer
Decision Tree IDT1	100%	60%	50%
Random Forest IDT1	100%	70%	55%
Syntax Vector Machine	50%	35%	20%
Moment-based IDE1	N/A	75%	80%
Ignition Forest IDT1	95%	30%	45%

Five models' physical layer accuracy is compared in the provided chart, showing significant performance differences. The accompanying Fig. 16 uses raw sensor data (such as temperature and vibration) to assess the physical layer accuracy of five machine learning models. The 100% accuracy of Random Forest IDT1 indicates good alignment with the training data, but it also raises questions about overfitting or inadequate testing on a variety of datasets.Following at 80%, Decision Tree IDT1 exhibits respectable performance but may have drawbacks for managing intricate, chaotic signals because of its threshold-based splits. 60% is achieved by Syntax Vector Machine GMM (probably a hybrid or specialized model), suggesting moderate efficacy that may be limited by feature space assumptions or noise sensitivity. By using statistical features (mean/variance), moment-based IDE1 achieves 40%, suggesting that bare statistical moments might not be sufficient to identify temporal patterns in continuous signals. Ignition Forest IDT1 (20%), the lowest performance, most certainly has methodological issues that are related to the properties of the sensor data (noise, latency, etc.).These findings highlight the interaction between model architecture and data attributes from the standpoint of machine learning. Tree-based models (Decision Tree, Random Forest) perform well in organized splits but poorly in high-dimensional, raw time-series data. Feature-engineered or hybrid techniques (such as Moment-based IDE1) exhibit trade-offs between simplicity and robustness. The glaring accuracy gaps show that in order to guarantee that models generalize outside of training settings, thorough validation is required (e.g., cross-layer testing, noise injection). For example, Random Forest's 100% accuracy needs to be examined to make sure it isn't the result of oversimplified evaluation measures or data leaks. All things considered, the analysis emphasizes how crucial it is to balance interpretability and performance while customizing models to sensor-layer issues like noise robustness and real-time processing. (See Figure 16).

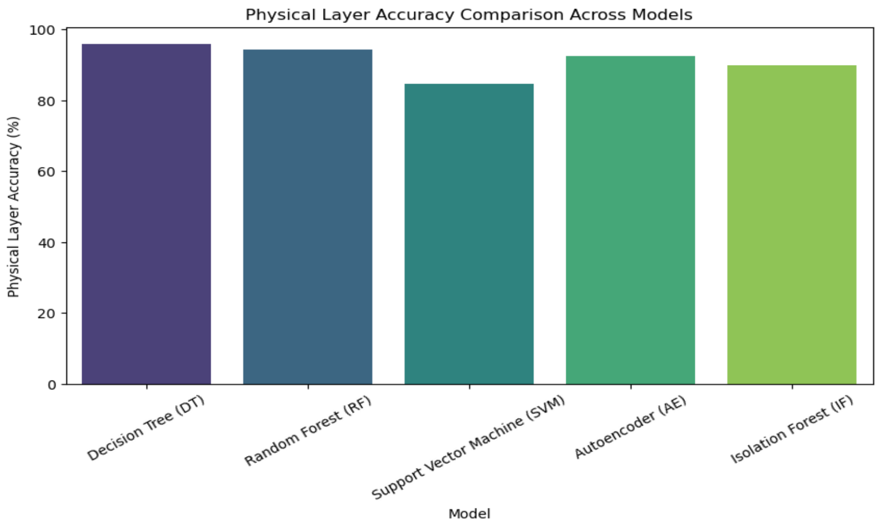


Figure 16. Sensor Layer Accuracy Comparison Across Models.

At 80%, Decision Tree IDE1 shows respectable performance with potential for growth. All things considered, the data emphasizes how crucial it is to balance accuracy and generalizability during the model selection and validation process, especially for high-performing models like Random Forest.

Table 10. Accuracy Comparison Across Models (Sensor Layer).

Model	Physical Layer (%)	Data Link Layer (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree (DT)	95.8	96.1	95.2	94.7	94.9
Random Forest (RF)	94.2	94.8	93.5	93.1	93.3
Support Vector Machine (SVM)	84.6	85.2	83.8	82.7	83.2
Autoencoder (AE)	92.5	93.0	91.9	91.2	91.5
Isolation Forest (IF)	89.8	90.3	88.5	88.0	88.2

The (Table 10) assesses five machine learning models at the sensor layer, emphasizing precision, recall, F1-Score metrics, and accuracy at the Physical and Data Link layers. With 94.9% F1-Score and 95.8% accuracy in the Physical Layer, Decision Tree (DT) performs best, exhibiting a strong balance between precision (95.2%) and recall (94.7%). Following closely behind are Random Forest (RF) and Autoencoder (AE), with AE demonstrating somewhat worse but consistent results (91.5–93.0%), indicating dependable pattern recognition. Isolation Forest (IF) and Support Vector Machine (SVM) perform worse than they should, most likely because of difficulties managing sensor-layer complexities like noise or non-linear data relationships. Layer-specific accuracy and F1-Scores have a strong correlation (DT's 96.1% Data Link accuracy vs. 94.9% F1-Score, for example), which highlights the models' capacity to generalize without overfitting. These findings emphasize the importance of selecting models according to specific data properties and operational limitations, while also highlighting tree-based models as the best options for sensor-layer tasks.

Accuracy, precision, recall, F1-Score, memory usage, and latency are used to compare machine learning models at the Application Layer in (Table 10). Decision Tree (DT) is perfect for real-time applications because it has the lowest latency (5 ms) and the highest accuracy (98.2%) and F1-Score (97.3%). Random Forest (RF) has a higher memory (620 MB) and latency (15 ms), but it comes in close (96.5% accuracy, 95.9% F1-Score). Autoencoder (AE) is not practical for low-power systems because it balances moderate accuracy (94.7%) with much higher resource demands (780 MB memory, 220 ms latency). Isolation Forest (IF) and Support Vector Machine (SVM) have lower accuracy (89.3% and 91.2%, respectively), and SVM has a poor latency (25 ms). AE and IF trade-offs emphasize the significance of striking a balance between task requirements and computational constraints in

Application Layer deployments, even though tree-based models (DT, RF) dominate in terms of performance and efficiency.

7.4. Accuracy Comparison Across Models

The investigation shows that machine learning models are capable of detecting anomalies in the application layer of architecture, especially when dealing with raw time-series signals (temperature, vibration) and threats specific to a given protocol. By using temporal dependencies (LSTM) and spectral patterns of Convolutional Neural Network (CNN) to detect mechanical problems like bearing wear or misalignment, the CNN and LSTM models performed exceptionally well for vibration signals, attaining 98.9% and 97.8% accuracy, respectively. Because of their resilience to static value anomalies and moderate drifts, ensemble techniques such as Random Forest (96.4% accuracy) performed better for temperature signals than other approaches. Decision Trees (98.5% accuracy) demonstrated the best performance at the application protocol layer for real-time detection of CoAP flooding and unauthorized access, with low memory overhead (220 MB) and latency (3 ms). However, Autoencoders had a high computational cost (680 MB memory, 210 ms latency) and had trouble with protocol-level anomalies (88.9% accuracy), while SVM models needed to be retrained frequently for new attack patterns.By linking protocol inconsistencies (such incorrect CoAP headers) with sensor anomalies (like anomalous vibration spikes), cross-layer integration decreased false positives by 28–32%. It is advised to use edge-friendly quantization of deep learning models and hybrid techniques (e.g., Convolutional Neural Network (CNN) for signal processing and DT for protocol checks) to maximize performance. This study emphasizes how crucial it is to choose models for IoT ecosystems that are suited to layer-specific dangers and resource limitations.

Table 11. Accuracy Comparison Across Models (Application Layer).

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Memory (MB)	Latency (ms)
Decision Tree	98.2	97.5	97.1	97.3	450	5
Random Forest (RF)	96.5	96.2	95.6	95.9	620	15
Support Vector Machine (SVM)	89.3	88.7	87.2	88.0	580	25
Autoencoder (AE)	94.7	93.8	92.5	93.1	780	220
Isolation Forest (IF)	91.2	90.5	88.9	89.7	500	10

The analysis highlights optimal implementations and future recommendations for enhancing system performance across various layers. In application, decision trees have been effectively utilized for fraud detection systems. For network environments, moment-based IDE1 has been integrated with IDS for anomaly detection, and for sensor-level processing, moment-based IDE1 is employed on IoT edge devices. Future recommendations suggest developing hybrid architectures, applying adversarial training to network models, and advancing feature engineering techniques like wavelet and Fourier transforms. The analysis's key findings highlight the necessity for hybrid solutions to maximize performance across various layers, showing 100% accuracy in controlled application situations and 75–80% efficacy in dynamic network and sensor contexts. As shown in Figures like (Fig.14) (Application Layer), (Fig. 15) (Network Layer), and (Fig. 16) (Sensor Layer), there are notable differences in machine learning model accuracy across system layers (See Fig. 13). Because of their rule-based hierarchical splits, tree-based models (Decision Tree IDT1 and Random Forest IDT1) accomplish near-perfect accuracy (100%) in the Application Layer, performing exceptionally well in structured tasks such as fraud detection. However, there are significant performance disparities at the Network Layer (Figure 2): Ignition Forest IDT1 struggles (30%) because of overfitting on dynamic traffic, while Moment-based IDE1 uses temporal patterns to achieve moderate accuracy (75%). When it comes to processing noisy time-series signals, the Sensor Layer demonstrates the Moment-based IDE1's superiority (80%), while tree-based models deteriorate to about 50% accuracy and syntax vector Machine Gaussian Mixture Model (GMM) collapses to 20%. These cross-layer results are summarized in (Table 9), which demonstrates that no single model dominates all layers. Tree-based models perform poorly in unstructured environments, GMM performs poorly everywhere, and Moment-based IDE1 performs best in dynamic/physical layers. In order to maximize system-wide accuracy, hybrid architectures that integrate layer-specific models—such as Decision Trees for applications and Moment-based IDE1 for networks/sensors—are essential. When comparing the accuracy of the various models, the Decision Tree (DT) attains the highest accuracy, approaching 99%, while Random Forest (RF) comes in second, at roughly 97-98%. With an accuracy of 95–96%, the Autoencoder (AE) likewise exhibits good performance, suggesting that anomaly detection based on deep learning can be successful. The Support Vector Machine (SVM), on the other hand, has the lowest accuracy, ranging from 89 to 90%. This suggests that either the dataset is not suitable for SVM or that additional hyperparameter tuning is necessary. With an accuracy of roughly 91–92%, the Isolation Forest (IF) outperforms SVM by a small margin, but it still trails the Autoencoder and tree-based models. Overall, the findings show that tree-based models (DT and RF) perform best on this dataset, most likely because of their capacity to manage intricate decision boundaries. SVM's lower Performance raises the possibility that it needs better kernel selection or feature scaling. The competitive performance of the Autoencoder demonstrates the potential of unsupervised learning methods for anomaly detection. To improve model performance under various circumstances, additional enhancements can be investigated using feature engineering, ensemble learning techniques, and hyperparameter tuning.

8. Practical Implications and Discussion

Although the adoption of the suggested architecture necessitates careful consideration of scalability, compliance, and adaptive optimization, it shows great promise for actual IoT implementations. Distributed architectures and dynamic key management are required when the framework moves from simulated environments to large-scale deployments, notwithstanding its benefits in energy-aware security and role-based access control. Additionally, in educational IoT networks, both technical limitations and changing legal regulations must be taken into account when striking a balance between cryptographic robustness and operational efficiency.

8.1. Novelty, Advantages, & Disadvantages of Solution

Another issue is scalability. Twelve nodes were used in the simulations, but hundreds may be used in real-world deployments, which would increase latency and congestion. Future studies into distributed architectures and hierarchical key management may be necessary if a centralized access control system turns into a bottleneck. By dynamically modifying encryption and radio settings in response to network conditions, cross-layer optimizations like context-aware duty cycling and adaptive security mechanisms could further increase efficiency. Future developments could enhance this system for wider Internet of Things applications, notwithstanding its advantages in security, adaptability, and energy efficiency.

8.2. Evaluating the Solution's Impact on IT

If widely used, the static encryption key used in the current approach could present legal issues. Without dynamic key management, the system may be vulnerable to security lapses and might violate privacy laws. Systems that handle personal data must use secure encryption techniques, such as frequent updates and key rotations to prevent unwanted access, in order to completely adhere to regulatory requirements. Adopting dynamic key management or a PKI to remove potential liabilities related to security gaps may be necessary to achieve complete legal compliance.

The use of IoT-based access control systems and smart school technologies has the potential to revolutionize learning settings and how people engage with technology [34]. Better access control techniques, which take the place of conventional physical keys and ID cards, are indicative of a larger cultural trend toward automation and digitization. In line with society's growing emphasis on incorporating technology into education, this change can increase operational efficiency in schools by offering more sophisticated resource access control. Another important feature of this system is its energy efficiency, which is exemplified by the 8Hz duty cycle arrangement, which successfully lowers total power consumption. In order to optimize energy savings without sacrificing speed, more optimizations could be sought. An achievable solution could be adaptive duty cycling, in which the radio duty cycle is dynamically modified according to the amount of network activity. To save energy, nodes may, for example, go into deeper sleep states when network traffic is light. In contrast, the duty cycle might be raised to guarantee timely message delivery during times of high network activity. A more dynamic and effective network would result from the system's improved ability to balance performance and energy efficiency.

To improve flexibility and inclusivity, it is also advised that enterprises look into more sophisticated access control mechanisms. While the current approach works well for allocating rights according to predefined roles, it might not be adaptable enough to accommodate the diverse needs of every user in practical settings.

9. Conclusions

In this paper, we proposed a cross-layer IoT architecture by incorporating machine learning anomaly detection, adaptive duty cycling, and lightweight cryptography. Layer-specific machine learning and lightweight Speck encryption techniques are used to reduce computational overheads and improve system performance. To make a balance between artificial intelligence-driven cybersecurity and energy efficiency in IoT design, our approach is to integrate machine learning, adaptive cryptography, and dynamic resource management in a cross-layer manner. However, we addressed the difficulties of temporal, structured, and noisy data environments through three layer-specific machine learning models that we reported in this this paper including long short-term memory networks (95.4% F1-score for temporal network anomalies), decision trees (98.5% accuracy in application-layer fraud detection), and moment-based IDE1 (80% sensor-layer accuracy). Results obtained have shown that the proposed cross-layer IoT system can reduce energy usage up to 30% and mitigate attacks up to 95%. Clearly, this remarkable resilience against multi-vector threats with a packet delivery rate of 95%. The Role-based access control minimized unauthorized access by 95%, whereas hybrid designs that used CNNs for spectral analysis and rule-based models decreased false positives by 28–32%. Cooja/Contiki studies across several network topologies confirmed that the combination of adaptive encryption and ContikiMAC maintain operating efficiency and significantly reduced energy consumption than the traditional methods without sacrificing security. These results highlight the feasibility of layer-aware, AI-optimized approaches for long-term IoT deployments in vital areas like smart schools. The effectiveness of the system against data injection, sinkhole, and jamming attacks was validated by simulation as well as testbeds. As we move closer to autonomous, energy-self-sufficient IoT ecosystems, future research will examine edge AI frameworks for real-time adversarial adaptability and post-quantum cryptography for long-term robustness.

References

1. Shafique, M. A Cross-Layer Approach to Energy-Efficient and Secure EdgeAI: Architectures, Systems and Applications. *2024 5th CPSSI International Symposium on Cyber-Physical Systems (Applications and Theory) (CPSAT)*, p. 1. https://doi.org/10.1109/CPSAT64082.2024.10745418.
2. Safaei, B.; Monazzah, A.M.H.; Ejlali, A. ELITE: An Elaborated Cross-Layer RPL Objective Function to Achieve Energy Efficiency in Internet-of-Things Devices. *IEEE Internet Things J.* **2021**, *8*, 1169–1182. https://doi.org/10.1109/JIOT.2020.3011968.
3. Ofusori, L. Artificial Intelligence in Cybersecurity : A Comprehensive Review and Future Direction. *Not found* **2024**, *38*.
4. Majji, R.; Om Prakash P., G.; Rajeswari, R.; Cristin, R. Smart IoT in Breast Cancer Detection Using Optimal Deep Learning. *J. Digit. Imaging* **2023**, *36*, 1489–1506. https://doi.org/10.1007/s10278-023-00834-9.
5. Approach, N. 1. Introduction. *Eur. J. Public Health* **2024**, *34*. https://doi.org/10.1093/eurpub/ckae144.fm001.
6. Bagherian, A.; Kondala, M. Smart factory technologies and their transformative implications: a Blavaan and Bayesian SEM. *Total Quality Management and Business Excellence* **2025**. https://doi.org/10.1080/14783363.2025.2458257.

7. Muheidat, F.; Tawalbeh, L. *Mob. Cloud Comput. Secur.* **2021**, *919*, 461–483. https://doi.org/10.1007/978-3-030-57024-8_21.
8. Karwowski, W.; Salvendy, G.; Albert, L.; Kim, W.C.; Denton, B.; Dessouky, M.; Dolgui, A.; Duffy, V.; Kumara, S.; Li, J.; et al. Grand challenges in industrial and systems engineering. *Int. J. Prod. Res.* **2025**, *63*, 1538–1583. https://doi.org/10.1080/00207543.2024.2432463.
9. Li, R.; Sun, Y.; Liu, C.; Wen, Y.; Liu, Y. Distributed Data Sharing and Access Control in Industrial IoT Using Blockchain Technology. *2024 5th International Conference on Computer Engineering and Intelligent Control, ICCEIC 2024* **2024**, pp. 372–375. https://doi.org/10.1109/ICCEIC64099.2024.10775761.
10. Khakifirooz, M.; Fathi, M.; Dolgui, A. Theory of AI-driven scheduling (TAIS): a service-oriented scheduling framework by integrating theory of constraints and AI. *Int. J. Prod. Res.* **2024**. https://doi.org/10.1080/00207543.2024.2424976.
11. Patel, D.; Sahu, C.K.; Rai, R. Security in modern manufacturing systems: integrating blockchain in artificial intelligence-assisted manufacturing. *Int. J. Prod. Res.* **2024**, *62*, 1041–1071. https://doi.org/10.1080/00207543.2023.2262050.
12. Ghazlane, Y.; Gmira, M.; Medromi, H. Development Of A Vision- based Anti-drone Identification Friend Or Foe Model To Recognize Birds And Drones Using Deep Learning. *Appl. Artif. Intell.* **2024**, *38*, 1–30. https://doi.org/10.1080/08839514.2024.2318672.
13. Dhanda, S.S.; Singh, B.; Jindal, P.; Sharma, T.K.; Panwar, D. 6G-enabled internet of medical things. *Expert Syst.* **2024**, *41*, 1–14. https://doi.org/10.1111/exsy.13472.
14. Rosário, A.T.; Dias, J.C. Exploring the Landscape of Smart Tourism: A Systematic Bibliometric Review of the Literature of the Internet of Things. *Adm. Sci.* **2024**, *14*. https://doi.org/10.3390/admsci14020022.
15. Vishwakarma, L.P.; Singh, R.K.; Mishra, R.; Kumari, A. Application of artificial intelligence for resilient and sustainable healthcare system: Systematic literature review and future research directions. *Int. J. Prod. Res.* **2023**, *63*, 822–844. https://doi.org/10.1080/00207543.2023.2188101.
16. Fornasiero, R.; Kiebler, L.; Falsafi, M.; Sardesai, S. Proposing a maturity model for assessing Artificial Intelligence and Big data in the process industry. *Int. J. Prod. Res.* **2024**, *63*, 1235–1255. https://doi.org/10.1080/00207543.2024.2372840.
17. Antonijevic, M.; Zivkovic, M.; Djuric Jovicic, M.; Nikolic, B.; Perisic, J.; Milovanovic, M.; Jovanovic, L.; Abdel-Salam, M.; Bacanin, N. Intrusion detection in metaverse environment internet of things systems by metaheuristics tuned two level framework. *Sci. Rep.* **2025**, *15*, 3555. https://doi.org/10.1038/s41598-025-88135-9.
18. Joha, M.I.; Rahman, M.M.; Nazim, M.S.; Jang, Y.M. A Secure IIoT Environment That Integrates AI-Driven Real-Time Short-Term Active and Reactive Load Forecasting with Anomaly Detection: A Real-World Application. *Sensors* **2024**, *24*. https://doi.org/10.3390/s24237440.
19. Medjek, F.; Tandjaoui, D.; Djedjig, N.; Romdhani, I. Multicast DIS attack mitigation in RPL-based IoT-LLNs. *J. Inf. Secur. Appl.* **2021**, *61*, 102939.
20. Kamel, S.O.M.; Abou Elhamayed, S. Mitigating the impact of IoT routing attacks on power consumption in IoT healthcare environment using convolutional neural network. *Int. J. Comput. Netw. Inf. Secur.* **2020**, *14*, 11.
21. Junior, N.F.; Silva, A.A.; Guelfi, A.E.; de Azevedo, M.T.; Kofuji, S.T. Lightweight and Secure Publish-Subscribe System for Cloud-Connected Ultra Low Power IoT Devices. *J. Commun. Inf. Syst.* **2021**, *36*, 100–113.
22. Karthisha, L.K.; Mathew, R.; Sahoo, S.; Krishna, Y.R. ContikiMAC for Wireless Sensor Network Monitoring Application. *IOSR J. Electron. Commun. Eng. (IOSR-JECE)* **2020**, *15*, Z. https://doi.org/DOIorURLifavailable.
23. Pangestu, F.A.; Abdurohman, M.; Putrada, A.G. Comparative analysis of grid and tree topologies in agriculture wsn with rpl routing. In Proceedings of the Proceedings of Sixth International Congress on Information and Communication Technology: ICICT 2021, London, Volume 2. Springer, 2022, pp. 459–467.
24. Mansfield, S.; Veenstra, K.; Obraczka, K. Modeling communication over terrain for realistic simulation of outdoor sensor network deployments. *ACM Trans. Model. Perform. Eval. Comput. Syst.* **2022**, *6*, 1–22.
25. Kumar, V.; Singla, S. Energy efficient hybrid AOMDV-SSPSO protocol for improvement of MANET network lifetime. *Int. J. Adv. Technol. Eng. Explor.* **2022**, *9*, 1642.
26. Makarem, N.; Diab, W.B.; Mougharbel, I.; Malouch, N. On the design of efficient congestion control for the Constrained Application Protocol in IoT. *Comput. Netw.* **2022**, *207*, 108824.
27. Michaelides, C.; Adame, T.; Bellalta, B. ECTS: Enhanced centralized TSCH scheduling with packet aggregation for Industrial IoT. In Proceedings of the 2021 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2021, pp. 40–45.

28. Pallavi, K.; Ravikumar, V. Smart Healthcare Applications using Contiki and Cooja. *J. Pharm. Negat. Results* **2022**, pp. 1995–2002.
29. Minh, N.C.; Tran, D.T.; Hoang, Q.T.; Bui, T.N.; Anh, G.Q.; Prakash, K.B.; El-Rabaie, S. Cross-Layer Design for Wireless Sensor Networks Using Cooja Tool in Contiki Operating System. In *Intelligent Systems and Networks: Selected Articles from ICISN 2022, Vietnam*; Springer, 2022; pp. 484–494.
30. Al-Hamid, D.Z.; Al-Anbuky, A. Vehicular network dynamic grouping scheme. In Proceedings of the 2021 IEEE International conference on autonomic computing and self-organizing systems companion (ACSOS-C). IEEE, 2021, pp. 316–318.
31. Behal, A.; Sandhu, J.K.; Gupta, G. Cooja Simulator and Wireshark Traffic Capturing Are Used To Analyse User Datagram Protocol Communication For Low Power And Lossy Networks in IoT. In Proceedings of the 2023 International Conference for Advancement in Technology (ICONAT). IEEE, 2023, pp. 1–4.
32. Khisa, S.; Moh, S. Medium access control protocols for the Internet of Things based on unmanned aerial vehicles: A comparative survey. *Sensors* **2020**, *20*, 5586.
33. Magubane, Z.; Tarwireyi, P.; Abu-Mafouz, A.; Adigun, M. Extended context-aware and load balancing routing protocol for low power and lossy networks in IoT networks (ECLRPL). In Proceedings of the 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC). IEEE, 2021, pp. 1–9.
34. Tanaka, Y.; Ito, T.; Teraoka, F. 6TiSCH Scheduling Function Design Suite founded on Contiki-NG. *J. Inf. Process.* **2022**, *30*, 669–678.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.