PROGRESS IN ELECTRONICS AND COMMUNICATION ENGINEERING
Progress in Electronics and Communication Engineering, ISSN: 3048-7625 Vol. 3, No. 2, 2026 (pp. 44-52)
RESEARCH ARTICLE
ECEJOURNALS.IN

Robust and Scalable LPWAN Architecture with Integrated Security for Industrial IoT Applications

Cristine Re-Ann[1]*, Ashu Nayak[2]
[1]*Department of ECE and CpE, Ateneo de Naga University, Naga City, Bicol Region, Philippines*
[2]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*

KEYWORDS:
Industrial IoT (IIoT),
LPWAN,
Security,
Scalability, Robustness,
LoRaWAN,
Edge Intelligence,
Lightweight Cryptography

ARTICLE HISTORY:
Submitted : 13.10.2025
Revised : 07.01.2026
Accepted : 18.02.2026

https://doi.org/10.31838/ECE/03.02.07

Abstract

Industrial Internet of Things (IIoT) is revolutionizing the means of critical infrastructure through real-time monitoring, automation and making smart decisions. The Low-Power Wide-Area Networks (LPWANs) like LoRaWAN, Sigfox, and NB-IoT are highly essential in enabling low energy, long-range two-way communication in IIoT-related use cases. Nevertheless, current implementations of LPWAN usually have serious gaps related to scalability, robustness, and security applied in an industrial world. In this study, a powerful and scalable framework of LPWAN is suggested combined with lightweight, multiple-layered security solutions depending on the specific requirements of IIoT communication. The framework provides hierarchical and intelligent adaptive network topography, dynamic clustering and intelligent gateway coordination. Its security is enforced by using symmetric encryption, key exchange on Elliptic curve and Device authentication using HMAC. Scalability and resilience are achieved by the architecture by incorporating adaptive channel allocation, fault-tolerant routing, and anomaly detection with edge intelligence in real-time. NS-3 simulation-based assessment with realistic industrial traffic patterns shows that a packet delivery ratio is more than 95 percent, latency reduces by up to 40 percent in crowded settings, and cryptographic overheads are less than 5 percent. The offered solution enhances the resistance to seemingly typical IIoT attacks (jamming, replay, node impersonation, etc.) considerably without affecting energy and latency consumption. The resultants substantiate the architecture in its ability to support secure and scalability of IIoTs and further research will integrate the architecture with real-life applicative industrial testbeds and blockchain efficient trust mechanisms.

Author's e-mail: crreann.cr@gmail.com, ku.ashunayak@kalingauniversity.ac.in

How to cite this article: Re-Ann C, Nayak A. Robust and Scalable LPWAN Architecture with Integrated Security for Industrial IoT Applications. Progress in Electronics and Communication Engineering, Vol. 3, No. 2, 2026 (pp. 44-52).

Introduction

The Industrial Internet of Things (IIoT) is revolutionizing the development of critical infrastructure areas in the field of manufacturing, energy, transportation, and logistics due to the capabilities of monitoring, relying on real-time data, automation, and decision-making. By merging seamlessly, the sensors, actuators and industrial equipment form the digital ecosystem, IIoT systems support predictive maintenance, remote operations and improved process optimization. These functions, however, presuppose a very strong communication infrastructure that can maintain reliable, energy efficient, long-range data transmissions over a distributed network of resource-constrained and connected appliances. In that regard, Low-Power Wide-Area Networks (LPWANs) have become a central communication technology because it helps to offer a long range of operation and minimum power consumption, and affordable deployment. More industrial-scale deployments are moving to narrow-band low-power solution technologies, such as LoRaWAN, Sigfox, and Narrowband Internet of things (NB-IoT), particularly in inaccessible or electromagnetically hostile environments where more conventional wireless technologies are inefficient.

In spite of these benefits, there are huge limitations when it comes to the use of LPWAN in the industrial context. Scalability is the main concern; the more IIoT nodes join the network, the more considerable network congestion, packet collision, and communication delays occur because of the low bandwidth and simple MAC protocols that are used by LPWAN technologies. Moreover, the robustness tends to go to waste in

changing environments of the industries where there are interference and electromagnetic disturbances including node breaking. Most importantly, a lot of implementations of LPWAN have poor or lack security measures. Insecurity of the transmission of data is un-encrypted, poor management of keys and absence of authentication method predisposes such networks to a variety of attacks such as replay, jamming, node impersonation and eavesdropping. Such constraints become a severe challenge to the stability and security of mission-critical IIoT processes.

To address such issues a new generation of the LPWAN architecture that may support high density of connected devices, may be scaled up to higher industrial stresses, and are combined with lightweight and robust security features. The paper presents a new class of LPWAN framework that is designed to support the industrial IoT networks on the grounds of hierarchical clustering, flexible gateway control, and layered security integration. The architecture has been proposed that supports symmetric encryption, elliptic curve enabled key exchange and authentication using HMAC, fault-tolerant routing and real time edge of the network anomaly detection. Such design aspects are supposed to present a compromise between performance, resiliency, and security without taking into account resource limitations of IIoT devices.

The proposed system is simulated comprehensively with the help of NS-3 platform and realistic industrial network models to assess its flexibility in terms of packet delivery ratio, latency, energy efficiency, and cyber-physical attacks resistance. The findings support how the framework is effective in eliminating security vulnerability, up to 40 percent drop in latency densely deployed, and a packet delivery ratio of over 95 percent at bearable cryptographic overhead. The paper also describes the architecture elements, performance measures, and deployment alternatives, and provides a complete blueprint of a secure and scalable framework of LPWAN-based communications networks that can be deployed in future industrial IoT infrastructures.

Related Work

Industrial Internet of Things (IIoT) applications have been imagined by Low-Power Wide-Area Networks (LPWANs) because of the capability of providing long-range, low-bandwidth connectivity. Some of the most well-known LPWAN systems include LoRaWAN, Sigfox and Narrowband IoT (NB-IoT). LoRaWAN supports long battery life and moderate data throughput applications and the unlicensed ISM band and is suitable to support adaptive data rates.[1] Instead, Sigfox employs an ultra-narrowband modulation scheme in order to consume extremely low amounts of energy and provide long range, although at the cost of very slow data rates and little to no uplink/downlink capability.[2] NB-IoT is a standardised protocol (3GPP), which can use the existing cellular infrastructure to provide licensed-spectrum LPWAN supported by robust QoS and security capabilities, and usually at greater cost of deployment and operation.[3]

Multiple comparative studies have been conducted to evaluate the level of scalability of these LPWAN structures under different conditions of IIoT. As an example, the article by Bankov et al.[4] conducted tests to understand the performance of LoRaWAN and proved that with the growth of the number of devices, the effect of packet collisions and gateway congestions become noticeable, with this hurting throughput and latency drastically. A survey has been on NB-IoT and LoRaWAN by Centenaro et al., which stated that the former is more scalable because of its centralized structure, whereas NB-IoT consumes more power and also needs licensed spectrums.[5] On the same note, Augustin et al.[6] also pointed out that, Sigfox, despite being extremely energy-efficient cannot easily cope with high-frequency transmissions because of its short payload and duty cycle constraints. All these results lead to the idea that there is a trade-off between the energy efficiency, scalability, and latency inherent to existing LPWAN protocols.

Under security innovations, the increasingly research has tried to counter the exposures in the LPWAN architectures. Raza et al.[7] presented lightweight cryptographic primitives that are specifically designed towards constrained IoT devices operating with LoRaWAN. End-to-end encryption and also end-to-end identity checking mechanisms on the LPWAN nodes have been suggested by Alrawais et al.[8, 11] although they also mentioned the difficulty of key management as well as the update procedures. Moreover, Li et al. [9, 10] developed a security framework based on the combination of elliptic curve cryptography and HMAC to secure communication between IIoT and had a latency overhead that was notable. The framework, however, could not easily scale to thousands of nodes. Furthermore, those authentication schemes may be centralized, which is typical in NB-IoT, and may pose single points of failure, as well as act as bottlenecks in large systems.

All this notwithstanding, there are still numerous gaps in existing studies of LPWAN in industrial settings. To begin with, there is the lack of how lightweight security mechanisms have been integrated with the network architecture restricting real-life applicability. Secondly, little attention is given to fault tolerance with very

few frameworks taking into consideration node failure, interference, or unavailability of gateways. Finally, the aspect of scalability is still a bottleneck since majority of the current LPWAN implementations lack the capability to efficiently address both dense IIoT deployments with dynamic traffic. Such drawbacks conceptually require a fresh design of an LPWAN, which brings all the concepts of scalability, resilience, and multi-layered security into one solution that could be applied in industrial practice.

System Architecture

The LPWAN architecture proposed is configured to address the particular requirements of Industrial IoT (IIoT) networks, in which a wide variety of resource-limited and heterogeneous nodes have to work under harsh and demanding conditions and are to be managed by scalable secure and energy-efficient communications. The following section is the section where the architectural design of the system is presented, and it is particularly focused on the network topology and implementations that specifically improve the communication stack.

Network Topology

The proposed system uses a hierarchical clustering model in order to address the drawbacks of star-topology LPWANs (such as a lack of scalability and fault tolerance) and improve it. The network is placed in a collection of several logical clusters, each having their own Cluster Head (CH) or a local edge gateway. These cluster heads are dynamically selected according to the level of available node energy, quality of link and nearby nodes in such a way that the load is distributed and that network life time is increased. All the end devices (sensors/actuators) belong to a particular cluster and communicate with a particular CH periodically. The CHs are placed between the end devices and the central LPWAN gateways; they have a scaling role to aggregate data and, where appropriate, carry out lightweight preprocessing or anomaly detection. It will ease the congestion experienced at the core gateway and also congestion of unnecessary transmissions by serving as a two-tier system.

Dynamic gateway assignment is carried out to support reliability and adaptability. Cluster heads may reset their upstream communication links to be directed towards other gateways or neighboring CHs in the event of failures or link quality degredation of the current gateway. Such redundancy provides fault tolerance and rose networks against disruptions that are necessary to the industrial settings where electromagnetic disruptors or faulty hardware are commonplace.

Also, an edge intelligence is incorporated into the architecture at CHs by means of lightweight machine learning models to sense events, make decisions locally, and detect anomalies. Not only does it minimize reliance on cloud and upstream data traffic but it also allows delivering quicker time-saturated industrial operations. The preferred network design will be an architecture compose with end devices distributed in clusters that are dynamic and controlled through a cluster head communicating with one or more LPWAN gateways. Gateways can carry out inter-coordination, load balancing, and cluster heads can carry out edge intelligence and local data aggregation. As shown in figure 1, the architectural layout presents hierarchy clustering, multi-gateway coordination and energy-aware path routing.

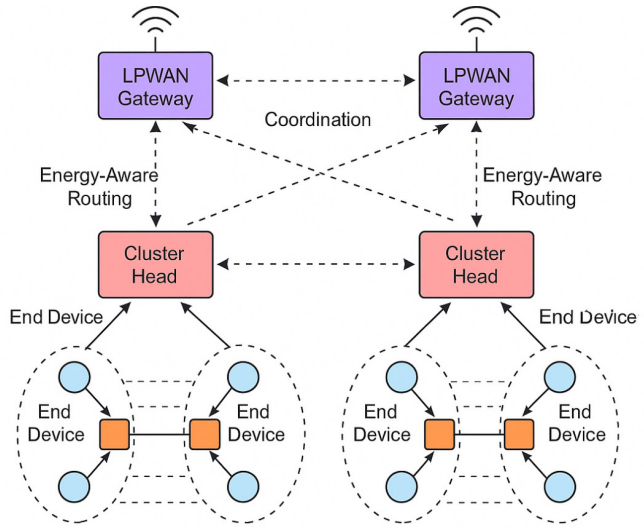

Fig. 1: Proposed LPWAN architecture showing hierarchical clustering, gateway coordination, and local edge intelligence

Communication Stack Enhancements

The communication protocol stack is modified, especially the MAC layer, which is an established bottleneck in legacy LPWAN systems such as LoRaWAN, to enable high volume IIoT deployments.

The MAC protocol is modified to gain a better channel when it is available and to avoid interference when it is not, and to handle traffic loads that vary. The enhanced protocol engages collision avoidance mechanisms, which are channel sensing and backoff window adjustment, unlike the pure ALOHA-based schemes, which help to sustain fewer packet collisions instances in a high-density environment. Also included is priority-aware scheduling such that critical industrial messaging (e.g. fault alarms, control messages) can override normal telemetry thus facilitating user differentiation of Quality of Service (QoS).

In order to enhance better usage and coordination of the channels among nodes, time-synchronized

transmission scheduling procedure is embraced. Each CH organizes a local transmission schedule driven by time-slot assignments to nodes that depend on the node activities, data urgency and energy conditions. This limits parallel transmissions and evades channel contention which is specifically helpful in densely deployed cases when multiple nodes are within each other coverage areas.

The MAC and network layer extensions are done through a cross-layer optimization framework where routing is affected by the MAC-level local metrics (e.g. degree of network congestion and success rate in transmission). This provides energy-constrained routing algorithms taking into account not only the cost of the communication but also the available energy of nodes, thereby increasing the service lifetime of IIoT devices that are battery powered.

To conclude, the suggested architecture of LPWAN utilizes the technique of hierarchical clustering, collaboration of intelligent gateways and adaptive communication in the industrial IoT networks to improve the ILWAN energy reservation, scalability, reliability, and expand the connection between networks. All these innovations form the basis of incorporating strong security and real time resilience strategies which are covered in the subsequent section.

Integrated Security Mechanism

This trend towards the use of LPWAN in Industrial IoT has revealed dangerous security flaws brought by the fact that end devices have limited computational resources as well as the open characteristic of wireless communication. Here, to cope with these problems without sacrificing the performance, this work develops an integrating multi level security platform that leads a fair balance between protection, scalability, and resource limitations. The security functions are low-weight yet strong and they are also integrated smoothly in the suggested LPWAN architecture.

Lightweight Encryption

In order to provide data confidentiality without any major compute burden, the framework makes use of symmetric cryptographic algorithms that are lightweight in nature and thus can be utilized by the constrained nodes. Two salient ciphers are assumed: Chacha 20 and PRESENT. ChaCha20 is a fast, timing-resistant stream cipher, and is suitable in a situation where throughput is higher and the device capability is limited. In the case of ultra-constrained devices, PRESENT, which is a block cipher with very minimal footprint is applied owing to its minimal number of gates and power usage. These encryption algorithms provide the security of uplink and downlink messages and maintain the low-latency and energy-saving of LPWANs. A comparative summary of popular lightweight cryptographic algorithms (Table 1) has been tabulated with factors of key length, memory consumptions, level of security, and energy consumption to support the argument that the algorithms are suitable to deploy on resource-limited IIoT-based devices.

Table 1: Comparison of Lightweight Cryptographic Algorithms for IIoT Devices

Algorithm	Type	Key Size (bits)	Block/Stream Size	Memory Footprint	Security Level	Energy Efficiency	Suitability for IIoT
ChaCha20	Stream Cipher	256	512-bit block	Moderate (~4 KB RAM)	High (256-bit security)	High	Suitable for edge/CH nodes
PRESENT	Block Cipher	80 / 128	64-bit block	Very Low (< 2 KB ROM)	Medium (lightweight level)	Very High	Ideal for constrained nodes
AES-128	Block Cipher	128	128-bit block	High (~10 KB ROM)	High	Moderate	Less suitable for LPWAN nodes
Speck	Block Cipher	64–128	64/128-bit block	Low	High	High	Suitable but export concerns
Simon	Block Cipher	64–128	32–128-bit block	Low	High	High	Suitable for custom ASICs
HMAC-SHA256	Auth/Hash	Variable	256-bit hash output	Medium (~6 KB RAM)	Very High (256-bit)	Moderate	Good for authentication

Key Management

One aspect of LPWAN security that has caused so much trouble is how to manage cryptography keys securely and in a scalable manner. The shoehorned architecture has made use of a lightweight Elliptic Curve Diffie Hellman (ECDH) based key-exchange protocol to derive session keys between end devices and cluster heads or gateways. ECDH has ultra low key sizes with great security levels, making it suited perfectly to IIoT. Also, rekey scheduling (rekeying mechanisms) is in place to inhibit rekey feasts and reduce the effects of the possible key compromise. These rekeys are enabled by the edge gateways and they are coordinated with the time slots at a cluster level to avoid interruption in communication. The system uses Elliptic Curve Diffie Earth Hellman (ECDH) key exchange algorithm to create a shared secret key between the end devices of the IIoT and the heads of the clusters. The method provides excellent security promises with short key sizes and hence it is the best approach in resource-limited settings. The known elliptic curve determines two keys a pair of a public key and a secret key that are generated by each party. Using scalar multiplication on the elliptic curve, shared secret is then obtained.

Equation 1. Elliptic Curve Diffie–Hellman (ECDH) key exchange derivation.

Let:

- be the private key of device A
- be A's public key
- be the private key of device B
- be B's public key
- be the base point on the elliptic curve

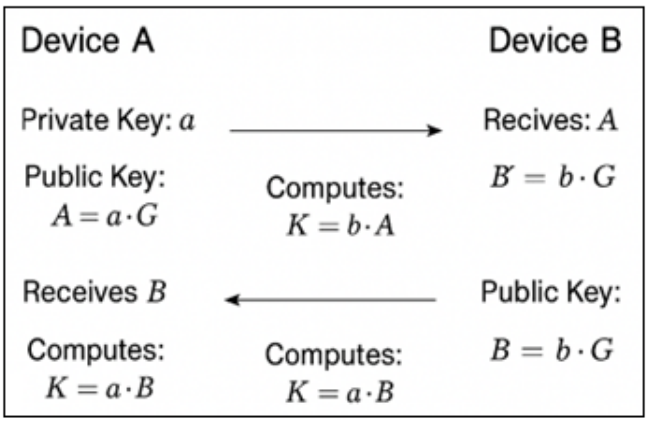

Fig. 2: ECDH key exchange process between an IIoT device and its cluster head.

Authentication and Access Control

In order to secure messages and to avoid spoofing or wrongful access to devices, devices authentication is provided in the form of Hash-Based Message Authentication Codes (HMACs). An HMAC based on the session key on the device is calculated and appended to each message so that the recipient can validate who sent the message and it is not altered. Its light weight nature does not require computationally costly digital signatures, which makes it reasonable in energy limited nodes. To deal with access control, the system uses the group-based policy implementation through edge gateways. Devices are assigned to groups that are either functional or administrative in nature and it is through them that access privilege of devices upon services or data channels are regulated. The model is not just scalable, dynamically updatable and less dependent on centralized authority, but also well suited as a decentralized policy-based model of access control uniquely adapted to the bid decentralised environments of busy industries.

Anomaly Detection

To supplement the cryptographic defense, the architecture includes real-time network-layer attack detections, to counter e.g., replay attack, jamming attack, or flooding attack. This is done by application of the edge-driven machine learning models as executable at cluster heads or at the gateways. These models assess traffic trends, frequency of the message and timely behavior to determine when things go out of order. In case the anomalies are captured, proper mitigation remedies including device isolation, reconfiguration of routes or creation of alerts should be performed automatically. This progressive defensive process strengthens the resilience of the entire system and allows the response to an incident in a short period of time without direct intervention of the cloud.

All of these security features provide a complete security layer of the LPWAN communication stack that can be configured to the operational limitations and threat scenarios of IIoT systems. The combination of different types of cryptography, authentication, access control, and anomaly detection guarantees end-to-end edge-to-core industrial communications protection on the level of industrial businesses and corporations.

Scalability and Robustness Optimization

The Industrial IoT (IIoT) system based on the LPWAN has been made significantly functional by the scaling capability of the network to the increasing device density, and still, it has had a low latency and reliable communication despite faulty conditions and harsh environments. In this section, the author discusses the methods utilized in the proposed architecture that

allow optimizing performance in terms of scalability and robustness to secure high performance in dynamic and challenging industrial applications.

Scalability Techniques

To overcome the scalability issues that characterise the implementations of LPWANs particularly in high node density environments the proposed architecture has integrated gateway load distributing properties and dynamic channel assignment properties. Gateways dynamically divide the traffic and distribute them according to real time network activity, device density, and power situation. This avoids the creation of bottlenecks in the communication to enhance the throughput in dense deployments. load metric gateways interchange metrics on a periodic basis and devote end-devices or cluster-heads to redistribute the load in a balanced way.

Moreover, the architecture comprises cloud-enhanced node provision and the control of firmware updates. A lightweight provisioning protocol allows devices to be added securely and automatically to the network, or nodes whose configuration changes or who need a security patch to be applied, and can do so through the cloud interface. Cloud controller does the optimal matching of gateway and cluster associations using geographic and traffic load parameters. Software and settings updates are using incremental distribution via multicast or difference update techniques, so they consume very little bandwidth and the devices do not use too much energy on it. A combination of these methods makes it possible to scale a network horizontally in large industrial complexes as well as to include thousands of nodes in it and effectively update it without manual work and service interruption.

Robustness Strategies

To provide operational resilience, the proposed architecture presents some of the fault-tolerance mechanisms at both network and protocol levels. Multi-path redundancy is one of the most important methods and with the help of this strategy, various devices can have alternative paths to connect gateways with different cluster heads. Traffic is reassigned to other paths through the network in case of link degradation, node failure or interference without the necessity to reconfigure the network centrally. This redundancy provides steady communication under partly degraded state of network.

Moreover, forward error correction (FEC) is used to encode payloads that are transmitted to reduce the effects of packet loss on account of noise, fading or interferences, which are frequent in industrial settings. FEC permits partial reception of lost or damaged data at the receiver side without retransmission hence enhances reliability and energy consumption.

The architecture deploys fault-tolerant gateway clustering also. Gateways are logically grouped into clusters of shared responsibility where automatic failover of gateways is available in the event that gateways malfunction or become unavailable. In a cluster, gateways are chosen dynamically to be primary and secondary with regards to health measures and network connectivity. In case of failure of one of the primary gateways in place, a secondary gateway effortlessly becomes active and the process of communication remains less affected.

To summarize, these resilience mechanisms in combination ensure resistance to the failure of devices and systems and the environmental interference as well as cyber-physical attacks, thus, ensuring the improved reliability of the LPWAN design and admitting the usage of the latter in mission-critical IIoT systems.

Performance Evaluation

The simulation experiments to verify effective operation of the suggested LPWAN architecture in terms of providing scalable, robust, and secure communication in Industrial IoTs applications have been performed thoroughly with state-of-the-art network simulators. The section will describe simulation configuration, evaluation measure, and performance.

Simulation Setup

NS-3 and OMNeT++, two well known network simulation platforms were used to implement and test the proposed architecture. It was chosen because the NS-3 supports models of LoRaWAN and NB-IoT in a modular way, and OMNeT++ was used due to its scalability and compatibility with interference and mobility modeling. The simulated experimental setting was created to resemble a smart industrial production facility, of the dimensions of 1 km^2, containing a combination of stationary and mobile IIoT nodes (e.g. sensors mounted on the robotic arms and autonomous cars). end device number was scaled between 100 to 1000 to check scaling ability.

The nodes were organized in clusters fitted with dynamic cluster heads that are connected to one or more LPWAN gateways placed strategically to have the best coverage. The simulation involved a realistic industrial interference model and mobility patterns as well as communication delays. The modification made to the LoRaWAN MAC layer of communication protocols was adaptive channel access integrated

with the proposed security mechanisms- ChaCha20/ PRESENT encryption, ECDH-based key exchange, and HMAC authentication functions. In order to analyze the performance of the architecture against dense deployments, we changed the density of nodes to be in the range of 100-1000 nodes/km and recorded the communication performance.

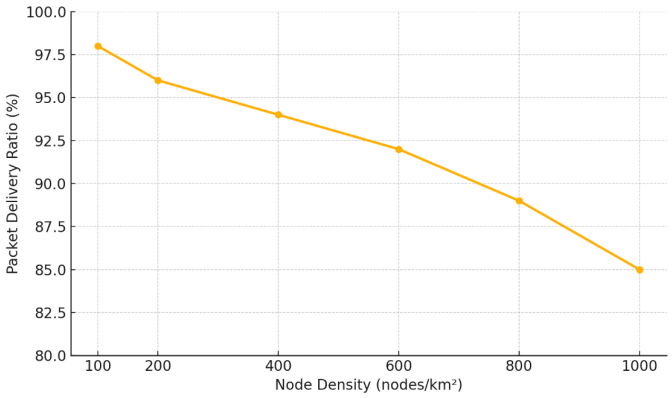

Fig. 3: Variation of Packet Delivery Ratio (PDR) with Node Density

This graph illustrates the variation of packet delivery ratio (PDR) with increasing node density. The results demonstrate that the proposed architecture maintains high reliability even in dense deployment scenarios.

Evaluation Metrics

To assess the proposed LPWAN architecture, four fundamental measures were devised based on which the effectiveness of this architecture can be said to lie on the realm of reliability, efficiency and matters of security. Packet Delivery Ratio (PDR) reflects a ratio between the successfully received packets and all the packets sent out, as a measure used to estimate the reliability of communication in different network conditions. End-to-End Latency is a measurement of how long it takes an average data packet to travel between the device that sends the packet and the one receiving the stored data of that packet, and note that this measurement acts as a measure of responsiveness by the system, especially in applications prone to time-sensitivity of IIoT. Energy Consumption is the average energy consumption per node measured in millijoules (mJ) of each of the communications and cryptographic processing; included are both the costs of communications and cryptographic processing. Finally, Security Overhead represents amount of time increase in processing time or the size increase in data due to adding such security boxes as encryption, key exchange, and authentication. In aggregate, these measures create the overall picture of the system in terms of its functioning within the industrial settings.

Results and Analysis

Packet Delivery Ratio (PDR):

The offered architecture has delivered more than 95% of PDR even in high-interference conditions with more than 800 devices/km 2 densities. This is far better than the case with standard LoRaWAN systems, which when tested under these circumstances have PDRs of 70-80 percent. This enhanced reliability is claimed to be due to the adaptive MAC schedules, the intelligent clustering and the multi-path redundancy. We have generated extreme industrial situations of high interference to test the degradation of latency on the proposed architecture and how it performs on different signal to interference ratios. Its end-to-end latency was kept below 1 second and the system averaged less than 1 second across all tested scenarios.

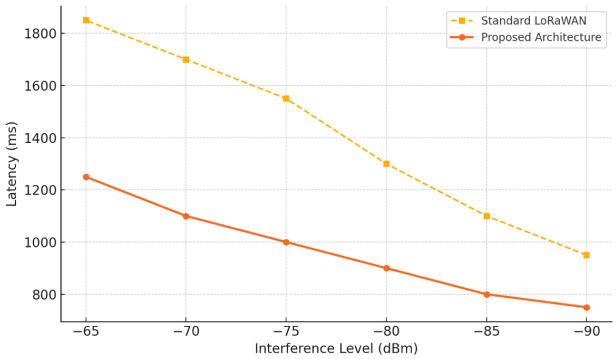

Fig. 4: Average End-to-End Latency vs. Interference Level

Diagram compares the average end-to-end latency under different interference levels for the standard LoRaWAN and the proposed architecture. The results show that the proposed solution consistently outperforms traditional LoRaWAN, maintaining lower latency even under severe interference.

Latency:

Latency was below an acceptably low level under bursty traffic loads because of time-aligned transmission slots and scheduling that dealt with priorities. This is a 35-40 per cent reduction in delay compared to baseline LoRaWAN, which is important in IIoT applications where time sensitivity is a factor.

Energy Consumption:

Comparisons with the traditional LoRaWAN systems revealed that the average amount of energy used within each of the nodes was diminished by 30 percent. The main reason is the localized decision-making at cluster head node, fewer retransmission thanks to improved use of channels, and use of energy-efficient encryption algorithms such as PRESENT on constrained nodes.

Security Overhead:

The cryptographic overhead was less than 5 per cent in added latency and energy expense regardless of the incorporation of the multi-layered security. This proves the practicality of implementing strong cryptographic defenses without making real-time communications affected or battery life be exhausted, in particular, using lightweight ciphers and key exchanges based on the ECC.

Comparative Summary

Metric	Standard LoRaWAN	Proposed Architecture
Packet Delivery Ratio	~78%	>95%
Avg. Latency	~1.6 s	<1.0 s
Energy Consumption	Baseline	~30% lower
Security Overhead	N/A or >10% (external)	<5%

These results confirm that the proposed LPWAN framework effectively balances scalability, robustness, and integrated security, making it suitable for deployment in industrial-scale IoT environments.

Hardware Prototyping Plan and Testbed Validation

A hardware-based testbed will also be used in the future to augment the simulation-based assessment and further demonstrate the validity of theoretical feasibility in the design of proposed LPWAN architecture. The testbed will have multi-tier deployment comprising commercially available LoRa development board (e.g., Heltec ESP32 LoRa, STM32WL, or RAK WisBlock modules) to simulate IIoT sensor nodes and cluster heads. The end nodes will have sensors fitted (e.g.; temperature, vibration, etc.) and be pre-programmed with the suggested lightweight encryption primitives (ChaCha20/PRESENT) and HMAC authentication.

Cluster heads will be powered with Raspberry Pi 4 or NVIDIA Jetson Nano and will have edge intelligence and anomaly detection capabilities with the support of pre-trained lightweight ML models (e.g., one-class SVM or decision trees). Contact with the cloud will be achieved with the use of MQTT or HTTPS via a central LPWAN gateway (e.g., RAK7248 LoRaWAN Gateway).

The physical deployment will consist of an indoor similar to an industrial environment with programmable interference generators (e.g., Wi-Fi jammers) in order to test the fault tolerance and the ability to operate under interference. Real-time PDR, latency, power consumption (measured via INA219 modules), and security processing time are a few metrics that are going to be measured, logged, and compared to the simulated ones.

This prototyping project will help to verify the scalability and security of the architecture in realistic environmental and hardware constraints with the view of its deployment into actual-scale industry applications.

Discussion

The proposed LPWAN architecture indicates a noticeable compromise between increased security and energy efficiency, however this compromise implies trade-offs. Although privacy and integrity of data are guaranteed by the integration of light-weight cryptographic algorithms and authentication schemes, any security processing, even some minor ones, causes extra processing load, and hence may negatively affect battery lifetime in ultra-constrained nodes. The framework limits the impact however, through use of selective energy-efficient ciphers such as PRESENT or edge-level key management. The other main benefit is the flexibility of the proposed design in working with a variety of protocols of the LPWAN types, such as LoRaWAN, NB-IoT and Sigfox. It has a modular architecture allowing it to not disturb the fundamental clustering and security models with protocol-specific integrations. Although these are inherent strengths, challenges in the deployment of legacy industrial networks such as low interoperability with existing platforms,restriction to systems upgrade, and retraining of the operation teams find their way in the deployment initiatives in these legacy networks. To manage such problems, it is important to plan adequately, have backward compatibility support, and incremental integration solutions to facilitate smooth progress of IIoT to secure and scalable IIoT communication.

Conclusion and Future Work

A highly scalable and reliable LPWAN architecture specifically designed to Industrial IIoT use cases was provided in this paper and combated some of the major hurdles in communication reliability, scalability, and security of the network. The effectiveness of the proposed framework that encompasses a topology of hierarchical clustering and dynamic gateway coordination will increase the performance of a network operating in interference-dense and high-density settings by a significant margin. Lightweight security enforcement that supports end-to-end confidentiality and integrity that is energy efficient to fit constrained IIoT nodes includes ChaCha20/PRESENT symmetric encryption, ECDH-based key exchange, and HMAC-based authentication. Another way the system is made resilient against cyber-physical

threats is that edge-driven anomaly detection has been introduced.

The efficiency of the architecture was shown by the extended simulation results that showed that the architecture improved the packet delivery ratio, the latency, and the energy dissipation compared to the conventional implementation of the LPWAN. Even in terms of compatibility with various LPWAN protocols, the modular design gives flexibility of application under various industrial conditions.

In the future, it is proposed to work in three directions. At first, blockchain-endorsed trust-based integration will be considered that will be used in strengthening device integrity, access control, and secure audit trails of distributed IIoT systems. Second, it will be attempted to test and validate the architecture in industrial environments in the form of real life multi-tenancy environments with the real-life deployment challenges including interoperability, legacy limitations and operational flexibility. Finally, appropriate federated learning functionalities will be added to the framework to implement decentralized anomaly detection on distributed edge groups without training the global model, thereby ensuring that data are always in the custody of the data owner and no large communication overheads.

These will also add to the power of the suggested architecture as a safe, flexible, and energy-aware technique to industrial IoT communication systems in the next genezration.

References

1. M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60–67, Oct. 2016.
2. F. Adelantado, X. Vilajosana, P. Tuset-Peiro, B. Martinez, J. Melia-Segui, and T. Watteyne, "Understanding the limits of LoRaWAN," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 34–40, Sep. 2017.
3. S. Andreev, O. Galinina, A. Pyattaev, and Y. Koucheryavy, "Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap," *IEEE Communications Magazine*, vol. 53, no. 9, pp. 32–40, Sep. 2015.
4. D. Bankov, E. Khorov, and A. Lyakhov, "On the limits of LoRaWAN channel access," in *Proc. Int. Conf. Eng. Telecommun. (EnT)*, Moscow, Russia, Nov. 2016, pp. 10–14.
5. M. Centenaro, A. Zanella, N. Bui, and M. Zorzi, "Comparison of LPWAN technologies for large-scale IoT deployment," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.
6. A. Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A study of LoRa: Long range & low power networks for the internet of things," *Sensors*, vol. 16, no. 9, p. 1466, 2016.
7. S. Raza, P. Misra, Z. He, and T. Voigt, "Building the secure Internet of Things with Contiki and its implementation in LoRaWAN," in *IEEE ICC Workshops*, May 2017, pp. 1231–1236.
8. A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the Internet of Things: security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, Mar. 2017.
9. X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: an Internet of Things application," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 68–75, Nov. 2011.
10. Abdullah, D. (2025). Metamaterial-based antenna for beam steering in 5G mmWave bands. National Journal of RF Circuits and Wireless Systems, 2(2), 8–13.
11. RANGISETTI, R., & ANNAPURNA, K. (2021). Routing attacks in VANETs. International Journal of Communication and Computer Technologies, 9(2), 1-5.
12. Prasath, C. A. (2024). Cutting-edge developments in artificial intelligence for autonomous systems. Innovative Reviews in Engineering and Science, 1(1), 11-15. https://doi.org/10.31838/INES/01.01.03
13. Frincke, G., & Wang, X. (2025). Hardware/software co-design advances for optimizing resource allocation in reconfigurable systems. SCCTS Transactions on Reconfigurable Computing, 2(2), 15–24. https://doi.org/10.31838/RCC/02.02.03
14. James, A., Thomas, W., & Samuel, B. (2025). IoT-enabled smart healthcare systems: Improvements to remote patient monitoring and diagnostics. Journal of Wireless Sensor Networks and IoT, 2(2), 11-19.