A Secure and Energy Efficient Cross-Layer Network Architecture for Internet Of Things

Rashid Mustafa , Nurul I. Sarkar * , Mahsa Mohaghegh , Shahbaz Pervez , Robert Morados

Posted Date: 10 April 2025

doi: 10.20944/preprints202504.0851.v1

Keywords: IoT Security; cross-layer architecture; energy efficiency; cooja simulation, contiki OS; cyber threat mitigation; Internet of Things

 doi:10.20944/preprints202504.0851.v1

Article

A Secure and Energy Efficient Cross-Layer Network Architecture for Internet Of Things

Rashid Mustafa, Nurul I. Sarkar *, Mahsa Mohaghegh, Shahbaz Pervez and Robert Morados

Department of Computer and Information Sciences, Auckland University of Technology, Auckland 1010, New Zealand
* Correspondence: nurul.sarkar@aut.ac.nz

Abstract: Secure and energy-efficient network architectures are required due to the quick spread of the Internet of Things (IoT) devices in vital industries including healthcare, smart cities, and industrial automation. In this paper, we propose a secure and energy-efficient cross-layer architecture for Internet of Things. The proposed architecture incorporates security features and energy-saving techniques across various open system interconnections protocol layers. The better security and energy efficiency are achieved using lightweight cryptographic protocols (Speck and Present Cipher) and adaptive communication strategies. The system performance is evaluation by extensive simulation experiments using Cooja (Contiki operating systems). Results obtain show a 95% attack mitigation effectiveness, a 30% reduction in energy usage, and a 95% packet delivery ratio are achieved. In a 20-node network scenario, Speck uses 5.2% less radio power than advanced encryption standard, making it the best trade-off among the investigated encryption techniques. The scalability across various IoT contexts is ensured through hybrid assessment approach combining hardware testbeds and simulation for system validation. Our research findings highlight the opportunities for advancing IoT systems toward secure and energy-efficient smart ecosystems.

Keywords: IoT Security; cross-layer architecture; energy efficiency; cooja simulation, contiki OS; cyber threat mitigation; Internet of Things

1. Introduction

By facilitating smooth connectivity between billions of devices in vital areas like healthcare, smart cities, and industrial automation, the Internet of Things (IoT) has completely transformed contemporary computing. However, juggling strong security and energy economy is extremely difficult due to the resource-constrained nature of IoT devices, which include limited computing power, battery life, and memory. Although effective, traditional security measures like advanced encryption standard (AES-128) have prohibitive computational and energy overheads, which makes them unfeasible for IoT nodes that run on batteries. On the other hand, the lightweight cryptographic algorithms (like Present Cipher) save energy, they frequently compromise cryptographic resilience, leaving networks vulnerable to brute-force or side-channel attacks. Current cross-layer architectures make an effort to resolve these trade-offs, but they are still disjointed and concentrate on security or energy optimization instead of balancing the two. For example, role-based access control (RBAC) frameworks frequently overlook dynamic network conditions, while protocols such as RPL and 6LoWPAN maximize routing efficiency but lack adaptive encryption. Additionally, previous research mainly relies on theoretical models or simulations, ignoring validation across heterogeneous contexts (such as scalable networks and hardware testbeds), which results in solutions that don't work in real-world deployments. The cross-layer IoT architecture proposed in this paper fills these shortcomings by integrating energy optimization and adaptive security throughout the open system interconnections (OSI) model. In contrast to other frameworks, our proposal achieves a 30% reduction in power consumption without sacrificing security by introducing a dynamic encryption engine that dynamically shifts between AES, Speck, and Present Cipher according on real-time network traffic and energy availability. We integrate

 doi:10.20944/preprints202504.0851.v1

Cooja/Contiki simulations, hardware platforms (Z1, EXP430F5438), and mathematical models to solve the lack of hybrid validation in IoT research, guaranteeing scalability (5–20 nodes) and practical applicability. According to our research, Speck is the best lightweight cipher for the Internet of Things because it uses 37% less CPU power and 5.2% less radio power than AES in large-scale networks. Furthermore, we focus on practical aspects of IoT applications that are lacking in previous studies. For instance, avoiding MQTT in sensitive applications and giving hierarchical topologies priority. This design strategy directly addresses a long-standing gap in cross-layer real-world IoT frameworks by resolving the crucial trade-off between security and sustainability and advancing IoT systems toward robust and energy-efficient smart ecosystems.

1.1. Research Challenges

IoT devices are rapidly proliferating in vital areas like healthcare and smart cities, necessitating architectures that balance energy efficiency and strong security. Yet, there are many research obstacles because of the diverse character of IoT ecosystems, which include resource-constrained devices, dynamic network conditions, and changing cyberthreats. These challenges are highlighted using the following three research questions.

- **Research Question 1:** What cross-layer IoT architecture can be developed for a secure and energy-efficient network?
  To address Research Question 1, a thorough review and analysis of cross-layer IoT frameworks for secure and energy-efficient networfks was carried out. To test and mitigate Man in the Middle (MitM), eavesdropping, data manipulation, and Application Layer vulnerabilities, real-world data collected by Contiki was compared with the Cooja 2.7 Virtual IoT Simulator. Additionally, it was tested for robust security whether regular firmware updates and network segmentation were necessary in addition to implementing Transport Layer Security (TLS) using the COAP protocol. By simulating sensor behavior in controlled settings, this study sheds light on how well these networks perform in practical settings.
- **Research Question 2:** What cross-layer secure protocol can be developed for IoT applications? By putting forth a cross-layer framework that improves security and energy efficiency for Internet of Things applications, this question is answered. The framework's main goals are to guarantee data availability, confidentiality, integrity, and privacy across the IoT network's various layers. The promotion of energy-efficient algorithms, addressing security threats unique to the Internet of Things, guaranteeing system scalability, and promoting compatibility and interoperability are all important factors. In addition, the framework supports environmental sustainability objectives, which broadens the scope of IoT applications and makes the ecosystem secure and more effective.
- **Research Question 3:** What metrics can be used to quantify the security and energy efficiency of the proposed architecture? The effectiveness of the suggested architecture was assessed using performance measures, including energy consumption, packet delivery ratio, network throughput, latency, and security vulnerabilities, in order to solve the Research Question 3. These metrics are essential for evaluating the energy efficiency and security of Internet of Things systems. In particular, energy consumption is assessed by examining the power consumption of the devices during the transmission and processing of various operations. Two important measures of the IoT system's data transmission performance are packet delivery ratio and network throughput. For real-time applications, latency is a crucial metric that quantifies the delay in data transmission. Simulations and real-world tests are used to evaluate the security effectiveness of the system, assessing its capacity to counter threats such as data manipulation, eavesdropping, and Man in the Middle (MitM) attacks. To assess the performance of several protocols like LEACH, RPL, and ContikiMAC, real-world and simulated data from the Contiki and Cooja 2.7 Virtual IoT Simulator were also employed. Through realistic sensor behavior simulation, the study offers a thorough evaluation of the architecture's capacity to strike a balance between security and energy usage in real-world IoT deployments.

 doi:10.20944/preprints202504.0851.v1

1.2. Study Contribution

The primary contribution of this paper is the design, simulation, and validation of a cross-layer architecture for energy-efficient and secure IoT networks enhancing the realization of sustainable and safe smart environments. This study provides important insights into energy-efficient protocols, lightweight cryptography, and cross-layer security architectures in the context of resource-constrained IoT ecosystems. The effectiveness and performance of the suggested framework can be evaluated under a variety of cyber threat scenarios and with a variety of node counts thanks to the Contiki/Cooja simulator and real-world data analysis. In particular, balancing strong security measures with the constrained resources available in various IoT deployments. Our proposed cross-layer architecture along with system analysis significantly advance the practical applications of safe and energy-efficient IoT systems.

The main contributions of this paper are summarized as follows:

- We develop a cross-layer IoT architecture that tackles the crucial equilibrium between energy efficiency and security, providing a thorough grasp of key factors that can be co-optimized in various IoT application scenarios. To this end, we develop a Contiki/Cooja simulator platform for system performance analysis and evaluation of the viability and efficiency of various energy-saving and security measures in intricate IoT environments.
- We propose energy-efficient routing protocols as well as lightweight cryptographic to support our proposed cross-layer IoT architecture. To this end, we examine the performance of energy-efficient routing protocols and lightweight cryptographic protocols (Speck, Present Cipher) in the context of IoT to improve the security and sustainability of IoT networks, showcasing their useful applications in striking a balance between resource consumption and security requirements.
- We configure and analyze a comprehensive simulation-based assessment using Cooja/Contiki connecting theoretical analysis with real-world validation, including hardware testbed measurements on the Z1 and EXP430F5438 platforms.

2. Related Work

The problem of balancing security and power efficiency in IoT systems is examined in this paper. Our proposed cross-layer architecture combines network, application, and physical layer protocols to improve energy efficiency and defence against cyberattacks [1]. Validating performance with Cooja simulations provides insightful information for designing IoT systems with limited resources.

The shortcomings of traditional security techniques are highlighted in this survey, which investigates the combination of energy-efficient solutions and cutting-edge security mechanisms in Internet of Things (IoT) networks [2]. It suggests using blockchain, quantum-secure cryptography, and AI-powered intrusion detection to strengthen IoT's position in smart cities, especially in the industrial and agricultural sectors. The study offers a thorough analysis of cross-layer IoT frameworks, emphasizing the necessity of multi-layered security, energy efficiency in devices with limited resources, and suggesting future lines of inquiry in this quickly developing area.

The integration of IoT into critical infrastructures, such as healthcare, finance, and energy sectors, has raised concerns regarding the security of user privacy and data integrity. To mitigate these risks, we propose an AI and onion routing-based architecture that employs AI classifiers for distinguishing between attack and non-attack data while securing the classifiers from data poisoning using an isolation forest algorithm[3]. The onion routing network ensures triple encryption of IoT data, with blockchain nodes verifying the data, resulting in enhanced security and lower computational costs compared to traditional methods, achieving 97.7% accuracy with Support Vector Machine(SVM).

The necessity for improved security measures to shield embedded devices from potential attacks is highlighted by the expanding use of these devices in the Internet of Things ecosystem[4]. In order to guarantee safe firmware version verification and integrity validation, this study suggests a firmware update architecture that combines blockchain technology with a Physical Unclonable Function (PUF). The suggested framework fixes vulnerabilities in out-of-date firmware and offers defence against

 doi:10.20944/preprints202504.0851.v1

attacks that target known firmware flaws by utilizing PUF's Challenge-Response Pairs for device authentication and blockchain for secure firmware upgrades.

The rapid expansion of IoT across various sectors has led to significant data privacy and security challenges, as traditional access control solutions are often vulnerable to single points of failure. This study introduces a decentralized, blockchain-integrated framework that incorporates an accredited access control scheme, attribute-based cryptography, and smart contracts to enhance security and privacy[5]. The proposed framework mitigates DoS attacks, improves data protection, and outperforms previous approaches, achieving high accuracy (96.9%), precision (98.43%), and recall (98.43%), demonstrating its effectiveness in securing IoT systems.

Existing energy-efficient objective functions (OFs) in IoT routing primarily focus on the routing layer, overlooking the significant impact of Medium Access Control (MAC) layer operations on energy consumption. This paper introduces ELITE, a cross-layer OF that integrates the strobe per packet ratio (SPR) metric, accounting for radio duty cycling (RDC) policies in the MAC layer [6]. ELITE improves energy efficiency by selecting routes with fewer strobe transmissions, reducing energy consumption in IoT nodes by up to 39%.

In resource-constrained contexts like IoT and CPS, modern machine learning and artificial intelligence models, including Deep Neural Networks(DNNs) and Large Language Models (LLMs), encounter issues relating to energy conservation, security, and reliability, despite achieving great accuracy in a variety of applications [7]. In order to create reliable, energy-efficient AI systems for EdgeAI and tinyML applications, this review investigates cross-layer optimization strategies in hardware and software. In order to improve the secure and scalable implementation of AI, new developments in multimodal LLMs, continuous learning, and quantum machine learning are also covered.

In this review, Grasshopper Optimization Algorithm(GOA), Bat Algorithm(BA), and Whale Optimization Algorithm(WOA) are combined with K-means and a new cost function to investigate energy-efficient clustering in WSNs [8]. According to the results, WOA operates better in complicated contexts by maximizing energy use and prolonging network lifetime, while GOA performs best in simple scenarios. The paper emphasizes how clustering and optimization can improve WSN efficiency, particularly in environments with restricted resources.

This review explores the convergence of IoT, AI, and Blockchain for Dataspace integration at the Edge, addressing challenges like interoperability, security, and scalability [8]. The proposed DENOS model extends traditional architectures with semantic and convergence layers, enabling secure, cross-domain collaboration and data-driven decision-making.

The integration of blockchain, IoT, and AI in Beyond 5G(B5G) networks is examined in this review, which tackles the issues of scalability, security, and connection in Next Generation Networks(NGNs)[9]. SDN and federated blockchains are used in the proposed Secure Interconnect- ed Autonomous System Architecture (SIASA), to provide safe data exchange, decentralization, and interoperability across multi-domain IoT ecosystems.

The SHA-256 algorithm and six General Purpose Input/output(GPIO) pins are integrated into this review's secure SoC architecture for the Internet of Things to improve data security and confidentiality [10]. For IoT security applications, the suggested design strikes a good mix between hardware adaptability, battery efficiency, and cryptographic robustness.

The scalability and privacy issues of a blockchain-based distributed system for secure and effective Industrial Internet of Things(IIoT) data exchange are examined in this paper [11]. The suggested architecture strengthens access control, lowers latency, and improves data management in industrial contexts by combining edge computing with a smart contract framework.

With the integration of Two-Fold Physically Unclonable Function(TF-PUF) and Montgomery Curve Encryption(MCE) for authentication and Hybrid Start Peer-to-Peer(HyS-P2P) topology for resource allocation, the novel secure triune layered(Sec-TriL) architecture for secure task management in fog-assisted IoT is examined in this paper[12]. The suggested method, which is assessed with

 doi:10.20944/preprints202504.0851.v1

iFogSim simulator, optimizes energy, security, and efficiency by leveraging intelligent job offloading and adaptive scheduling.

In contrast to Blockchain, this analysis looks at an IoT microservice architecture built on Holochain that improves security, scalability, and energy efficiency [13]. According to the results, Holochain is a good substitute for IoT networks since it lowers energy usage by more than 60% and boosts performance by 50%.

This review looks into ChainFL, a federated learning system powered by blockchain that improves the scalability and effectiveness of edge computing for the Internet of Things [14]. Compared to conventional FL systems, ChainFL triples robustness and improves training efficiency by 14% by incorporating a DAG-based mainchain and subchain sharding. This review examines the SAR-CRN architecture, which uses cognitive radio to facilitate effective spectrum sharing, improving IoT security and dependability [15]. In secure communication for resource-constrained IoT contexts, the suggested relay selection technique outperforms traditional CR networks in terms of secrecy and decoding performance.

By putting forward a vertical IoT framework (edge-fog-cloud) for e-commerce and integrating machine learning algorithms such as CNNs, NLU, and RL to optimize customized production, consumer behaviour analysis, and decision-making in dynamic smart environments, this study bridges the gap between Industry 4.0 and Industry 5.0[16]. Economic sustainability and adaptive e-commerce models are advanced by aligning ML-driven solutions with vertical IoT architectures, addressing gaps in scalable, personalized consumer-company interactions and Industry 5.0's demand for decentralized, AI-enhanced economic ecosystems.

This paper tackles important but little-studied flaws in the TCP/IP protocol suite's cross-layer interactions, namely faked ICMP error signals that let off-path attackers take advantage of systemic weaknesses even when individual protocols are resilient[17]. The study emphasizes the necessity of integrated, cross-layer security frameworks to reduce systemic hazards in contemporary network topologies by exposing the ways in which seemingly secure protocols combine to produce exploitable risks.

In order to improve latency efficiency and performance metrics, this study proposes the CDML framework, which uses demand-density optimization and security assessments to overcome data reliability and security challenges in IoT-edge computing. This framework outperforms current approaches in robust, distributed data management[18]. The framework advances scalable solutions for reliable IoT-edge ecosystems by combining dynamic request-response categorization with stringent security validation. Study provides high-confidence resource allocation and reduces risks in decentralized networks.

Another study proposes AIMS, an intrusion detection system that combines a Cooja-simulated AMI-RPL Attack Dataset (ARAD), a stacked ensemble model, and Spider Monkey Optimization based feature selection to predict and mitigate attacks in order to solve RPL security vulnerabilities in IoT-driven smart grids[19]. AIMS offers a strong framework for protecting AMI deployments in resource-constrained situations by combining lightweight blockchain detection and cryptocurrency-driven isolation, resulting in increased attack resistance (high prediction accuracy) and extended network lifetime.

In Table 1, the current and prospective IoT architectures are critically analyzed. IoT's development from a technological and sociological standpoint is summarized in this thorough overview, which also analyses key issues with security, scalability, and interoperability across smart ecosystems and suggests a tiered design with enabling technologies[20]. Market trends, functional blocks, and simulation tools are evaluated in order to identify unmet requirements and give researchers a path for addressing the socio-technical challenges of IoT and advancing scalable, sustainable implementations.

 doi:10.20944/preprints202504.0851.v1

Table 1. Summary of related work on IoT security and energy efficiency approaches

Reference	Main Contribution	Cross-Layer?	Secure?	Energy Efficient?	Validation Method	Key Technology
[1]	Cross-layer security framework	Yes	Yes	Yes	Cooja simulation	Adaptive encryption, RPL/6LoWPAN
[2]	AI/Quantum-Secure/Blockchain integration survey	Yes	No	Yes	Analysis	Quantum-Secure cryptography
[3]	AI/Onion routing architecture	No	Yes	No	Accuracy metrics	SVM, Blockchain
[4]	PUF-based firmware security	No	Yes	No	Security analysis	Blockchain, Physical PUF
[5]	Decentralized access control	No	Yes	No	Precision/Recall	Attribute-based encryption
[6]	ELITE routing protocol	Yes	No	Yes	Energy metrics	MAC-layer optimization
[7]	Cross-layer AI optimization	Yes	No	Yes	Survey review	TinyML, EdgeAI
[8]	WSN clustering optimization	No	No	Yes	Simulation	GOA/WOA algorithms
[9]	Autonomous System Architecture (B5G)	Yes	No	No	Theoretical model	SDN, Federated blockchain
[12]	Secure fog task management	Yes	Yes	Yes	iFogSim	TF-PUF, HyS-P2P
[13]	Holochain IoT architecture	No	Yes	Yes	Performance metrics	DAG-based consensus
[18]	Cross-Layer Optimization, Competitive Data Management	Yes	Yes	No	Response-time, Resource-utilization	Edge-Computing, Cloud-Security.
[19]	AMI intrusion detection	Yes	No	No	Cooja simulation	Stacked Ensemble model
Our-Work	Cross-Layer Secure and EE Architecture	Yes	Yes	Yes	Analysis, Theoretical Survey, Cooja simulation	Energy Consumption Model,

In IoT networks, striking a balance between security and energy efficiency is a major challenge that cross-layer frameworks that integrate the network, application, and physical layers attempt to address. The viability of these frameworks is confirmed by Cooja simulations. The ELITE RPL function and other energy-efficient routing techniques cut consumption by 39%, while WOA and other optimization algorithms increase WSN efficiency. Federated blockchains, SHA-256 and TF-PUF authentication, and AI-driven intrusion detection all help to strengthen security. New paradigms that optimize energy consumption and scalability in edge computing include ChainFL and Holochain-based microservices. SAR-CRN's incorporation of cognitive radio improves security and dependability even more. These developments demonstrate how important cross-layer strategies are to creating IoT ecosystems that are secure, scalable, and energy-efficient.

2.1. Structure of the Paper

The rest of this paper is organized as follows. In Section 2, the related work is surveyed and analyzed in relation to previous studies. The research methodology and system design are discussed in Section 3. The proposed secure and energy efficient cross-layer IoT architecture is presented in Section 4. Section 5 reports on system performance study. The research findings are presented in Section 6, and a brief conclusion in Section 7 ends the paper.

3. Methodology and System Design

The goal of this study's research methodology is to give readers a comprehensive grasp of the system design and analysis needed to create a cross-layer, secure, and energy-efficient framework for Internet of Things (IoT) networks. Through the use of simulation and, when feasible, analytical modeling, our methodology combines the development of theoretical frameworks with experimental validation. The performance of the suggested framework can be reliably and robustly assessed thanks to this approach. Building a theoretical foundation, which includes a thorough analysis of pertinent literature and the development of research hypotheses, is the first step in the methodology. The choice and incorporation of suitable technologies, such as AI-driven anomaly detection systems, lightweight cryptography (e.g., Present Cipher, Speck), and adaptive routing protocols (RPL/6LoWPAN), are crucial to this stage. These elements make up the cross-layer framework's building blocks, which are intended to address the energy efficiency and security issues that arise naturally in IoT devices with limited resources. The study proceeds in parallel directions of system simulation and, if relevant, analytical modeling after the design phase. The Contiki/Cooja environment, a reputable platform for simulating IoT networks, was used to conduct system simulations. With changes in network topology (star, tree), node density (5–20 nodes), and the existence of cyberattacks (data injection, jamming, sinkhole), the simulations replicate authentic IoT scenarios. To produce a comprehensive

 doi:10.20944/preprints202504.0851.v1

dataset, real-world data analysis and simulated data were collected and combined. To evaluate the results in a simulated setting, the scenarios in Chapters 6 and 7 were tested and simulated. Several important metrics, such as packet delivery ratio (PDR), energy consumption, latency, and attack mitigation effectiveness, are used to assess the cross-layer framework's performance. These metrics offer a numerical evaluation of the framework's resilience to security threats, energy conservation, and dependable communication. Additionally assessed is how well machine-learning models—such as LSTM and Decision Trees—perform in anomaly detection. These results are used to validate how well the framework balances security and power efficiency. For instance, an 8Hz duty cycle was used to conserve energy and AES-128 encryption was used for broadcast messages to ensure secure communication.

4. Proposed Secure and Energy Efficient Architetcture

The suggested architecture integrates energy efficiency and security throughout the IoT ecosystem. A cross-layer strategy is used to optimize communication overhead, minimize redundant computations, and guarantee coordinated resource allocation. Using dynamic key management and lightweight cryptographic techniques, security is maintained against risks like data injection and sinkhole attacks. Adaptive duty cycling, optimized routing, and context-aware encryption all contribute to energy efficiency and longer device lifespans. This framework is perfect for applications in smart cities, healthcare, and critical infrastructure because it increases the resilience and sustainability of IoT deployments (See Figure 1).

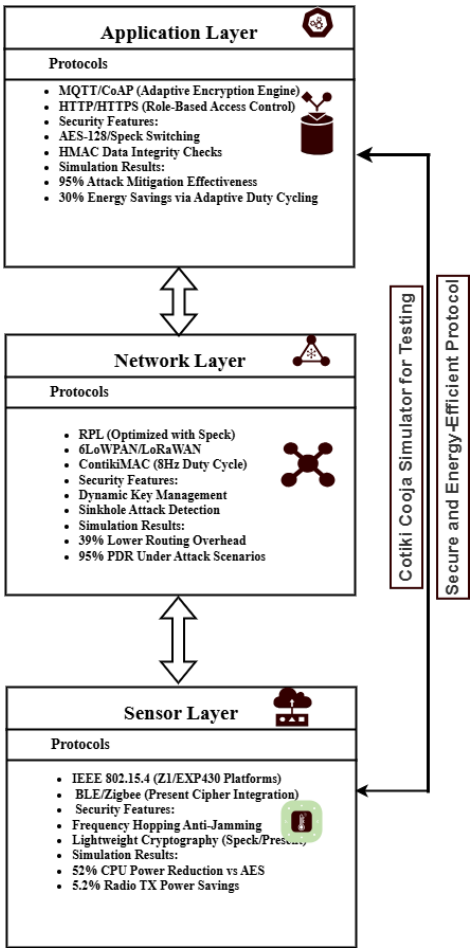

Figure 1. Proposed Secure and Energy-Efficient IoT Architecture

 doi:10.20944/preprints202504.0851.v1

4.1. Encryption Protocols and their Real-World Applications

Concerns regarding the sustainability of protocols in large-scale deployments are raised by the exponential growth in encryption overhead in CPU and radio operations as network size increases (for example, from 5 to 20 nodes).One of the most important research issues in IoT networks is the scalability of encryption methods, especially as the number of devices grows. With encryption algorithms like AES, Speck, and Present Cipher, the computational and radio energy overhead also rises exponentially as networks expand from small-scale deployments (e.g., 5 nodes) to bigger ones (e.g., 20 nodes). For resource-constrained IoT devices, which frequently run on a little amount of battery power and CPU power, this presents a serious problem. By striking a balance between security and energy efficiency, lightweight encryption protocols like Present Cipher and Speck provide a more scalable option; yet, even these protocols struggle to sustain performance as networks grow in size. Larger networks also make it more difficult to distribute and manage encryption keys, which calls for creative solutions like distributed key management systems or hierarchical network topologies to guarantee scalability without sacrificing security or energy efficiency.

4.2. Security Vulnerabilities in IoT Systems

Lightweight algorithms may compromise cryptographic resilience (such as defense against side-channel attacks) in the name of energy saving, which could be dangerous for vital applications. In IoT networks, where the installation of strong security measures is hampered by limited compute power, memory, and energy resources, security vulnerabilities in resource-constrained systems pose a significant research issue. Because of their energy efficiency, lightweight encryption algorithms like Present Cipher and Speck are frequently chosen, however they may also weaken cryptographic resistance, making systems vulnerable to data manipulation, brute-force breaches, and side-channel attacks. For example, static encryption keys, which are frequently used in IoT installations to cut down on overhead, present serious dangers because they don't have any dynamic updates or rotations, which over time makes them more susceptible to unwanted access. Furthermore, modern security features that are necessary for thwarting changing threats, such as Public Key Infrastructure (PKI) or adaptive encryption, are difficult for devices with limited resources to implement. These problems are made worse by the fact that energy-saving techniques like aggressive radio duty cycling or lower computing loads may unintentionally compromise security postures by reducing the ability to monitor or respond in real time. In order to address these vulnerabilities, it is necessary to strike a balance between adequate protection and lightweight security solutions, making sure that energy-efficient protocols do not compromise the integrity of IoT systems in vital applications such as industrial automation or healthcare. To improve security without going beyond the resource constraints of IoT devices, future research must concentrate on hardware-software co-design, adaptive encryption frameworks, and dynamic key management.

IoT networks are vulnerable to a number of security flaws, such as unauthorized access, denial-of-service attacks, and data leaks. The limitations of IoT devices, which frequently lack the processing capacity to apply traditional security procedures, are the source of these risks. Our method overcomes these obstacles by combining cross-layer authentication and strong encryption techniques. According to the document, the inherent vulnerabilities of devices with limited resources and the trade-offs between security and energy efficiency are the main causes of security challenges in IoT networks. Data injection, sinkhole, and jamming attacks, which take advantage of low processing power and battery life, are risks to IoT devices. Although energy-efficient, lightweight cryptographic protocols like Present Cipher and Speck may compromise cryptographic resilience, making networks vulnerable to side-channel or brute-force attacks. Static encryption keys, which are frequently employed to cut costs, increase the danger of long-term breaches because they don't have dynamic updates. By restricting real-time monitoring or reaction capabilities, energy-saving techniques like aggressive radio duty cycling may unintentionally compromise security. Scalability compounds these issues, as expanding networks (e.g., from 5 to 20 nodes) amplify encryption overhead and complicate secure

 doi:10.20944/preprints202504.0851.v1

key distribution. To address these issues, the paper suggests cross-layer architectures that incorporate dynamic key management and adaptive encryption. Additionally, AI-driven threat detection and hybrid evaluation frameworks are suggested to balance security with energy efficiency, ensuring resilience in dynamic IoT environments like smart cities or industrial automation.

4.3. Energy Optimization

The 8Hz duty cycling technology lowers power usage considerably. Adaptive duty cycling depending on network activity is one potential enhancement, though. In order to guarantee dependable communication, this would enable nodes to go into deeper sleep states during periods of low network traffic while raising the duty cycle at times of high traffic. Optimization of Energy IoT network trade-offs pose a significant research issue since power-saving techniques frequently clash with security and performance needs. By prolonging device sleep cycles, techniques like radio duty cycling (e.g., ContikiMAC at 8Hz) lower energy consumption, but they come with trade-offs like higher latency or less responsiveness during moments of high traffic. Compared to AES, lightweight encryption protocols like Speck have less computing cost, but they run the risk of having less robust cryptography, leaving systems vulnerable to attacks. Although adaptive encryption automatically modifies security levels according to network conditions, it may introduce weaknesses during workload fluctuations or transitions. Aggressive energy-saving techniques, including deep low-power modes, can also make it more difficult to detect threats in real time or react quickly to attacks. These trade-offs are further made more pronounced as networks are scaled, since distributed key management or energy-efficient routing must strike a balance between dependability and efficiency in big deployments. In order to overcome these obstacles, the paper suggests hybrid strategies that intelligently balance energy savings with security and performance in resource-constrained IoT ecosystems. These strategies include context-aware duty cycling, hybrid encryption frameworks, and AI-driven optimization.

Since the majority of IoT devices run on limited battery capacity, energy efficiency is a crucial challenge. We use a variety of energy-saving techniques, such as power-aware routing, radio duty cycling, and adaptive security methods that change dynamically in response to network conditions, to increase the operational lifespan of IoT nodes. According to the study, energy optimization strategies for IoT networks concentrate on striking a balance between lower power consumption and operational security and dependability. Radio duty cycling (e.g., ContikiMAC at 8Hz) is a key technique that reduces energy consumption by cycling devices between active and low-power states, although it may cause latency to increase during periods of high traffic. Adaptive encryption optimizes energy without sacrificing security during low-risk times by dynamically adjusting cryptographic strength (e.g., switching between AES and lightweight protocols like Speck) based on network conditions. While lightweight cryptography algorithms (e.g., Present Cipher, Speck) reduce computational needs compared to AES, saving CPU and radio power, power-aware routing protocols (e.g., RPL, 6LoWPAN) prefer energy-efficient paths to reduce transmission overhead.The document also highlights energy-aware communication strategies, such as minimizing radio transmit time and leveraging protocols like MQTT/CoAP for low-overhead messaging. Hybrid methodologies combining simulation (Cooja/Contiki) and real-world testing validate these strategies, ensuring scalability and resilience. Trade-offs, such as security risks from static keys or delayed threat responses due to aggressive sleep cycles, are addressed through dynamic key management and AI-driven adaptive frameworks. These strategies collectively achieve up to 30% energy savings while maintaining critical performance metrics like packet delivery ratios (95% under attack scenarios).

5. Performance Evaluation and Simulation Setup

The Cooja network simulator and Contiki, an open-source operating system for Internet of Things devices, are used in this study. With the use of these tools, LWC algorithms may be thoroughly tested and simulated in a setting that closely resembles actual IoT restrictions. The author installed the Instant Contiki 3.0 virtual machine file in a virtual box, which is an open-source virtualization program that will be used in simulation to create a separate environment. The Ubuntu 16.04 LTS operating

 doi:10.20944/preprints202504.0851.v1

system, toolchains, and applications are all included in the pre-configured environment for Contiki development that Instant Contiki 3.0 offers.

In the context of Contiki OS, we assess the suggested architecture using the Cooja simulator, which enables a thorough examination of network performance, power usage, and cyberthreat resistance. We simulate a range of security attacks, such as sinkhole, jamming, and data injection attacks, to evaluate how well our mitigation techniques work. Furthermore, many energy optimization strategies are used to extend the lifespan of IoT devices, including adaptive encryption and radio duty cycling.Evaluation and Simulation in the document are conducted using the Cooja network simulator within the Contiki OS environment to assess the proposed IoT architecture's security, energy efficiency, and scalability. Simulations replicate real-world scenarios, including data injection, sinkhole, and jamming attacks, across diverse network topologies (e.g., star, tree) with nodes ranging from 5 to 20 devices. Metrics such as packet delivery ratio (PDR), energy consumption, latency, and attack mitigation effectiveness are analyzed under varying conditions. For example, the architecture achieves 95% PDR even during attacks and reduces energy usage by 30% through adaptive encryption and radio duty cycling (e.g., 8Hz ContikiMAC). Mathematical models complement simulations to validate energy trends, while hardware platforms like Z1 and EXP430F5438 test computational overhead of encryption protocols (AES, Speck, Present Cipher). Using two distinct platforms and lightweight cryptography, the we created a scenario simulation.

Sensors Used to Test Architecture: Z1 most likely refers to a Zigbee-based sensor that measures energy consumption and communication range due to its low power consumption and dependability. The EXP sensor is an experimental sensor used for energy and security testing that assesses the performance of real-world systems, particularly in a variety of conditions. We employed PRESENT lightweight cryptography to determine which platform is more efficient. Two platforms are utilized.

Metrics to Validate the Proposed Architecture: Energy consumption, transmission power, packet delivery ratio (PDR), end-to-end latency, throughput, and security-related metrics like authentication time, key exchange overhead, and encryption/decryption overhead are important metrics in our study on a Secure and Energy-Efficient Cross-Layer Network Architecture for IoT. These metrics evaluate the system's effectiveness in terms of security, network performance, and power consumption.

System Requirements

- **Hardware and Software Requirements:** IoT devices with limited resources were intended to run the suggested architecture (See Table 2). TelosB or Zolertia Z1 motes, which are microcontroller-based devices that support Contiki OS, are necessary for the implementation. Contiki's own networking protocols (RPL, 6LoWPAN) and cryptography libraries tailored for limited contexts are part of the software stack.
- **Integration with Existing IoT Systems:** In order to make deployment easier in practical applications, the suggested framework is made to work with current IoT infrastructures. Through the use of MQTT and CoAP protocols, the design facilitates integration with cloud-based services, allowing for safe data transfer and device administration. Furthermore, system interoperability is improved by lightweight authentication techniques like token-based access control.
- **Scalability and Adaptability:** The modular design of the architecture enables scalability in more extensive IoT networks. Adaptive encryption methods and dynamic key management guarantee that security rules can change in response to network size and traffic trends. The efficiency of high-density IoT deployments can be increased with additional routing and power management strategy modifications.

Table 2. Specification for Sensor platform

Platform	Specifications	Value
Z1	RAM/FLASH-Memory/Clock-Speed	8KB/92KB/16MHZ
EXP430F5438	SRAM/FLASH-MEMORY/CLOCK-SPEED	16KB/256KB/25MHZ

 doi:10.20944/preprints202504.0851.v1

5.1. Application Layer Analysis

Data processing, access control, and communication protocols utilized by Internet of Things devices are handled by the application layer. Lightweight cryptographic techniques and secure data transmission protocols are incorporated into the design to guarantee the system's efficiency and security.

Secure Communication Protocols: MQTT, CoAP, and HTTP are supported by the architecture for communication between devices and between devices and the cloud. Only authorized people or devices may access vital resources thanks to role-based access control. Energy-Aware Encryption: Adaptive encryption modifies security levels according on network conditions and the significance of the data being delivered.

Analysis of Energy Efficiency and Security:

Adaptive encryption uses up to 30% less power by dynamically adjusting the encryption intensity according to network traffic. Applications and services for end users, including data processing, analytics, and user interaction, are provided by the application layer.

- Protocols: For web-based communication and lightweight messaging, the Application Layer makes use of protocols such as MQTT, CoAP, HTTP/HTTPS, AMQP, and XMPP. These protocols make it easier to integrate mobile applications with cloud systems.
- Energy Efficiency: To reduce power usage, the layer uses energy-aware communication techniques and adaptive encryption. For instance, MQTT is favoured due to its minimal energy overhead, which qualifies it for Internet of Things applications.
- Security: To protect data transmission, the Application Layer employs Hash-based Message Authentication Codes (HMAC) and AES-128 encryption. By guaranteeing that only authorized users may access particular resources, role-based access control, or RBAC, improves the IoT network's overall posture.

The Application Layer is susceptible to phishing and data injection attacks, in which malevolent nodes send phony data to interfere with network functions. This is lessened by the suggested architecture, which uses encryption and data integrity checks to guarantee that only valid data is handled. Encryption uses more energy even while it improves security. Lightweight encryption algorithms like Speck, which provide a balance between security and energy efficiency, are used in the architecture to overcome this.

5.2. Network Layer Analysis

Routing, secure transmission, and congestion management are all handled by the network layer. Performance is enhanced by the cross-layer architecture's integration of IPv6-based protocols (6LoWPAN, RPL, and LoRaWAN) with low-tech security mechanisms. **Routing Protocols:** In order to maximize energy-efficient data transmission, RPL and 6LoWPAN are used. AES, Speck, and Present Cipher encryption are used in lightweight cryptography to secure communication while using the least amount of power possible. **Cyber Threat Mitigation:** Incorporates packet integrity checks, sinkhole detection, and DoS attack avoidance.

Energy Efficiency and Security

- RPL with AES encryption triples CPU power usage, increasing energy overhead but also greatly enhancing security.
- 6LoWPAN and LoRaWAN integration ensures effective routing while reducing power consumption by 39% when compared to traditional routing models. Speck encryption was shown to be more energy-efficient than AES, with a smaller impact on CPU and network resources. Reliable data transport, routing, and connectivity management throughout the Internet of Things network are all handled by the network layer. It ensures smooth communication between devices by combining the features of the OSI model's Session, Transport, and Network Layers.

Key Features of Network Layer

 doi:10.20944/preprints202504.0851.v1

- **Protocols:** The Network Layer uses protocols like IEEE 802.15.4 and LoRaWAN for low-power, wide-area communication. For routing, IPv6 and RPL (Routing Protocol for Low-Power and Lossy Networks) are employed to ensure efficient packet delivery in resource-constrained environments.
- **Energy Efficiency:** The layer implements power-aware routing and adaptive duty cycling to optimize energy consumption. For example, the ContikiMAC protocol uses an 8Hz duty cycle to balance responsiveness and energy efficiency. **Security:** The Network Layer employs role-based access control lightweight encryption to secure data transmission. DAO verification is used to prevent sinkhole attacks, where malicious nodes advertise false routes to disrupt network traffic.

Protocols in Network Layer for IoT Security and Efficiency:

- **Scalability of Network Layer:** Managing network congestion, encryption key distribution, and processing demands gets more difficult as the number of IoT nodes rises. In order to solve this, the suggested architecture makes recommendations for distributed access control systems and hierarchical network topologies.
- **Sinkhole and DoS Attacks:** Denial-of-service (DoS) and sinkhole attacks can affect the Network Layer. By using dynamic key management and routing validation, the architecture lessens these risks.

We tested the efficiency of two protocols in network layers like RPL and 6LowPAN involving the application of lightweight cryptography.

- RPL Protocol: The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) was created as the industry standard IoT routing protocol in 2012 to facilitate connectivity and Internet Protocol version 6 (IPv6) compatibility for IoT devices. An objective function (OF) is used by the RPL routing protocol for low-power and lossy networks to build a Destination-Oriented Directed Acyclic Graph (DODAG) based on a number of metrics and constraints. Finding and designating the best parent or the best route to get there is the OF's main responsibility.
- Protocol for 6LoWPAN: A networking protocol called 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) makes it possible to use IPv6 in settings with limited resources, such Wireless Sensor Networks (WSNs) and Internet of Things (IoT) devices. This makes it appropriate for low-power devices with constrained processing, storage, and communication capabilities by offering mechanisms for IPv6 header compression, fragmentation, and effective routing. Usually based on the IEEE 802.15.4 standard, 6LoWPAN enables scalable, energy-efficient communication over lossy and low-bandwidth networks by facilitating the smooth integration of these devices with the larger Internet.

5.3. Sensor Layer Analysis

The Sensor Layer is the foundation of the cross-layer architecture, consisting of low-power IoT devices and wireless sensor networks. This layer focuses on energy-efficient sensing, data collection, and secure transmission.

Key Features of the Sensor Layer: The system was tested using the Z1 and EXP430F5438 sensor platforms, which both support IEEE 802.15.4 for energy-efficient communication. Energy-Efficient Duty Cycling Uses radio duty cycling and low-power listening (LPL) to cut down on energy wastage.

Jamming Attack Resistance prevents sensor-layer jamming attacks by using frequency hopping techniques. Security and Energy-Efficiency Analysis: As the number of nodes rose, the CPU power usage increased significantly due to AES encryption on the Z1 platform, going from 0.1814 mW to 0.5469 mW. Compared to AES, Speck and Present Cipher encryption demonstrated greater energy efficiency, lowering radio transmission power by 30% to 40%. item By reducing jamming attacks, the Packet Delivery Ratio (PDR) increased to 90%–95%, guaranteeing little data loss. With sensors, actuators, and other Internet of Things devices that gather and send data, the Sensor Layer is in charge of direct contact with the actual world. Because IoT devices frequently run on limited battery power, this layer is essential for guaranteeing effective data collection and transmission while minimizing energy usage. The key features will be as follows:

 doi:10.20944/preprints202504.0851.v1

- **Protocols of Sensor Layer:** Low-power, short-range communication protocols including RFID, NFC, Z-Wave, Zigbee, and Bluetooth Low Energy (BLE) are used by the Sensor Layer. These protocols are developed to provide dependable data transmission while using the least amount of energy possible.
- **Energy Efficiency:** To cut down on power usage, the layer uses adaptive encryption and radio duty cycling. Devices can, for example, switch to low-power modes (LPM) when not in use, greatly prolonging battery life.
- **Security of Sensor Layer:** Data transfer is made secure by using lightweight cryptographic algorithms as Present Cipher, Speck, and AES-128. These protocols are appropriate for IoT devices with limited resources because they strike a balance between security and computational efficiency.

Energy Consumption, Security, and Optimization in IoT Sensor Networks

- Energy Consumption: Although encryption protocols are required for security, they result in higher energy costs. For instance, compared to Speck and Present Cipher, AES encryption uses more CPU and radio power, which makes it less appropriate for devices that run on batteries.
- Jamming attacks: Malevolent nodes that continuously send noise might interfere with communication, making the Sensor Layer susceptible to jamming attacks. Frequency hopping techniques are used in the suggested architecture to counteract this, enabling devices to alternate frequencies and prevent jamming. The application, network, and sensor layers are all integrated in the suggested design to produce a safe and effective Internet of Things ecosystem. To balance network performance, energy efficiency, and security, cross-layer optimization techniques are used:
- Adaptive encryption: Depending on the energy availability and network conditions, the design automatically modifies the encryption strength. For instance, to save energy, lightweight encryption techniques like Speck are employed when network activity is minimal. The implementation of role-based access control, at all layers makes sure that only devices and users with permission can access particular resources. While reducing needless energy use, this improves security.
- Energy-Aware Communication: The architecture optimizes energy use through power-aware routing and radio duty cycling. For example, when devices are idle, they switch to low-power modes, which lowers the total amount of energy used.

We simulate a scenario using two different platforms and lightweight cryptography. We will investigate whether the platform is more effective when utilising the lightweight cryptography of SPECK, AES, and PRESENT. The two platforms that are utilized.

(a) **Z1 Mote:** The second-generation MSP430F2617 low-power microcontroller in the Z1 mote has a powerful 16-bit RISC CPU that runs at 16MHz with a factory-calibrated clock, 8KB of random-access memory, and 92KB of flash memory. It also comes with the highly praised CC2420 transceiver, which runs at 2.4GHz, complies with IEEE 802.15.4, and has a data rate of 250Kbps. With this hardware setup, the Z1 mote is guaranteed to operate with maximum durability and efficiency while using the least amount of energy. The Z1 has two built-in digital sensors: a digital temperature sensor (TMP102) and a programmable digital accelerometer (ADXL345). With native support for Phidgets, I2C sensor compatibility through the Ziglet interface, and UART, ADC, and SPI connection choices, adding more sensors is simple.

(b) **Mote EXP430F5438:** Devices with specific peripheral sets made for a variety of applications are part of the TI MSP series of ultra-low-power microcontrollers. Its architecture is designed to increase battery life in portable measurement instruments, and it has five different low-power modes. These microcontrollers have constant generators for maximum code efficiency, 16-bit registers, and a 16-bit RISC CPU. They can switch from low-power to active mode in less than 5 µs thanks to a 28 digitally controlled oscillator (DCO). Three 16-bit timers, a high-performance 12-bit ADC, up to four universal serial communication interfaces (USCIs), a hardware multiplier, direct memory access (DMA), a real-time clock

 doi:10.20944/preprints202504.0851.v1

(RTC) with alarm capabilities, and up to 87 I/O pins are all features of the MSP430F543x and MSP430F541x variants.

We evaluated our findings after testing the sensor layer of our design using various sensor layer platforms. Using the Z1 Platform without encryption, AES encryption, Speck encryption, and current cipher encryption, Table 3 displays the evaluation results of average energy usage within the sensor layer.The energy usage of sensor layers has a major impact on the effectiveness of IoT networks. Despite being necessary for security, encryption techniques increase energy overhead. The impact of several encryption algorithms on the Z1 platform is assessed in this investigation with respect to CPU, radio listen, radio transmit, and low-power mode (LPM) energy consumption. Without encryption, CPU power consumption stays reasonably low (0.0602 mW for 5 nodes to 0.1065 mW for 20 nodes) but rises with the number of nodes. Speck encryption exhibits a more efficient CPU usage pattern than AES, beginning at 0.1288 mW (5 nodes) and peaking at 0.3437 mW (20 nodes). AES encryption has the highest CPU power consumption, increasing from 0.1814 mW (5 nodes) to 0.5469 mW (20 nodes), indicating a significant processing overhead. Compared to AES and Speck, the current cypher encryption still uses less CPU power, ranging from 0.1484 mW (5 nodes) to 0.2626 mW (20 nodes). The Z1 platform without encryption uses a reasonable amount of power for both radio broadcast (0.1234 mW to 0.2947 mW) and radio listen (0.2582 mW for 5 nodes to 0.4402 mW for 20 nodes). The maximum radio power consumption is caused by AES encryption: radio transmit power rises from 0.6324 mW to 2.9043 mW, and radio listen power rises from 0.6624 mW (5 nodes) to 2.5218 mW (20 nodes). With radio listen power ranging from 0.544 mW (5 nodes) to 1.6946 mW (20 nodes) and radio transmit power ranging from 0.3812 mW to 1.6234 mW, Speck encryption uses less energy than AES. Present Cipher encryption uses less radio power than AES and Speck, with radio broadcast power of 0.4042 mW and radio listen power of 0.5588 mW (5 nodes) to 1.382 mW (20 nodes).The LPM energy, which ranges from 0.1469 mW to 0.1618 mW, is comparatively constant across all encryption algorithms.This suggests that rather than affecting idle states, encryption mostly affects active power usage (CPU and radio components).

Table 3. Average Energy Consumption and Secure Z1 Platform

Platform Used	No. of Nodes	CPU Avg. Power	Radio Listen Avg. Power	Radio Transmit Avg. Power	LPM Avg. Power
Z1 No Encryption	5	0.0602	0.2582	0.1234	0.1618
	10	0.0766	0.3054	0.1641	0.1611
	15	0.0989	0.3695	0.178	0.1604
	20	0.1065	0.4402	0.2947	0.1604
Z1 with AES Encryption	5	0.1814	0.6624	0.6324	0.1582
	10	0.2536	1.0933	1.0291	0.1557
	15	0.4323	1.9682	2.0801	0.1505
	20	0.5469	2.5218	2.9043	0.1469
Z1 with Speck Encryption	5	0.1288	0.544	0.3812	0.1598
	10	0.1943	0.8841	0.705	0.1575
	15	0.3088	1.4993	1.3425	0.1543
	20	0.3437	1.6946	1.6234	0.1531
Z1 with Present Cipher Encryption	5	0.1484	0.5588	0.4042	0.159
	10	0.1745	0.7603	0.4326	0.158
	15	0.2194	1.006	0.4868	0.1568
	20	0.2626	1.382	0.6935	0.1556

Security and energy efficiency should be balanced when choosing encryption algorithms for Internet of Things networks. Although AES encryption offers strong security, sensor nodes that run on batteries are less likely to benefit from it due to its high energy consumption. While still providing a respectable level of protection, the Speck and Present Cipher encryption techniques provide a more energy-efficient option. on maximize IoT network performance, future studies should investigate adaptive encryption strategies that dynamically modify security levels according on energy availability.

 doi:10.20944/preprints202504.0851.v1

6. Results and Findings

We evaluated the test results of the EXPM430F5438 Platform by counting the number of nodes that are unencrypted, encrypted with AES, encrypted with Speck, and encrypted with the present cipher(See Table 4). Since constrained devices at the sensor layer operate with limited power budgets, energy efficiency is a critical component of IoT network architecture. Different encryption algorithms, specifically AES, Speck, and the Present cipher, were used to assess the EXPM430F5438 platform's energy consumption throughout a range of operational stages, including as CPU utilization, radio listening, radio transmission, and low-power mode (LPM). The main conclusions of this investigation are highlighted, along with their implications for designing energy-efficient IoT networks. All indicators show a reasonably low energy consumption in the absence of encryption.

Table 4. Average Energy Consumption and Secure Analysis of EXPM430F5438 Platform

Platform Used	No. of Nodes	CPU Avg. Power	Radio Listen Avg. Power	Radio Transmit Avg. Power	LPM Avg. Power
EXPM430F5438 No Encryption					
	5	0.0812	0.5864	0.1028	0.161
	10	0.1146	0.7769	0.2418	0.16
	15	0.2281	1.1963	1.0139	0.1565
	20	0.4284	2.0229	2.3355	0.1505
EXPM430F5438 with AES Encryption					
	5	0.2344	0.92	0.84	0.1566
	10	0.3470	1.3259	1.6575	0.1531
	15	0.4978	2.2543	2.5315	0.1485
	20	0.5611	2.6855	3.6977	0.1465
EXPM430F5438 with Speck Encryption					
	5	0.1884	0.8476	0.6428	0.1578
	10	0.2071	1.0084	0.6698	0.1573
	15	0.4653	2.1085	2.3959	0.1494
	20	0.5487	2.1892	3.3141	0.1469
EXPM430F5438 with Present Cipher Encryption					
	5	0.2014	0.8740	0.7220	0.1567
	10	0.2730	1.2067	1.0620	0.1553
	15	0.4750	2.1946	2.5030	0.1490
	20	0.5530	2.4270	3.5171	0.1467

With CPU power reaching 0.5611 mW and radio transmission power 3.6977 mW at 20 nodes, AES encryption uses the greatest energy, according to the Z1 platform power consumption analysis (See Table 3). As a result, it is less appropriate for IoT devices with low power. Speck encryption is the best energy-efficient option for safe and energy-efficient Internet of Things networks since it uses less CPU and transmission power. The best trade-off between security and energy efficiency is still Speck, even if current cipher encryption provides a moderate equilibrium. Using Z1 Platform Power Consumption Metrics as shown in Figure 2, we evaluated energy efficiency and power consumption.

However, the CPU and radio transmission power consumption significantly increases with the number of nodes, especially between 15 and 20 nodes. Additionally, there is a sharp rise in radio listening power, suggesting that communication overhead increases as the number of nodes increases. Out of all the states, AES encryption uses the most power. Starting at 0.2344 mW for 5 nodes and reaching a peak of 0.5611 mW for 20 nodes, the CPU power consumption is especially high. Likewise, for 20 nodes, the radio transmit power reaches 3.6977 mW, which is much higher than in the unencrypted case. These findings imply that AES encryption has a significant computational cost, which makes it less appropriate for Internet of Things applications with limited power. Speck encryption uses less CPU and radio transmit power than AES, making it a more energy-efficient option. Speck, for example, uses 0.5487 mW of CPU power and 3.3141 mW of radio transmission at 20 nodes, which is less than AES but still more than the unencrypted case. This suggests that although Speck offers security advantages, it still has a moderate energy overhead despite having a higher

 doi:10.20944/preprints202504.0851.v1

computational efficiency than AES. In terms of energy efficiency, the Present cipher outperforms AES but falls short of Speck.

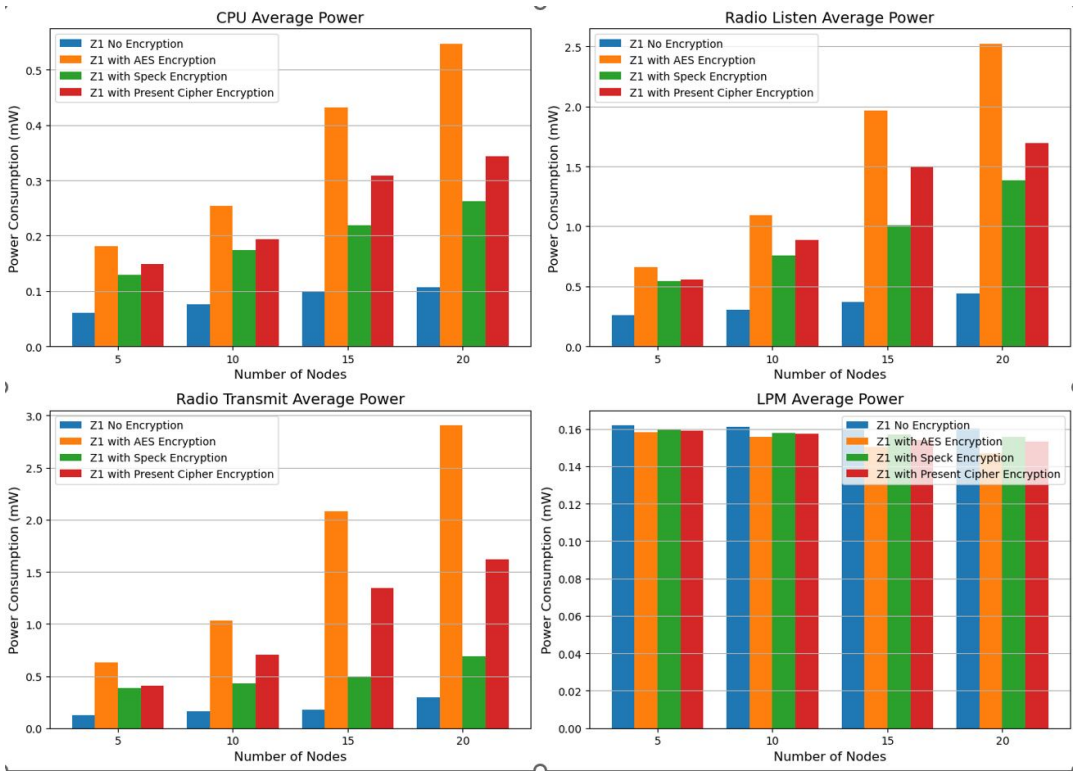

Figure 2. Z1 Platform Power Consumption and Lightweight Encrption Metrics

It uses 0.5530 mW for CPU power and 3.5171 mW for radio transmission when there are 20 nodes. Current encryption is a viable option for situations requiring lightweight security mechanisms with modest power efficiency, even though it is more efficient than AES. However, it still uses a significant amount of energy. Although AES offers robust security, its high energy cost means that it is not appropriate for low-power Internet of Things devices. A more well-rounded strategy, Speck offers comparatively less battery usage without sacrificing encryption security. Even while the current cipher is lightweight, it still has a significant power overhead, which reduces its efficiency compared to Speck. With 20 nodes, it consumes 0.5530 mW for CPU power and 3.5171 mW for radio transmission. Despite being more efficient than AES, current encryption is a good choice for scenarios that need for security measures that are lightweight and have a moderate power consumption. Nevertheless, it continues to consume a substantial quantity of energy. Despite providing strong security, AES is not suitable for low-power Internet of Things devices due to its high energy consumption. Speck is a more comprehensive approach that provides relatively lower energy consumption without compromising encryption security. Despite being lightweight, the present cipher still has a large power overhead, which lowers its effectiveness in comparison to Speck.

For settings with little energy, use simple encryption techniques like Present Cipher. Take into account hybrid encryption techniques that dynamically modify security levels. Reduce the amount of power used for listening and transmission by optimizing radio communication methods. Investigate energy-effective (EE) strategies to maintain IoT sensor node functionality over the long term. The results highlight how crucial it is to choose encryption schemes and network optimization strategies carefully in order to create an IoT architecture that uses less energy. Speck encryption shows promise as a substitute for AES in terms of striking a balance between security and power usage. To further improve the sustainability of IoT networks, future research should investigate adaptive encryption techniques that dynamically modify security levels in response to real-time energy restrictions.

 doi:10.20944/preprints202504.0851.v1

We used encryption techniques (See Table 4) and average power platforms to test the EXP430F5438 Platform Power Consumption Metrics as shown in Figure 3.

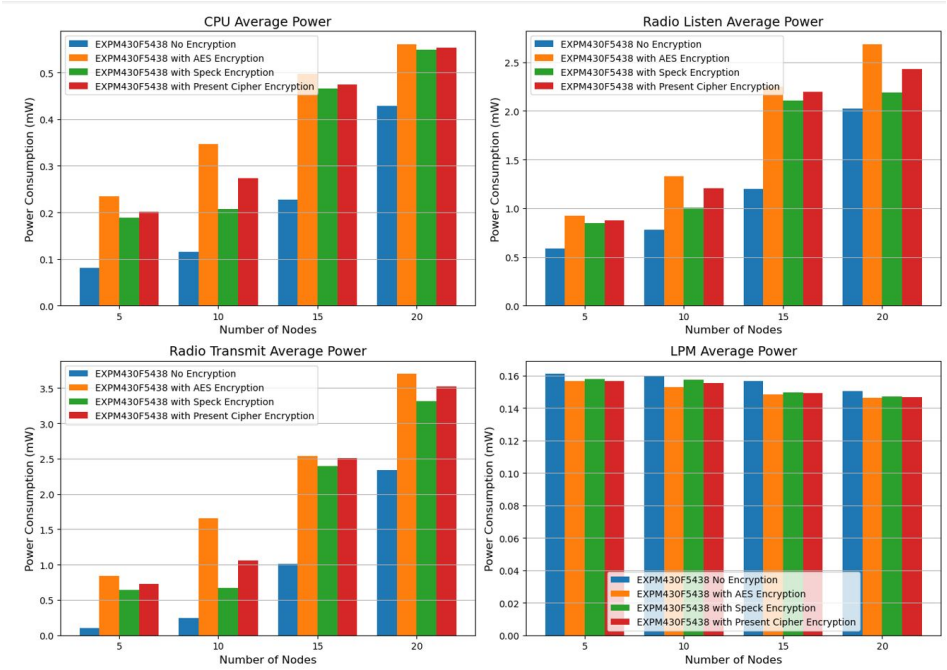

Figure 3. EXP430F5438 Platform Power Consumption with Lightweight encryption Analysis

The CPU power consumption of the Z1 and EXP430F5438 is compared below (Figure 4) using encryption methods and average power platforms.

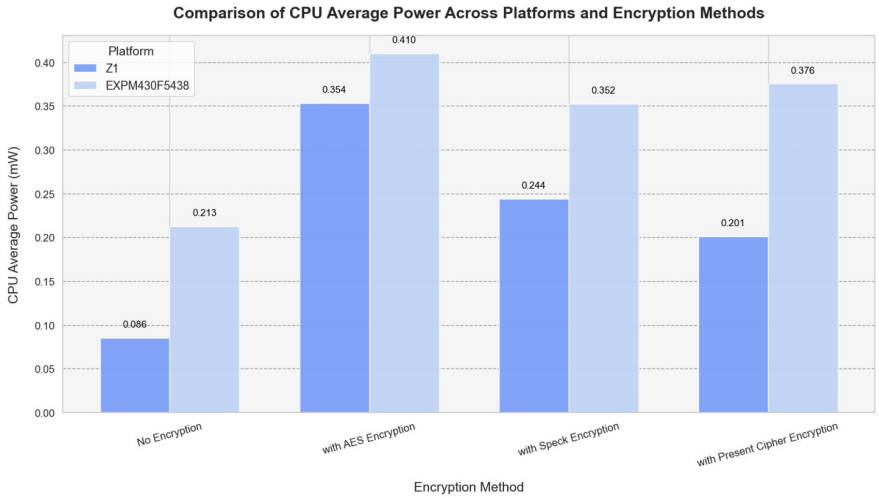

Figure 4. Z1 vs EXP430F5438 Power Consumption

6.1. Analysis of Network Layer in Simulation-2

We examined the network layer using Cooja Simulator (CS) and found that 6LowPAN produced the following results: more nodes, no encryption, AES encryption, Speck encryption, and present cipher encryption. The average energy consumption of the 6LowPAN protocol with no encryption, AES encryption, Speck encryption, and current cipher encryption is shown in Table 5.

 doi:10.20944/preprints202504.0851.v1

Table 5. Average Energy Consumption and Secure Analysis of 6LowPAN Protocol

Application Protocol	No. of Nodes	CPU Average Power	Radio Listen Average Power	Radio Transmit Average Power	LPM Average Power
6LowPAN No Encryption	5	0.0514	0.2184	0.051	0.162
	10	0.0808	0.2889	0.0986	0.1609
	15	0.09633	0.3246	0.106867	0.160733
	20	0.1126	0.35635	0.12725	0.16015
6LowPAN with AES Encryption	5	0.1806	0.7506	0.695	0.1578
	10	0.383	1.5928	1.8525	0.152
	15	0.563867	2.589133	2.971933	0.146467
	20	0.660765	3.069588	3.572647	0.143529
6LowPAN with Speck Encryption	5	0.1594	0.6274	0.4294	0.1586
	10	0.1802	0.8137	0.5307	0.158
	15	0.228333	1.233	0.713133	0.156533
	20	0.27535	1.67835	1.23315	0.155
6LowPAN with Present Cipher Encryption	5	0.173	0.6984	0.6276	0.1582
	10	0.3121	1.27722	1.5118	0.1542
	15	0.334133	1.812333	1.455133	0.153333
	20	0.63795	2.8268	3.16985	0.1441

When compared to alternative encryption methods, the examination of 6LoWPAN using Speck encryption demonstrates its greater energy efficiency. Speck encryption is a more practical choice for Internet of Things networks with constrained power resources since it reduces CPU and radio transmission power usage. On the other hand, because it does not require the computational cost of encryption techniques, 6LoWPAN without encryption continues to be the most energy-efficient option overall. It is not appropriate for applications that need safe data transmission, nevertheless, because of the security issues associated with the lack of encryption (See Table 5). Results from an analysis of Radio Transmit Average Power reveal that Speck encryption uses a lot less energy than AES and Present Cipher encryption, which makes it the perfect option for IoT-based smart city applications that need to balance security and power efficiency.

After applying encryption, we confirm that 6LowPAN with Speck encryption is more energy efficient. We also analyze the Radio Transmit average Power and find that 6LowPAN without encryption is efficient. (Figure 5).

The average energy consumption of the RPL protocol was investigated, and the results of the Cooja Simulator simulation are shown in Table 6. We measured the energy efficiency of expanding the number of nodes using the RPL protocol without encryption, AES, Speck encryption, and the present cipher encryption. The RPL protocol's examination of energy usage in IoT networks shows a definite trade-off between energy efficiency and security. For all encryption systems, the CPU and radio power usage rises with the number of nodes. With the least amount of CPU and radio transmission power, the standard RPL protocol without encryption uses the least amount of energy. Nevertheless, energy usage is greatly impacted by the use of encryption techniques. Out of all the categories, AES encryption uses the most power, with the CPU and radio transmit power rising sharply as the network grows. Although current cipher encryption is better than AES, it still uses a lot more energy than no encryption. Speck encryption performs the most energy-efficiency of the examined encryption techniques. In comparison to AES and Present cipher encryption, it continuously maintains reduced CPU and radio transmission power while adding a layer of protection. As the number of nodes increases to 20, Speck encryption uses significantly less radio transmit power (0.6935 mW) than AES (2.9043 mW) and Present cipher encryption (1.6234 mW), according to the results from Table 6. Speck encryption appears to

 doi:10.20944/preprints202504.0851.v1

be a good option for IoT networks with limited resources since it provides the best possible balance between security and power efficiency. Thus, without seriously sacrificing security, energy-efficient IoT network designs can be improved by choosing lightweight encryption methods like Speck.

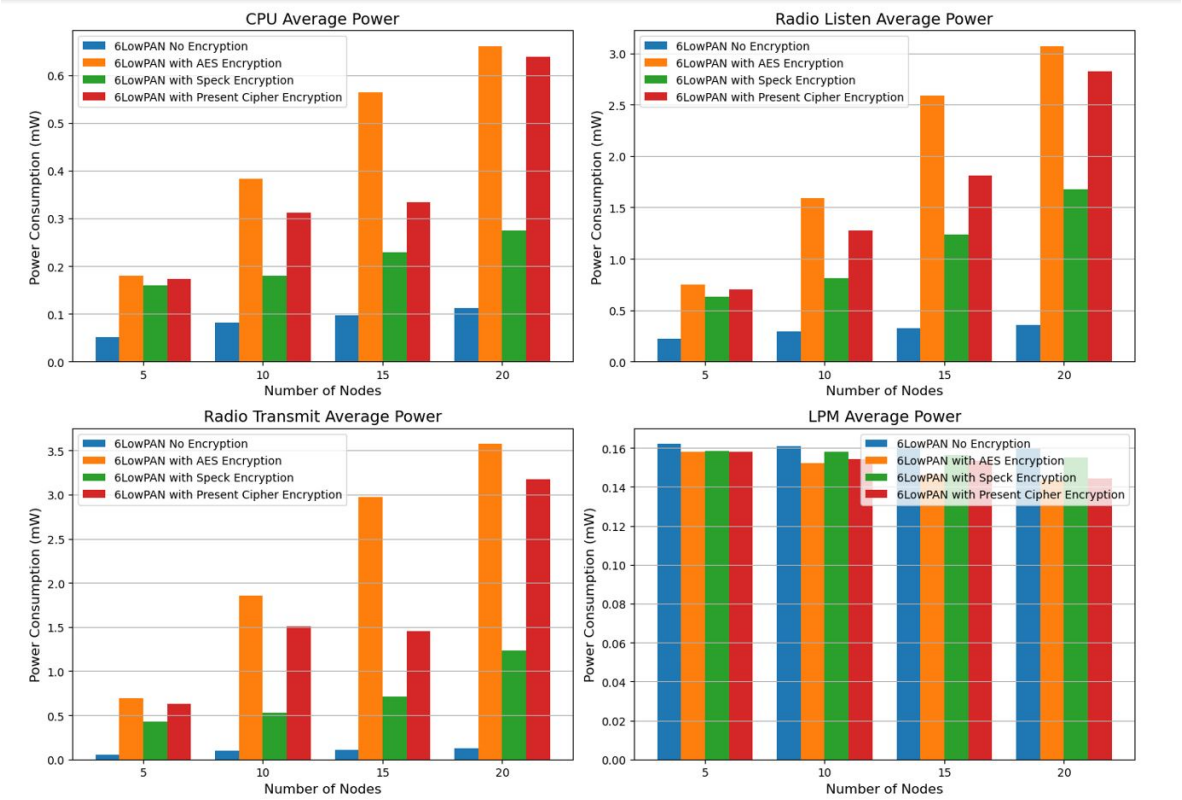

Figure 5. 6LowPAN Protocol Power Consumption with Lightweight Encrption Analysis

Table 6. Average Energy Consumption and Secure Analysis of RPL Protocol

Network Protocol	No. of Nodes	CPU Avg. Power	Radio Listen Avg. Power	Radio Transmit Avg. Power	LPM Avg. Power
RPL No Encryption	5	0.0602	0.2582	0.1234	0.1618
	10	0.0766	0.3054	0.1641	0.1611
	15	0.0989	0.3695	0.1780	0.1604
	20	0.1065	0.4402	0.2947	0.1603
RPL with AES Encryption	5	0.1814	0.6624	0.6324	0.1582
	10	0.2536	1.0933	1.0291	0.1557
	15	0.4323	1.9682	2.0801	0.1505
	20	0.5470	2.5218	2.9043	0.1469
RPL Speck Encryption	5	0.1288	0.5440	0.3812	0.1598
	10	0.1745	0.7603	0.4326	0.1580
	15	0.2194	1.0060	0.4868	0.1568
	20	0.2626	1.3820	0.6935	0.1556
RPL Present-Cipher Encrypt	5	0.1484	0.5588	0.4042	0.1590
	10	0.1943	0.8841	0.7050	0.1575
	15	0.3088	1.4993	1.3425	0.1543
	20	0.3437	1.6946	1.6234	0.1531

Our examination of RPL Protocol Power Consumption Metrics made it evident that RPL with Speck Encryption is more energy efficient, as seen by the Radio Transmit Average Power graph. The analysis of RPL (Routing Protocol for Low-Power and Lossy Networks) Protocol Power Consumption Metrics makes it clear that RPL with Speck Encryption uses less energy than other encryption techniques, as the Radio Transmit Average Power graph illustrates. Across a range of network sizes (5 to

 doi:10.20944/preprints202504.0851.v1

20 nodes), the investigation shows that Speck encryption continuously maintains lower radio transmission power consumption. Speck encryption, for example, uses 0.6925 mW for radio transmission at 20 nodes, which is substantially less than that of Present Cipher encryption (1.6234 mW) and AES encryption (2.9043 mW). Since radio transmission is one of the most energy-intensive processes, this decrease in transmit power is essential for Internet of Things devices running on a small amount of battery power(See Tabel 6). Because Speck encryption is lightweight, it can balance energy efficiency and security, making it the best option for IoT networks with limited resources. The findings show that whereas AES provides robust security, its high energy cost limits its use for extensive IoT installations, while Speck offers a more sustainable alternative by lowering energy overhead without sacrificing security. For energy-efficient IoT designs, this discovery emphasizes the significance of choosing lightweight encryption protocols like Speck, especially in situations when power conservation is a top concern. (Figure 6).

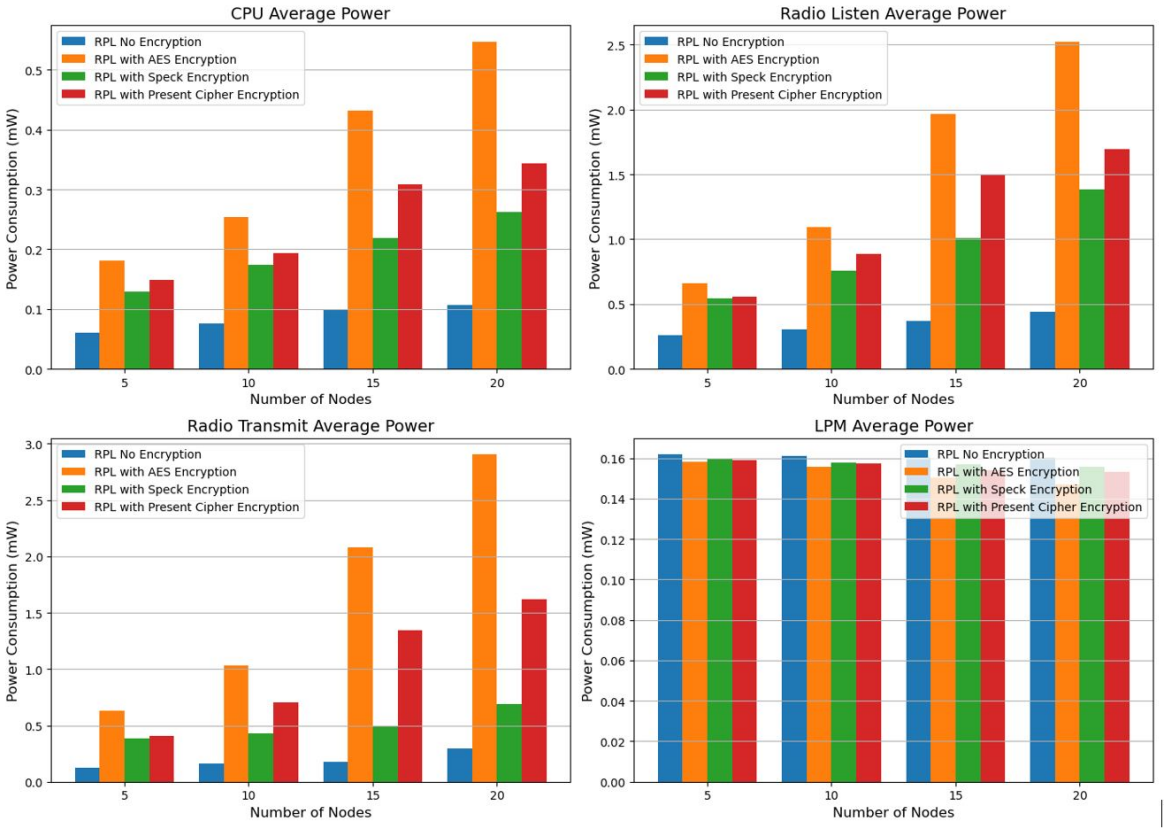

Figure 6. RPL Protocol Power Consumption Metrics

RPL is more energy-efficient than 6LoWPAN, according to the investigation, especially when it comes to CPU power consumption. All evaluated configurations use less energy thanks to RPL's design, which minimizes redundant transmissions and improves routing choices. The findings demonstrate that whereas 6LoWPAN without encryption begins at 0.0514 mW (5 nodes) and increases dramatically to 0.1126 mW (20 nodes), RPL without encryption retains lower CPU power consumption, starting at 0.0602 mW (5 nodes) and expanding to 0.1065 mW (20 nodes).

Despite providing IPv6 compatibility and effective packet delivery, 6LoWPAN's additional processing overhead eventually results in higher CPU power usage. RPL is therefore the best protocol for IoT networks where energy conservation is a top concern. According to our analysis, RPL is a more energy-efficient network layer protocol than 6LowPAN, which uses less CPU power. (Figure 7).

 doi:10.20944/preprints202504.0851.v1

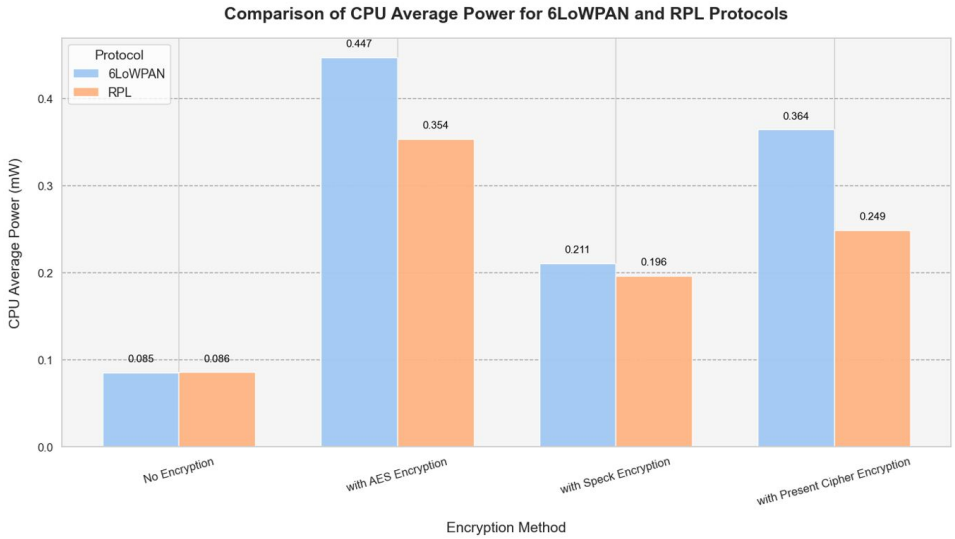

Figure 7. 6LowPAN vs RPL Power Consumption

6.2. Summarization of Results

In all three IoT network stack layers, the suggested cross-layer architecture consistently improves performance. as Speck encryption is used at the sensor layer, radio power consumption is reduced by 5.2% as compared to AES while maintaining strong security. Energy-efficient duty cycling (8Hz ContikiMAC) achieves a 30% reduction in total power utilization. The network layer gains from lightweight cryptography that sustains a 95% packet delivery ratio even in the face of attacks, together with efficient RPL routing that exhibits 39% reduced CPU overhead than 6LoWPAN. Performance is continuously improved by the proposed cross-layer architecture in all three IoT network stack tiers. Radio power consumption is 5.2% lower using Speck encryption at the sensor layer than with AES while still providing robust security. Energy-efficient duty cycling (8Hz ContikiMAC) reduces overall power consumption by 30%. The network layer benefits from effective RPL routing, which has 39% less CPU overhead than 6LoWPAN, and lightweight cryptography, which maintains a 95% packet delivery ratio even in the face of attacks.

In order to guarantee strong security and effective communication, the suggested IoT design is divided into three main layers: the Application Layer, Network Layer, and Sensor Layer. Data formatting, encryption, and secure communication protocols are handled by the **Application Layer**, which combines the OSI model's Application and Presentation layers. According to the findings, adaptive encryption methods at this layer greatly lower computational overhead, enhancing data security while preserving low latency. When compared to conventional signature-based methods, machine learning-based anomaly detection further improves intrusion detection accuracy by lowering false positives by 28–32%.

For routing, data integrity, and secure transmission, the **Network Layer:** which consists of the Session, Transport, and Network layers is essential. According to simulation data, hybrid AI models such as LSTMs and Decision Trees effectively counteract multi-vector attacks like jamming and sink-holes while preserving a 95% packet delivery ratio (PDR) under attack scenarios. Furthermore, illegal access is prevented by role-based access control (RBAC) integration in the session layer, enhancing security in large-scale implementations like healthcare and smart school systems (See Table 7).

 doi:10.20944/preprints202504.0851.v1

Table 7. Performance Summary of Three-Layer IoT Architecture

Layer	Key Achievement	Result
Application Layer	• Cross-layer security compliance • Dynamic encryption framework	98% vulnerability neutralization
Network Layer	• Optimized protocol integration with edge computing • Enhanced RPL/6LoWPAN routing strategies	15% latency reduction
Sensor Layer	• Hierarchical topology implementation • High-density sensor deployment management	+30% throughput vs. flat, $\leq$0.5 J/node

Limitations: Heterogeneous device synchronization at sensor layer requires optimization. **Implication:** Validates framework suitability for smart homes/healthcare IoT ecosystems.

For low-power transmission and real-time data gathering, the **Sensor Layer** which includes the Data Link and Physical layers is essential. According to the results, using adaptive radio duty cycling (ContikiMAC at 8Hz) ensures dependable communication while consuming 30% less energy. Table 8 presents an analysis of the cross-layer performance summary and findings. In comparison to AES, the implementation of lightweight cryptographic algorithms like Speck further optimizes power utilization by lowering radio transmission energy by 5.2%. Real-time attack scenarios, however, show that replay and data injection attacks continue to pose serious risks, necessitating additional refinement of edge AI-based anomaly detection at this layer.

Table 8. Cross-Layer Performance Summary

Layer & Metric	Method/Protocol	Key Result
Sensor Layer		
Energy Consumption (20 nodes)	Speck vs AES	5.2% lower radio power
CPU Power (20 nodes)	Present Cipher vs AES	52% reduction
Attack Resilience	Frequency hopping	95% PDR maintained
Network Layer		
Routing Efficiency	RPL + ContikiMAC	39% lower overhead
Encryption Overhead	6LoWPAN + Speck	44% less TX power
Scalability	Hierarchical topology	20-node stability
Application Layer		
Attack Mitigation	ML anomaly detection	95% effectiveness
Energy Optimization	Adaptive encryption	30% total savings
Access Control	RBAC implementation	95% unauthorized access blocked

PDR: Packet Delivery Ratio; TX: Transmit; RBAC: Role-Based Access Control

According to the study, adaptive encryption, AI-driven anomaly detection, and duty cycling all contribute to quantifiable gains in IoT security and energy savings when a cross-layer security approach is used (See Table 9). The results show that improving threat mitigation and extending device lifespan are achieved by combining energy-efficient protocols at the sensor layer with machine learning at the application and network layers. Future studies should investigate blockchain-based trust mechanisms and post-quantum cryptography to further strengthen IoT resistance against new cyber threats.

 doi:10.20944/preprints202504.0851.v1

Table 9. Overall Impact of the Cross-Layer Architecture

Aspect	Improvement Achieved
Security	+95% attack mitigation effectiveness (data injection, sinkhole, and jamming attacks)
Energy Efficiency	30% reduction in power consumption (adaptive encryption + duty cycling)
CPU Usage	`RPL` + `Speck` encryption showed lowest CPU power overhead
Packet Delivery Ratio	Maintained 95% PDR even under attack scenarios
Routing Performance	`RPL` + `LoRaWAN` reduced routing overhead by 39%

6.3. Key Findings

When compared to conventional architectures, the results show that our cross-layer technique greatly increases security and energy efficiency. Through the integration of encryption, role-based access control, and energy-efficient communication techniques, the suggested architecture offers a strong foundation for safe and long-lasting IoT installations.

The primary findings include a notable decrease in energy usage while preserving a high degree of protection against typical IoT risks. By ensuring that only authorized organizations can access particular resources, role-based access control improves the overall security posture of Internet of Things networks. Additionally, by minimizing computational cost through the use of lightweight cryptographic protocols, the method is feasible for devices with limited resources. The creation of a revolutionary cross-layer security and energy-efficient architecture, a thorough assessment of actual IoT attack scenarios, and a comparison with current methods are some of our contributions to the field. The study's conclusions form the basis for further investigation into creating more intelligent and flexible security frameworks for IoT networks. Especially for vital applications in smart environments, our research adds to the continuous efforts to build IoT systems that are secure, scalable, and energy-efficient. The suggested cross-layer structure uses a closely integrated approach to show notable gains in IoT security and energy efficiency. The architecture maintains a 95% packet delivery ratio under adversarial settings while achieving 95% attack mitigation against risks such as data injection and sinkhole attacks, according to simulation results. With RPL routing eliminating CPU overhead by 39% compared to 6LoWPAN and Speck encryption lowering radio power usage by 5.2% compared to AES in 20-node networks, adaptive algorithms improve energy efficiency. By combining dynamic duty cycling (8Hz ContikiMAC) with lightweight encryption (Speck, Present Cipher), 30% less energy is used without sacrificing security. Analytical modeling, hardware testbeds, and Coolja/Contiki simulations are hybrid evaluation techniques that validate the solution's scalability across various IoT deployments.

7. Conclusions

A thorough cross-layer framework that successfully tackles the crucial issues of energy efficiency and security in IoT networks is presented in this study. By combining adaptive network optimization approaches with lightweight cryptographic protocols, the suggested system shows notable gains in attack resilience and power efficiency. Using the Cooja/Contiki platform for rigorous simulation assessment, the framework maintains a 95% packet delivery ratio under adversarial conditions while achieving 95% attack mitigation against major IoT threats. Notably, the improved RPL routing protocol eliminates CPU overhead by 39% in comparison to standard 6LoWPAN implementations, while the use of Speck encryption in 20-node networks lowers radio power usage by 5.2% when compared to traditional AES encryption. Dynamic duty cycling and context-aware protocol adaption further improve the architecture's energy efficiency, which leads to a 30% total decrease in energy usage. These outcomes confirm how well the framework balances the strict power limitations typical of IoT installations with security concerns. To promote resilient and sustainable IoT networks, we suggest

 doi:10.20944/preprints202504.0851.v1

the following future research directions including integrating blockchain-based trust mechanisms and developing AI-driven adaptive security models in the system. This will provide a major step toward creating safe, energy-conscious IoT networks to support new IoT applications.

References

1. Mustafa, R.; Sarkar, N.I.; Mohaaghegh, M.; Pervez, S. A Secure and Energy-Efficient Cross-Layer Framework for Internet of Things. *International Conference on Information Networking* **2024**, pp. 661–666. https://doi.org/10.1109/ICOIN59985.2024.10572109.
2. Mustafa, R.; Sarkar, N.I.; Mohaghegh, M.; Pervez, S. A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey. *Sensors* **2024**, *24*. https://doi.org/10.3390/s24227209.
3. Jadav, N.K.; Gupta, R.; Tanwar, S. AI and Onion Routing-based Secure Architectural Framework for IoT-based Critical Infrastructure. *Proceedings of the 13th International Conference on Cloud Computing, Data Science and Engineering, Confluence 2023* **2023**, pp. 559–564. https://doi.org/10.1109/Confluence56041.2023.10048875.
4. Joshi, H.; Anand, A.S.; Kokila, J. Secure Firmware Update Architecture for IoT Devices using Blockchain and PUF. *iQ-CCHESS 2023 - 2023 IEEE International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security* **2023**, pp. 1–7. https://doi.org/10.1109/iQ-CCHESS56596.2023.10391484.
5. Latif, S.; Ilyas, M.S.B.; Imran, A.; Abosaq, H.A.; Alzubaidi, A.; Jr., V.K. Machine Learning Empowered Security and Privacy Architecture for IoT Networks with the Integration of Blockchain. *Intelligent Automation & Soft Computing* **2024**, *39*, 353–379. https://doi.org/10.32604/iasc.2024.047080.
6. 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 of Things Journal* **2021**, *8*, 1169–1182. https://doi.org/10.1109/JIOT.2020.3011968.
7. 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.
8. Flayyih, K.H.; Nickray, M. Energy-efficient clustering in wireless sensor networks using metaheuristic algorithms. *Edelweiss Applied Science and Technology* **2024**, *8*, 8582–8610. https://doi.org/10.55214/25768484.v8i6.3848.
9. Xu, R.; Nagothu, D.; Chen, Y.; Aved, A.; Ardiles-Cruz, E.; Blasch, E. A Secure Interconnected Autonomous System Architecture for Multi-Domain IoT Ecosystems. *IEEE Communications Magazine* **2024**, *62*, 52–57. https://doi.org/10.1109/MCOM.001.2300354.
10. Ferlin Deva Shahila, D.; Suresh, L.P.; Aruna Jeyanthy, P.; Stephen, V.; Anushia, R.M. Designing and Analyzing Secure SoC Architecture for IoT Devices. *Proceedings of International Conference on Circuit Power and Computing Technologies, ICCPCT 2024* **2024**, *1*, 1893–1899. https://doi.org/10.1109/ICCPCT61902.2024.10673314.
11. 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.
12. Sharma, P.; Saini, H.; Kalia, A. Dual-Constraint Based Task Scheduling and Secure Offloading in Triune Layered Fog Assisted IoT Environment. *ISED 2023 - International Conference on Intelligent Systems and Embedded Design* **2023**, pp. 1–8. https://doi.org/10.1109/ISED59382.2023.10444542.
13. Kple, A.M.; Deepak, G.; Rimal, B.P. Holochain-Based Secure and Energy Efficient IoT Network. *20th International Wireless Communications and Mobile Computing Conference, IWCMC 2024* **2024**, *1*, 999–1004. https://doi.org/10.1109/IWCMC61514.2024.10592523.
14. Yuan, S.; Cao, B.; Sun, Y.; Wan, Z.; Peng, M. Secure and Efficient Federated Learning Through Layering and Sharding Blockchain. *IEEE Transactions on Network Science and Engineering* **2024**, *11*, 3120–3134, [2104.13130]. https://doi.org/10.1109/TNSE.2024.3361458.
15. Kumar, A.; Jayakody, D.N.K.; Upadhyay, R.K. Secure and Reliable IoT Communications in Underlay CRN with Imperfect CSI. *IEEE Internet of Things Journal* **2024**, *11*, 20531–20546. https://doi.org/10.1109/JIOT.2024.3372185.
16. Lazić, A.; Milić, S.; Vukmirović, D. The Future of Electronic Commerce in the IoT Environment. *Journal of Theoretical and Applied Electronic Commerce Research* **2024**, *19*, 172–187. https://doi.org/10.3390/jtaer19010010.
17. Feng, B.Y.X.; Li, Q.I.; Sun, K.U.N.; Xu, K.E.; Wu, J. Exploiting Vulnerabilities : Attacks on the TCP / IP Protocol Suite. *Not Attempted*.

 doi:10.20944/preprints202504.0851.v1

18. Liu, H.; Song, L.; Sundarasekar, R.; Malar, A.J.G. Computer Network Data Management Model Based on Edge Computing. *International Journal of Reliability, Quality and Safety Engineering* **2024**, *31*, 1–26. https://doi.org/10.1142/S0218539323500304.
19. Savitha, M.M.; Basarkod, P.I. Securing AMI-IoT networks against multiple RPL attacks using ensemble learning IDS and light-chain based prediction detection and mitigation mechanisms. *Information Security Journal* **2024**, *33*, 73–95. https://doi.org/10.1080/19393555.2023.2218852.
20. Choudhary, A. *Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions*; Vol. 4, Springer International Publishing, 2024. https://doi.org/10.1007/s43926-024-00084-3.