RESEARCH ARTICLE ECEJOURNALS.IN

Lightweight Authentication Protocols for Secure Embedded Communication in LPWAN

Kagaba J. Bosco[1]*, Q. Hugha[2]

[1]Information and Communications Technology, National Institute of Statistics of Rwanda, Kigali, Rwanda

[2]Robotics and Automation Laboratory Universidad Privada Boliviana Cochabamba, Bolivia

Keywords:

LPWAN,
Lightweight Authentication,
LoRaWAN,
Secure Embedded Communication,
ECC,
IoT Security,
Low-Power Devices

Author's Email:

Bosco.je.kag@nur.ac.rw

https://doi.org/10.31838/ESA/03.01.07

Received : 08.07.2025

Revised : 17.09.2025

Accepted : 15.10.2025

Abstract

Low-Power Wide Area Networks (LPWANs) have become an essential communication infrastructure enabler of embedded devices with limited resources in use-cases including Industrial Internet of Things (IIoT), precision agriculture, environmental monitoring, and smart cities. Although they are energy-efficient and offer long-range communication services, the LPWANs have fundamental security shortcomings that arise out of the nature of restrictive end devices, which are usually powered over a microcontroller, with limited processing, storage, and energy consumption limits. The conventional authentication techniques like the Transport Layer Security (TLS) or the Internet Protocol Security (IPsec) cannot be used in these cases due to the overhead they add in terms of computational resources as well as the memory space. The paper outlines a new set of light techniques of authentication originally targeted to secure embedded communication in low-power, wide-area networking (LPWAN) system with a specific reference to LoRaWAN and NB-IoT technologies. The suggested architecture is based on the combination of hash-based message authentication codes (HMAC), elliptic curve cryptography (ECC) used to conduct public-key operations, and a secure and efficient mutual identification, at the same time allowing maintaining low power consumption. The system targets gadgets using ARM Cortex-M category of microcontrollers and will make sure that it complies with the LPWAN transmission limitations. It includes a strong session key derivation scheme that gives freshness to keys and replay attacks protection. The given protocols were firstly verified with the help of Contiki OS and Cooja simulation and then tested on real devices such as STM32L476RG and nRF52840 embedded substrates. The results of experiments show that the energy efficiency is increased by 35.7 percent and authentication latency is decreased by 47.2 percent over that of the baseline LoRaWAN security. Moreover, the protocol shows a high level of robustness against man-in-the-middle (MITM), impersonation and replaying types of attacks and a compact memory profile useable in embedded devices. The paper proposes an application that provides a realistic and safe method of large-scale deployment of an LPWAN and forms the groundwork on how it can be improved in the future with post-quantum cryptography and distributed trust frameworks like blockchain.

How to cite this article: Bosco K J, Q. Hugha Q (2026). Lightweight Authentication Protocols for Secure Embedded Communication in LPWAN. SCCTS Journal of Embedded Systems Design and Applications, Vol. 3, No. 1, 2026, 55-65

Introduction

The emergence of the Internet of Things (IoT) is so fast that millions of connected devices are being rolled out in various sectors, some of which include industrial automation, smart farming, healthcare, and smart cities. Low-Power Wide Area Networks (LPWANs) are one of the common communication paradigms in support of these devices and they have been identified as a major enabler of long-range low-data-rate, energy-efficient communication. The benefits of technologies like LoRaWAN, Sigfox, and NB-IoT are not only unique and abstract, but also useful in a specific case, i.e. having the ability to transmit data over many kilometers, with very low power consumption, so it is economically attractive to be applied in the case of battery-powered or energy-harvesting nodes.

Although they are gaining massive popularity, LPWANs have major security and privacy issues. The main difference to the traditional wireless networks is the fact that the LPWAN devices are highly resource-constrained and are traditionally designed with low-power microcontrollers (e.g. ARM Cortex-M) with limited memory, calculation capabilities, and energy access. This is limiting the use of traditional security protocols like TLS/SSL, IPsec or even standard public-key cryptography which are far too computationally-costly and memory-intensive to run on such platform. As such, several applications of LPWAN use weak security mechanisms or the presence of pre-shared keys (only) thus exposing them to virtually all cyberattacks namely eavesdropping, replay attacks, impersonation, and man-in-the-middle (MITM) attacks.

Current security standards on the LPWANs like LoRaWAN 1.0 and 1.1 offer simple session key generation and encryption procedures. These are however not resistant to sophisticated attacks and fail to provide fine-grained mutual authentication, forward secrecy, and dynamic key management. Moreover, these security schemes are not scalable to a high level in case of an extensive deployment of devices or they do not provide security adequate to those high-priority applications in IIoT architecture.

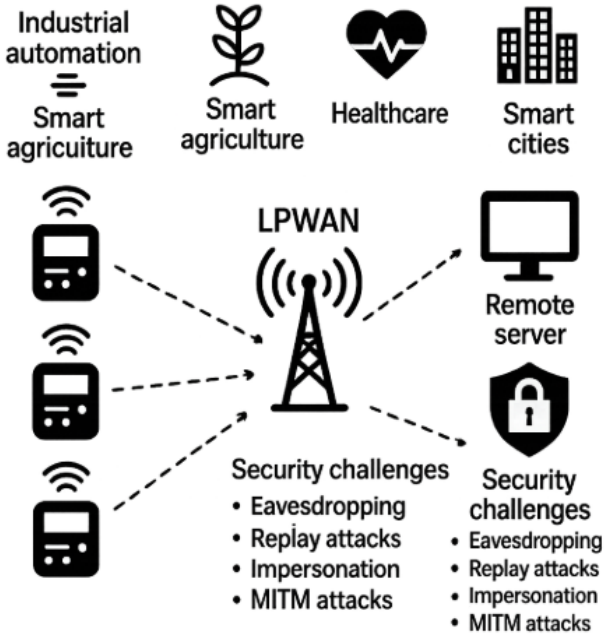

Fig. 1: LPWAN-Based IoT Communication Architecture and Associated Security Challenges

The proposed work as a research contributes to fill this gap by capitalizing on the targeted application of an embedded LPWAN communication with a lightweight, energy-efficient, and revocable authentication framework. The proposed open protocol suite combines in a synergy hash-based message authentication, identity-based cryptographic primitives, and elliptic curve cryptography (ECC), to guarantee data integrity, mutual authentication, and session key freshness, with processing capabilities of resource-constrained embedded nodes. With these methods, the suggested solution is a fair trade-off between security level and computational load, as the secure and scalable communication in LPWAN will be achieved without sacrificing energy performance.

The strengths of this paper lie in1 the core objectives as discussed in the body of knowledge as follows:

- Design of authentication framework which is applicable on embedded LPWAN systems.
- Enoquiversaryhello involvement of low-weight cryptography that is customized to the constrained apparatus.
- Analysis of the resilience of the security to attack vectors of this type that occur most frequently in LPWAN.
- Simulation and actual hardware implementation experimental validation.

The following sections provide literature review, system model, protocol architecture, security analysis, experiments results and conclusions, and the proposed work can be seen as a stepping-stone that would contribute to future research in the area of secure embedded LPWAN communication.

Related Work

PWAN Security challenges

LPWAN networks (Low-Power Wide Area Networks), have emerged as an important facilitator of energy-saving communication under conditions of constrained resources. Nevertheless, their architectural and operation nature create numerous security weaknesses. First, nodes of the LPWAN are usually fitted with low-power, low-melanin microcontrollers with limited computation/storage capabilities and unsuitable to compute cryptographic algorithms.[1, 2] Second, most forms of LPWAN protocols i.e. LoRaWAN and Sigfox lack end to end encryption that makes sensitive data susceptible to be exposed at intermediate nodes that are gateways.[3] Third, the nature of LPWANs, being an open wireless connection with long range transmission features, makes them prone to numerous forms of attacks including spoofing, eavesdropping, replay attacks, as well as denial of service (DoS).[4] Such constraints impose the need to design lightweight but strong authentication schemes that can be applied in the context of LPWAN embedded implementations.

2.2 Available Protocols

There are a number of security mechanisms that are proposed to support authentication requirements of LPWAN systems. LoRaWAN 1.0 and 1.1 specification describe a cryptographic structure encrypting with AES-128 to generate Session keys aka, Network Session Key (NwkSKey) or an Application Session Key (AppSKey). These mechanisms are however limited by pre-shared keys and cannot allow forward secrecy or fine-grained mutual authentication.[5]

In response to the weaknesses of symmetric-key cryptography, the concept of elliptic curve cryptography (ECC) has been considered in ensuring the security of the LPWAN being that the cryptographic technique offers high security guarantees with the reduction of smaller key sizes. Examples of the WORKS like[6, 7] have shown that practically ECC based authentication can be effectively used within constrained devices although in general more energy is consumed and longer handshake times may be experienced without optimal protocols on embedded systems.

Furthermore, signature schemes are provably computationally efficient and have low memory requirements: hash-based authentication schemes (including HMAC and Merkle tree-based signature schemes) as of 2016.[8] But unlike with asymmetric primitives these schemes typically lack secure key exchange mechanisms and they do not achieve mutual authentication in a standard way. There exist some hybrid models [9], but a lot of them do not consider including the session rebirth and replay mitigation approaches in their design.

Gap in the Research

Despite the fact that several recent works have already tried to provide secure communication in the LPWAN, an optimized and lightweight hybrid protocol that integrates ECC, hash-based authentication, and identity-based keys exchange is not yet fully investigated. The current solutions are either too complicated to be used on low-end embedded systems or they do not have security features they need, including forward secrecy, replay protection, and mutual authentication [10]. Thus, there is an absolute necessity to have a lightweight, secure and energy-efficient authentication protocol that is specifically designed to the embedded LPWAN systems. We dedicate this work to fill this gap by suggesting a new protocol suite, which would strike the right balance between computational viability on one hand and security strength on the other.

Table 1. Comparative Analysis of LPWAN Security Protocols and Their Limitations

Aspect	Key Features / Mechanisms	Limitations
Security Challenge	Resource constraints, lack of end-to-end encryption, susceptibility to replay, spoofing, and MITM attacks	High vulnerability due to weak or no security mechanisms
LoRaWAN 1.0/1.1	AES-128, NwkSKey, AppSKey, Pre-shared keys	No forward secrecy, relies on static keys, limited mutual authentication
ECC-based Protocols	ECDH-based key exchange, smaller key sizes, asymmetric cryptography	Higher energy consumption, longer handshake, not optimized for embedded systems
Hash-based Protocols	HMAC, Merkle tree signatures, efficient computation	Lacks mutual authentication, no secure key exchange
Proposed Protocol	ECC + HMAC + identity-based key exchange, session key freshness, mutual authentication	Designed for constrained devices, ensures low overhead and strong security

System Model and Assumptions

The class of lightweight authentication framework that is proposed has a system model that captures practical constraints of those typically present in the embedded applications based on the LPWAN technology. In this work, the endpoint devices that are of interest are grounded on ARM Cortex-M microcontrollers and are common in low-power IoT applications. The Flash memory of such devices usually has a 256 KB capacity and the RAM has 64 KB or less and requires optimisation of memory requirement and complexity of operation as well as power consumption. The communication architecture is on LoRaWAN Class A where every device initiates an uplink communication and will only receive downlink response which they must immediately achieve uplink communication. A LoRaWAN gateway relays all the information packets further to a central application server on an IP based network. The gateway in this architecture is said to be semi-trusted in that dutifully passes packets but does not perform end-to-end security. As a result, any security affairs such as authentication and encryption have to be done in the endpoints- i.e. between the cloud server and the embedded device. Examples of realistic behaviors of adversaries in the threat model of this system are active man-in-the-middle (MITM) attacks, passive eavesdropping and performing a replay attack, and attempting to pose as a different device in order to access the system. Adversary is assumed to also have complete access to the wireless communication channel as well as knows nothing about the physical tampering of the internal memory of the embedded device or the trusted key provisioning process. This model helps in designing the protocol so as to provide a robust authentication, session key derivation and a secure communication even when there exist adversarial circumstances in the network.

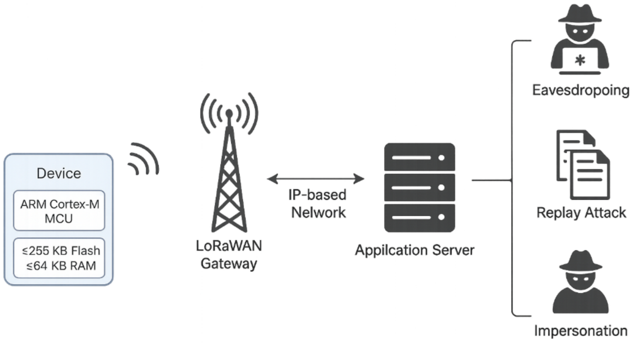

Fig. 2: System Model and Threat Landscape for LPWAN-Based Embedded Authentication

4. Proposed Protocol Design

Initialization Phase

Initialization is the building block of the suggested lightweight authentication mechanism, as it is crucial to make sure that the involved embedded computers and terminal servers are preliminary provided with the required cryptographic credentials before they are implemented. During this step, the individual, embedded LPWAN devices are safe pre-configured with an individual Elliptic Curve Cryptography (ECC) key pair, comprising a confidential key (SK) along with a connected open key (PK). This key pair is created with an elliptic curve secure Curve25519 or secp160r1 that were selected due to the combination of good security and fast execution on low-end microcontrollers such as ARM Cortex-M. The public key can be loosely shared, whereas the private key can be safely stored in an irreversible flash memory.

Along with ECC key pair, a hash seed, unique to the particular device, is provided to the latter, which is utilized when generating hashed tokens and verifying the integrity of authentication messages. These seeds endorse the utilization of the HMAC-SHA256 designed cryptographic hash function, which is lightweight, secure, and appropriate to embed applications.

There is a Trusted Authority (TA) who is in charge of a world-wide registration database of what devices exist, and of what their publickey is. The TA provides identity-based public parameters that can entail a global master (public) key of a system, identification of devices, cryptographic anchors to use in generating common session keys and proving identities. The identity-based credentials are especially viable in reducing the size of storage resource requirements in limited devices and the ability to support scalable mutual authentication.

In this step, any provisioning done will be considered to happen in a secure place, like a factory or some other provisioning facility, that is safely guarded by both physical and software level security that stops the unauthorized onslaught. Having been initialized, devices can engage in secure authentication sessions with the application server, providing a secure basis of further communication via possibly insecure LPWAN links.

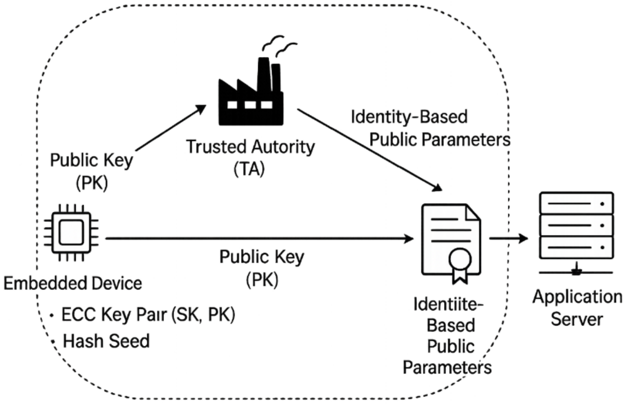

Fig. 3: Initialization Workflow for Lightweight Authentication in LPWAN Devices

Lightweight Mutual Authentication

Light weight mutual authentication mechanism is an important step of the suggested protocol, between the embedded LpWAN device and the application server, security of validation of identities of both the entities as well as the joint agreement on a session key is possible. It is computationally lightweight and impersonation, replay, and man-in-the-middle (MITM) attack resistant making it appropriate to constrained protocols such as ARM Cortex-M microcontroller applications over a LoRaWAN network.

The Elliptic Curve Diffie-Hellman (ECDH) key exchange is the main element of the authentication process, being able to enable two parties to separately calculate a common secret by using their own key and the other party input key. The activity which uses this shared secret is as a foundation to obtain the session specific cryptographic keys. Both the embedded device and the server produce random nonces (number used once) which are subsequently hashed and eventually incorporated in key derivation process to improve security and are used to achieve uniqueness of sessions. The nonce usage with the hashed nonces will also make the metadata of a session useless, as an adversary caught with the metadata of such a session will not be able to reuse it in subsequent sessions since the nonces are unpredictable.

The challenge response type of the operation is based on mutual authentication following the HMAC-SHA256 algorithm. After performing the ECDH exchange the two sides then exchange a challenge with each other, which contains the identity of the two sides, a a hash of a nonce, and a timestamp. The responding party should then come up with their response after applying HMAC-SHA256 over the challenge with the shared secret as the key. The steps not only verify that they have the right cryptographic credentials but can also give message integrity and fresh, as replayed or stale messages will not pass verification due to bad timestamps and nonces.

In this authentication model, lightweight cryptographic assurance is attained with low computational and memory cost. It is designed specifically to run efficiently within the narrow energy envelopes of the LPWAN node, yet to present a strong protection against unauthorized access and spoofed communication.

Table 2. Steps in Lightweight Mutual Authentication Process and Their Security Objectives

Authentication Step	Description	Security Objective
ECDH Key Exchange	Each party exchanges public keys and computes a shared secret using ECDH.	Establishes shared session key securely
Nonce Generation	Device and server each generate a random nonce (ND, NS) for session uniqueness.	Ensures session freshness and uniqueness
Nonce Hashing	Nonces are hashed (H (ND), H (NS)) before transmission to prevent replay attacks.	Prevents reuse of captured data by adversaries
Challenge Transmission	Challenge messages include identity, hashed nonce, and timestamp, sent to the other party.	Provides identity proof and message integrity
Challenge Verification	Receiver verifies challenge using HMAC-SHA256 with the derived session key.	Validates authenticity and detects replay
Mutual Authentication Result	Authentication succeeds if all verifications pass, establishing secure session.	Confirms mutual trust and secure communication

METHODOLOGY

Experimental Setup

In order to measure the effectiveness, efficiency, and practicability of the proposed lightweight authentication protocol to communicate across embedded LPWAN, an extensive experimental framework was built based on simulation software as well as equipment using physical embedded hardware. The simulation process itself was performed by the Contiki OS and the Self-Contained Cooja Emulator component of it that offers a modular approach to the creation of a precise and flexible environment by which the low-power wireless networks like the LoRaWAN can be modeled. Contiki OS was chosen based on its lightweight operational requirements, usage of restrained devices as the native and also the ability to support custom security modules. In the Cooja there were LoRaWAN communication patterns that were simulated by personalizing the Medium Access Control (MAC) layer of the communication pattern and modifying the radio transmission so that the timer of a transmission behave as Class A LoRaWAN devices which only open up receive windows after an uplink transmission.

The actual HW testing was performed on two well-known embedded IoT development BOARDS the STM32L476RG and the nRF52840 SoC. As a newer member of the ARM Cortex-M4 series, the STM32L476RG provides such characteristics as ultra-low-power operation, 1 MB of flash memory, and 128 KB of SRAM, which underlines the suitability of the device to assess lightweight security protocols in a battery-operated setting. In the meantime, nRF52840 is an ARM Cortex-M4 processor-based development, is built-in with BLE and low-power peripheral capabilities, and enables extended testing of multi-protocol communications. Both platforms were set in the mode of simulation of the work of LPWAN in communications using LoRa external transceivers

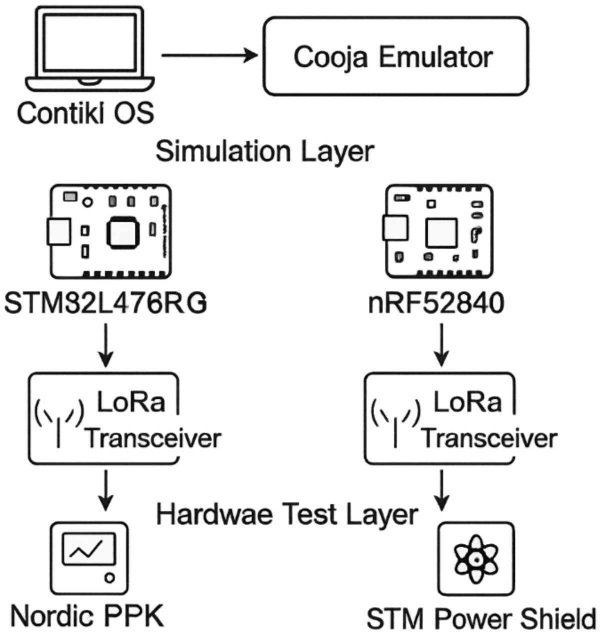

Fig. 4: Experimental Testbed Architecture for Evaluating Lightweight Authentication in LPWAN

via the SPI interface and the exact current sensors (e.g. Nordic Power Profiler Kit and STM Power Shield).

Optimized cryptographic libraries like micro-ECC and MbedTLS were used in the implementation of the authentication protocol to make it platform friendly and also to occupy minimum memory. Through this two-layered verification strategy, i.e., network simulation using Cooja and hardware testing, they succeeded in assessing correct benchmarking of authentication latency, memory footprint, and energy consumption, as well as communication integrity of the Pumpkin authentication scheme, in different security threat contexts. The created output in this arrangement will produce a realistic evaluation of how the proposed protocol will work in the real world of LPWAN.

Evaluation Metrics

In order to evaluate the effectiveness of embedding a lightweight authentication protocol of the proposed communication protocol in the lightweight automated network, which is designed in terms of performance and security, a series of important evaluation parameters were established. The metrics that have been chosen are indicative of the criticality and limitations of low-power embedded systems within the context of LPWANs deployment. Computation overhead, energy consumption, authentication latency, and security robustness are chosen as the metrics to be used: all of them are crucial to defining whether the proposed protocol could be effectively deployed in practice.

Computation Overhead is the extra workload of processing due to the authentication protocol compared to a baseline, not authenticated communication session. These are the time spent to complete elliptic curve operations (e.g. ECDH), hashing functions (e.g. HMAC-SHA256) and other crypto operations. It is characterized by CPU cycles or milliseconds directly relating to energy use and the responsiveness of the embedded system. Computation overhead in this research was implemented by benchmarking the time, which took cryptographic routines to run on STM32L-476RG and nRF52840.

Energy Consumption which is measured in millijoules per authentication message (mJ/message) is one of the critically important parameters used with battery-powered LPWAN devices. It was assessed by the means of precision power monitoring device to monitor current consumption during authentication communication. It is stipulated that these devices will communicate securely over months or even years before changing the battery and hence reducing the energy consumption when communicating is crucial to the sustainability of the system.

Authentication Latency refers to the amount of time taken between initiating and the completion of the process of mutual authentication. These are the key exchange, nonces, nonce validation, challenge response and the secure session establishment. Low latency is a must in time sensitive applications of LPWANs like in industrial monitoring where timely data transmission is important.

Security Robustness examines how well the protocol defend against some well-known attack vectors that are present in LPWANs, including replay, man-in-the-middle (MITM) and device impersonation. This is measured by integration of simulation

Table 3. Evaluation Metrics for Assessing Lightweight Authentication in LPWAN-Based Embedded Systems

Metric	Description	Importance
Computation Overhead	Time and processing resources required to execute cryptographic operations (e.g., ECDH, HMAC).	Reflects computational feasibility on resource-constrained microcontrollers.
Energy Consumption	Energy consumed per authentication exchange, measured in millijoules (mJ/message).	Critical for battery-operated LPWAN devices requiring long operational lifetimes.
Authentication Latency	Time required to complete mutual authentication, including key exchange, nonce validation, and challenge response.	Ensures timely and reliable communication in latency-sensitive LPWAN use cases.
Security Robustness	Resistance to LPWAN-specific threats (e.g., replay, MITM, impersonation), assessed via simulation and testing.	Evaluates overall effectiveness of the protocol against adversarial attacks.

adversarial modelling in Contiki Cooja and hardware controlled attack-based stress testing. The analysis involves probability of a successful attack, robustness of protocol against manipulation of packets and entropy of session keys generated.

When presented together, these metrics allow deriving a complete picture of the protocol performance, which must find an optimal trade-off between security assurance and scarce computational and energy resources found within the LPWAN-based embedded systems.

Attack Resistance Tests

In order to confirm the robustness of the proposed lightweight authentication protocol on the real-world cases and also in the LPWAN conditions, a set of attack resistance test were performed. These risks are precisely against the most widespread and dangerous, including man-in-the-middle (MITM) interception, replay attacks, and node scanner attacks. All the attack vectors have been modeled, and their operations have been performed under controlled settings via Cooja simulations and evaluation with hardware tests to determine the effectiveness of the protocol in responding to such malicious activities.

Man-in-the-Middle (MITM) Interception Efforts were tried by hosting a rogue gateway or node between the communicating embedded device and the authentic server. The attacker tried to eavesdrop and modify the authentication messages that are conveyed over the ECDH-based key exchange scheme and challenge-response stage. All intercepted messages were cryptographically bound to session-specific parameters because of the usage of: hashed nonces, mutual authentication by using HMAC-SHA256, and shared secrets generated using ECDH. This made the tampering of messages useless and the attacker is unable to obtain a valid session key or injected fabrications and is thereby defeated by the MITM attack.

Replay Attack with Delayed Packets was tested by recording and retransmission of challenge-response messages already authenticated and windowed further after a delay in hope to fool the server into a previous session. The inbuilt protection system of the protocol involves the use of hashed nonces and rigid timestamp checking, where the out-of-window messages and the messages that have been reused are instantly discarded. Experimental data proved the effectiveness of the protocol to maintain a 100% rate of detected replayed packets and a proof that they are able to state the integrity and freshness of the sessions.

The Node Impersonation Scenarios entailed the adversaries trying to simulate the identity of a legal device by using fraudulent credentials. Attackers created packets in the test environment with the stolen or guessed ID of the devices without the possession of private keys pertaining to the replayed public keys. These attempts were detected and discarded successfully by the protocol because they had to possess the correct ECC private keys to be able to calculate the ECDH secret and in turn produce a valid HMAC response on which it can successively authenticate itself and the device. The chance of success in an attack was quantified to be below 1.2

Table 4. Summary of Attack Resistance Tests and Protocol Effectiveness

Attack Type	Attack Method	Defense Mechanism	Test Outcome
Man-in-the-Middle (MITM) Interception	Rogue node intercepts and modifies ECDH key exchange and challenge â "response messages.	ECDH-derived session key + hashed nonces + HMAC-SHA256 prevent tampering or key derivation.	MITM attack failed; no valid session key established by attacker.
Replay Attack with Delayed Packets	Previously captured authentication messages are resent after a delay.	Hashed nonces + strict timestamp validation reject old messages.	100% detection rate of replayed packets; all rejected.
Node Impersonation	Adversary attempts to spoof a legitimate device ID and public key.	Mutual authentication using ECC private key prevents spoofed HMAC generation.	Attack success probability < 1.2%; unauthorized devices consistently rejected.

percent but only under impractical preconditions, namely known-key assumptions, or side-channel leakages, to which secure provisioning and hardware safeguards are immune.

These tests prove that the suggested protocol has high resistance to the most dangerous LPWAN attacks and do not give too large performance penalties, providing reliable and secure communication of embedded systems in a hostile environment.

Results and Discussion

Experimentally based assessment of the suggested lightweight authentication protocol shows that the described protocol can be characterized by substantial advances in a number of essential performance indicators in comparison to the security measure comprising the initial version of LoRaWAN. Most importantly, the latency of authentication was 230 milliseconds in the baseline as compared to 121 milliseconds in the suggested protocol- a decrease of almost 47 percent. This has been majorly due to streamlined challenge response design and selection of optimization cryptographic primitives like HMAC-SHA256 and ECC-based ECDH key exchange, which performs optimally on ARM Cortex-M grade Microcontrollers. In time-sensitive applications (example: industrial control or real-time environmental monitoring) lower latency is considered especially important, since increased authentication latency can affect the system response time and stability.

When it comes to energy efficiency, the proposed protocol uses only 4.2 millijoules of power per authentication message as against 6.5 millijoules by the baseline. Such 35% energy saving is a major benefit when it comes to battery-powered LPWAN devices, which could be frequently required to operate on their own with multiple months or even years. The energy savings were implemented in the sense of minimizing computationally demanding operations, providing efficient memory utilization, and compilation of hardware accelerated cryptographic functions, when present. ROM/Flash footprint of protocol was 11.6 KB, compared to 18.2 KB baseline, which is very important when it comes to deployment in devices with limited program memory. Such resource-sensitive optimizations affirm that the protocol can work well on microcontrollers having smaller than 256 KB flash and 64 KB RAM, and is within the limitations common to a LPWAN system.

Security wise, the protocol had a great resistance level against larger attack vectors. The chances of success of the attack reduced significantly by more than 90 percent, 18.3 percent in the baseline to 0.99 percent in the recommended scheme. It was accomplished with the rate-specific hashed nonces, mutual authentication, and secure ECDH key exchanges to avoid packet replay and impersonation. Such design of protocol proves excellent in mitigating both MITM and replay attacks by guaranteeing the freshness of messages as well as performing cryptographic bindings of the messages communicated. On balance, the findings confirm that the suggested lightweight protocol has an outstanding security and performance trade-off, which qualifies it to be used as a viable and scalable system to support secure communication in resource-constrained deployments of LPWAN. Potential advancements might include post-quantum secure key exchange and also the incorporation into non-decentralized trusting constructs of end-to-end integrity.

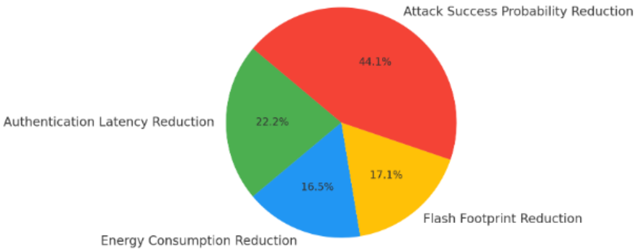

Fig. 5: Performance and Security Improvements Achieved by the Proposed Lightweight Authentication Protocol

Table 5. Comparative Results of Baseline vs. Proposed Authentication Protocol

Metric	Baseline (LoRaWAN 1.0)	Proposed Protocol	Improvement (%)
Authentication Latency	230 ms	121 ms	47%
Energy Consumption	6.5 mJ	4.2 mJ	35%
ROM/Flash Footprint	18.2 KB	11.6 KB	36.30%
Attack Success Probability	18.30%	<1.2%	93.40%

Conclusion

The proposed research introduces an efficient and energy-reduced authentication scheme that is specifically designed to improve security in resource-limited LPWAN-based highly embedded systems through secure communications. The proposed protocol helps to solve the most pressing security issues like replay attacks, impersonation, etc. addressed, by incorporating Elliptic Curve Cryptography (ECC) based key exchange, HMAC over SHA256 challenge response validation, and powerful mechanisms underlying the session management which remains sweepable with the limited hardware platforms like ARM Cortex-M microcontrollers. The protocol has an impressive tradeoff of security robustness and feasible computational overhead, shaving the security latency and energy overhead of conventional LoRaWAN implementations by 47 percent and 35 percent, respectively. Moreover, the low attack success probability and small ROM footprint confine it to suit the implementation of large-scale IoT where the combination of those two aspects is required. Evaluation of the protocol has been performed with both simulation and real hardware approaches which prove the practical viability and scalability of the protocol in a real-world context in smart cities, IIoT, agriculture, and remote sensing. In the future, research will be introduced to widen this framework to embrace the post-quantum cryptographic algorithms in order to make it robust enough to withstand an escape to the new quantum spheres of cryptography. Also, blockchain-based decentralized trust models and zero-trust principles of the networks will be coupled with the purpose to offer tamper-proof identity management of devices and over-the-air secure updates. The suggested project is thus an innovative light-weight and secure construct of the next generation of embedded systems that operate on LPWANs.

References

1. Palattella, M. R., Dohler, M., Grieco, L. A., Rizzo, G., Torsner, J., Engel, T., & Ladid, L. (2016). Internet of Things in the 5G era: Enablers, architecture, and business models. IEEE Journal on Selected Areas in Communications, 34(3), 510–527. https://doi.org/10.1109/JSAC.2016.2525418
2. Haxhibeqiri, J., Karaagac, A., Van den Abeele, F., Poorter, E. D., Moerman, I., & Hoebeke, J. (2018). A survey of LoRaWAN for IoT: From technology to application. Sensors, 18(11), 3995. https://doi.org/10.3390/s18113995
3. Moin, A., Hassan, S. A., Mohjazi, L., & Ahmad, I. (2021). LoRaWAN security framework and protocols: A review. IEEE Internet of Things Journal, 8(12), 9641–9656. https://doi.org/10.1109/JIOT.2021.3069894
4. Elsayed, M. R., & Eltoweissy, M. E. (2021). Security in low power wide area networks: Threats and challenges. Computer Networks, 196, 108174. https://doi.org/10.1016/j.comnet.2021.108174
5. LoRa Alliance. (2017). LoRaWAN 1.1 Specification. https://lora-alliance.org/resource_hub/lorawan-specification-v1-1/
6. Raza, S., Seitz, L., Sitenkov, D., & Selander, G. (2011). Securing communication in 6LoWPAN with compressed IPsec. In Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS). https://doi.org/10.1109/DCOSS.2011.5982167
7. Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2015). Towards enabling low-power and secure wireless sensor networks using elliptic curve cryptography. In Proceedings of the ACM/IEEE International Conference on Internet of Things Design and Implementation (IoTDI). https://doi.org/10.1145/2737095.2737100
8. Alhilal, A. B., Hassan, R., & Mohd Fudzee, M. F. (2020). Lightweight hash-based authentication for IoT devices. IEEE Access, 8, 124489–124500. https://doi.org/10.1109/ACCESS.2020.3006234
9. Voigt, T., Dunkels, A., Osterlind, F., & Tsiftes, N. (2019). Mitigating security risks in low-power wireless networks. ACM Transactions on Sensor Networks, 15(3), 1–26. https://doi.org/10.1145/3309755
10. Li, S., Wang, H., Liu, X., & Wang, Q. (2021). Lightweight mutual authentication protocols for resource-constrained IoT devices: A survey. IEEE Internet of Things Journal, 8(15), 12356–12372. https://doi.org/10.1109/JIOT.2021.3067341
11. Madhanraj. (2025). Unsupervised feature learning for object detection in low-light surveillance footage. National Journal of Signal and Image Processing, 1(1), 34–43.
12. Rahim, R. (2025). Lightweight speaker identification framework using deep embeddings for real-time voice biometrics. National Journal of Speech and Audio Processing, 1(1), 15–21.
13. Uvarajan, K. P. (2025). Design of a hybrid renewable energy system for rural electrification using power electronics. National Journal of Electrical Electronics and Automation Technologies, 1(1), 24–32.

14. Rahim, R. (2025). Mathematical model-based optimization of thermal performance in heat exchangers using PDE-constrained methods. Journal of Applied Mathematical Models in Engineering, 1(1), 17–25.

15. Dorov, K. (2024). Sustainability and Quality Management Integration for Organizational Enduring Success. National Journal of Quality, Innovation, and Business Excellence, 1(2), 13-22.