DOI: https://doi.org/10.26642/ten-2026-1(97)-324-331
UDC 004.056.55

B.V. Cherniavskyi, Postgraduate Student
Oles Honchar Dnipro National University

Cross-layer IoT security using radio frequency fingerprinting and lightweight cryptography

The paper discusses the results of research on a security protocol for IoT devices in an LPWAN environment. To test the hypothesis, a hybrid protocol using radio frequency fingerprinting (RFF), TESLA, and the lightweight Ascon-128a encryption method was developed and verified. Experimental results were obtained on 8 and 32-bit controllers, on the arm64 platform. This approach to data transmission protection provides an appropriate level of comprehensive protection with minimal computing resources and insignificant transmission delays. The architectural approach demonstrates the ability to effectively resist cloning and replay attacks, which is undoubtedly critically important in wireless networks. Special attention is paid to the problem of resource limitations in LPWAN systems, where the use of traditional DTLS protocols is impractical and resource-intensive, and in some cases technically impossible, since complex operations based on the RSA algorithm are used to agree on AES keys. This approach uses almost all resources for network coordination and encourages the use of more expensive controllers to achieve the required level of security in industrial solutions. The practical implementation was built on the Arduino Uno R4 WIFI platform using the LoRa library and a server component developed in Go for the ARM64 computing architecture, which confirmed the hypothesis. At the stage of system integration, specific synchronization methods were designed to prevent time deviation in the operation of the TESLA protocol, as well as algorithms for deriving radio frequency fingerprints using the database abstraction layer. Profiling on the Arduino platform proves the high efficiency of the approach with millisecond transactions and minimal memory consumption, and the use of radio frequency fingerprints allows you to reliably block malicious traffic even before the start of resource cryptographic checks.

Keywords: *IoT Security; LPWAN; Radio Frequency Fingerprinting; Ascon; TESLA; Cross-layer Security.*

Formulation of the problem. The integration of Internet of Things (IoT) architectures into critical infrastructure encompassing smart grids, environmental monitoring, and industrial automation has generated highly intricate security challenges. To facilitate this rapid technological expansion, Low-Power Wide-Area Networks (LPWAN), specifically NB-IoT and LoRaWAN [1], are predominantly utilized due to their optimal balance of energy efficiency and extended transmission range. Nevertheless, a profound vulnerability gap emerges from the fundamental hardware limitations inherent to LPWAN edge devices, which are generally driven by basic 32-bit ARM or 8-bit AVR microcontrollers [2; 3].

Implementing conventional cryptographic frameworks, such as Datagram Transport Layer Security (DTLS) [4], is highly problematic within these resource-deprived contexts. The inherent characteristics of standard protocols specifically their extensive handshake procedures, necessity for packet fragmentation, and heavy computational loads can rapidly exhaust the restricted bandwidth and severely deplete the power reserves of LPWAN deployments [5]. To circumvent these operational bottlenecks, network operators often adopt non-standard, lightweight security mechanisms based on security-by-obscurity paradigms or static cryptographic keys. Ultimately, such compromises inadvertently expose the infrastructure to severe threat vectors, including replay attacks, device cloning, and man-in-the-middle (MitM) interceptions. The fundamental challenge investigated in this dissertation is the absence of a standardized, resource-aware security framework tailored for «Arduino-class» IoT devices, which must simultaneously counteract physical cloning and digital intrusions, such as tampering and replay attacks, while strictly adhering to the severe energy and computational limitations inherent to LPWAN deployments.

Analysis of recent research and publications. Although the protection of resource-constrained IoT endpoints has received considerable scholarly attention [6–8], a universally applicable defense paradigm has yet to be established. The current body of research predominantly bifurcates into distinct domains: the mitigation of static key vulnerabilities, optimizations of cryptographic algorithms, physical-layer security enhancements, and the resolution of broadcast authentication bottlenecks. A fundamental flaw in contemporary LPWAN deployments, particularly within the LoRaWAN ecosystem [10; 11], stems from an overreliance on static symmetric keys (typically AES-128 [9]) for both network and application-level security. As highlighted by Ntshabele et al., this static key architecture exposes the infrastructure to severe threat vectors, including replay exploits and device cloning, especially when physical access to the edge node is compromised [12]. While dynamic session key management schemes have been proposed to address these vulnerabilities, they frequently introduce prohibitive

computational costs. Pathak et al. demonstrated that centralized lightweight key exchange mechanisms can reduce transmission overhead [13]. Recent advancements by Sravan et al. utilizing elliptic curve cryptosystems have shown promise in establishing dynamic session keys with forward secrecy [14]. However, the integration of these dynamic schemes on basic 8 or 32-bit microcontrollers continues to generate substantial computational and transmission overhead, rapidly exhausting the restricted bandwidth and severely depleting the power reserves of LPWAN deployments.

In response to the operational inefficiencies inherent in traditional cryptographic frameworks like DTLS 1.3 [4] and AES-GCM, the National Institute of Standards and Technology (NIST) finalized its lightweight cryptography standardization in 2023 with the adoption of Ascon [15]. Utilizing a permutation-based architecture, Ascon is specifically tailored for brief message payloads and severely limited hardware, rendering it a far more viable option for LPWAN telemetry. The cipher's ability to provide authenticated encryption with associated data (AEAD) ensures data integrity and confidentiality without the massive computational burden of conventional standards. Nevertheless, reliance on cryptography alone is fundamentally insufficient against physical device cloning attacks in scenarios where malicious actors manage to extract key material directly from a compromised edge node. This limitation necessitates the integration of supplementary security layers that operate independently of stored cryptographic secrets.

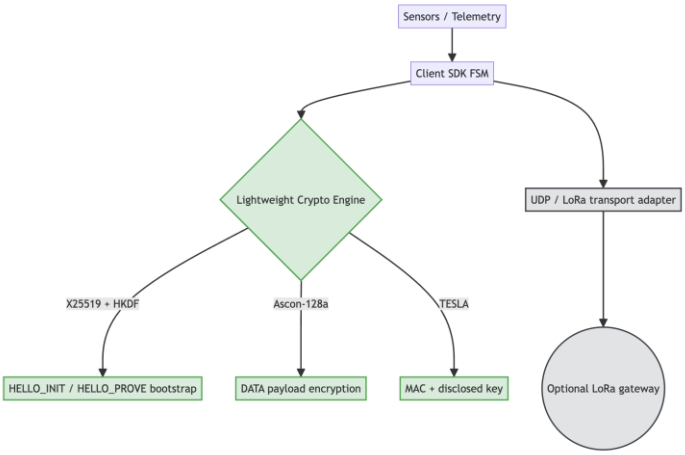
To address the vulnerabilities of purely cryptographic defenses, Radio Frequency Fingerprinting (RFF) has gained traction as a formidable method for hardware authentication. This approach exploits distinct, hard-to-replicate analog imperfections within radio transceivers such as non-linearities in the power amplifier and oscillator drift to generate a unique hardware signature [16]. Recent research has increasingly focused on applying deep learning methodologies to enhance RFF accuracy. For instance, Dhakal et al. proposed an RFF authentication approach utilizing Siamese neural networks to achieve high identification precision in IoT networks [17]. Despite the theoretical efficacy of these machine learning paradigms, a critical paradox emerges in applied deployments: the computational demands of executing deep neural networks, even in their quantized forms, far exceed the processing capabilities and memory constraints of «Arduino-class» microcontrollers. Furthermore, the probabilistic characteristics of RFF, coupled with its vulnerability to environmental dynamics like channel fading and SNR variations, preclude its use as an isolated defense mechanism. Consequently, contemporary literature increasingly advocates for cross-layer security architectures that synthesize PHY-layer attributes with upper-layer protocols [18], utilizing computationally efficient algorithms, such as Exponentially Weighted Moving Average (EWMA), to dynamically adapt baseline profiles without overwhelming the edge device.

Beyond point-to-point telemetry, the secure dissemination of control directives from a centralized server to multiple edge nodes presents a distinct set of challenges. Traditional broadcast authentication relies heavily on asymmetric digital signatures (e.g., RSA or ECDSA), which impose a paralyzing computational burden on resource-deprived IoT devices. To circumvent this bottleneck, the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol has been adapted for IoT environments, utilizing symmetric cryptographic functions and delayed key disclosure to achieve asymmetric security properties [19]. Recent adaptations of TESLA have sought to enhance reliability through decentralized architectures; for example, Garcia et al. explored a blockchain-backed μTesla implementation for secure broadcast communications in drone networks [20]. However, the integration of blockchain consensus mechanisms introduces latency and complexity that are antithetical to the stringent operational parameters of LPWANs. Therefore, a pure reverse-hash-chain TESLA implementation remains the most pragmatic approach for broadcast authentication in constrained environments. Yet, a substantial empirical gap remains: the practical integration of RFF alongside advanced, lightweight cryptographic protocols like TESLA and Ascon on standard commodity microcontrollers is currently underexplored in applied deployments.

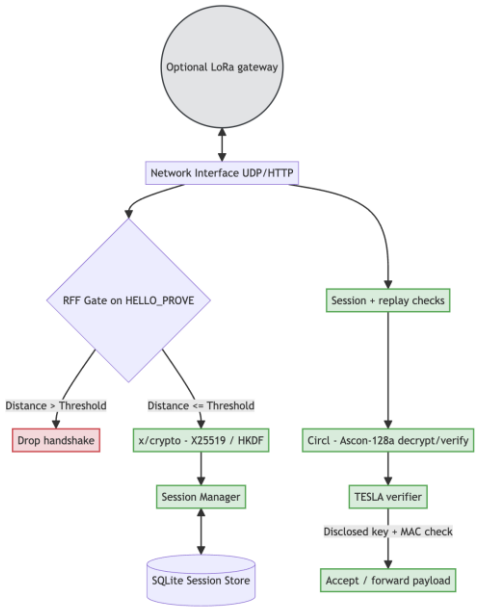
Task statement. To resolve this deficiency, the present research introduces and empirically validates a multi-layered security protocol that strategically integrates physical-layer authentication, specifically Radio Frequency Fingerprinting (RFF), with highly efficient cryptographic primitives, namely Ascon and TESLA.

Outline of the main material of the study. This proposed architecture is organized hierarchically across the Physical, Transport, and Application layers, establishing a robust defense-in-depth paradigm wherein the compromise of a single stratum does not jeopardize the integrity of the overarching system.

To visualize the proposed cross-layer security architecture, figures 1, *a* and *b* present the separated views of the resource-constrained IoT edge node and the centralized server.



a) IoT edge node architecture



b) Central server architecture

Fig. 1.

Operating at the foundational Physical layer, the framework utilizes an RFF Gate to verify the unique hardware signature of the transmitting node, functioning as the primary countermeasure against device cloning. During the feature extraction phase, the receiving entity derives a specialized vector from the incoming analog transmission, capturing essential metrics including the Received Signal Strength Indicator, Signal-to-Noise Ratio, Preamble Duration, and Frequency Error. The authentication mechanism relies on maintaining an established baseline profile for each registered endpoint. Consequently, upon the arrival of a transmission with feature vector V, the system computes the squared Euclidean distance $D^2(B_i, V)$ separating the stored baseline B_i from the incoming signal:

$$D^2(B_i, V) = \sum_{k=1}^{n} (B_{ik} - V_k)^2, \quad (1)$$

where n is the number of extracted features. To effectively compensate for environmental fluctuations, an Exponentially Weighted Moving Average (EWMA) algorithm is deployed to continuously adapt the baseline profile following each authorized communication:

$$B_i^{(new)} = \alpha \cdot V + (1 - \alpha) \cdot B_i^{(old)}, \quad (2)$$

where $\alpha \in (0,1)$ represents the learning rate. Should the calculated distance surpass a dynamic boundary, determined by the parameters ThresholdWarm and ThresholdStable, the HELLO_PROVE handshake request is

immediately discarded prior to expensive ECDH/HKDF operations, thereby substantially conserving both computational bandwidth and battery reserves.

To facilitate a protected transmission corridor at the Transport layer, the architecture executes an Elliptic Curve Cryptography (ECC) [21] handshake, deliberately exploiting Curve25519 (X25519) [22; 23] to achieve ephemeral key exchange. The negotiation sequence initiates with a HELLO_INIT message, wherein the edge device solicits a stateless cookie from the central server. To mitigate potential Denial-of-Service vulnerabilities, the server replies via a HELLO_COOKIE transmission containing a cryptographically signed cookie. Subsequently, the client node issues a HELLO_PROVE request, demonstrating possession of the valid cookie while concurrently transmitting its ephemeral X25519 public key. Following this exchange, both communicating entities derive a mutual shared secret utilizing ECDH. This secret is subsequently processed through a Hash-based Key Derivation Function (HKDF) [24] to generate two distinct session keys: an AsconKey of 16 bytes dedicated to encryption, and a 32-byte TeslaSeed reserved for broadcast authentication purposes. By exclusively utilizing ephemeral keys, the protocol guarantees perfect forward secrecy, ensuring that historical data exchanges remain mathematically secure even in the event of a future session key compromise [14].

At the Application layer, the protocol governs source authentication, data integrity, and overall confidentiality through the deployment of Ascon and TESLA. All transmitted telemetry payloads undergo authenticated encryption utilizing the Ascon-128a cipher [25], a mechanism that strictly prohibits unauthorized data interception or modification. Within this scheme, the Associated Data (AD) component cryptographically binds the payload to a designated timestamp, sequence number, and specific session, thereby neutralizing context-based exploitation attempts. Furthermore, to authenticate broadcast directives originating from the server and targeting multiple remote nodes without incurring the heavy processing overhead associated with per-packet asymmetric signatures [20], the architecture incorporates an adapted TESLA mechanism [19]. This process requires the central server to construct a cryptographic sequence using a one-way hash function. Implementing a delayed disclosure strategy, the server utilizes a specific key, denoted as K_t, to generate a Message Authentication Code (MAC) for a payload transmitted during interval t, while the actual key K_t is only revealed in a subsequent transmission during interval t+1. The receiving device temporarily buffers the initial packet P_t until the corresponding key K_t is disclosed. The MAC verification is performed as follows:

$$MAC_t = HMAC(K_t, P_t). \quad (3)$$

Upon receiving K_t, the node first verifies its legitimate presence within the hash chain by confirming $K_{t-1} = H(K_t)$ and then validates the MAC_t, thereby achieving rigorous source authentication with negligible computational penalty.

The practical viability of this theoretical model was substantiated through the development of a comprehensive full-stack prototype, comprising a firmware client and a centralized server, characterized by a highly modular codebase to ensure extensibility and facilitate rigorous testing. Engineered in Go (Golang), the central server functions as the primary authority for data processing and cryptographic authentication, heavily relying on the Cloudflare circl library to execute advanced operations such as X25519 and Ascon-128a. A critical server component, the RFF Manager, is responsible for the storage and dynamic EWMA-based updating of device profiles, optimizing performance by substituting computationally expensive square root operations with squared Euclidean distance calculations during the preliminary filtering stage. Additionally, active connections are governed by a Session Store backed by an SQLite database, which tracks expiration times, the max_seq parameter for replay prevention, key_id, and session_id, ensuring seamless persistence across potential system reboots. To support the TESLA protocol, the server dynamically generates a reverse hash chain, signing current communications with Kt while disclosing Kt-1 for historical verification. Interaction with the client SDK is facilitated through RESTful endpoints governed by an HTTP/SDK Interface, which enforces a custom HMAC-driven security protocol, designated as X-SDK-Signature, to guarantee that handshake initiations and data submissions are restricted exclusively to authenticated nodes.

On the endpoint side, the client firmware was specifically compiled for the Arduino Uno R4 WiFi, a platform driven by a Renesas RA4M1 32-bit ARM Cortex-M4 microcontroller. This firmware operates upon a custom C++ SDK engineered to abstract the intricate operations of the underlying security stack. The structural design of the SDK incorporates an IUdpTransport interface, a strategic abstraction that thoroughly decouples the cryptographic logic from the physical transmission medium. Within the context of this evaluation, long-range connectivity is achieved by mapping this interface to a LoRa adapter via the LoRa.h library. The cryptographic engine embedded within the SDK features highly optimized C++ implementations of Ascon-128a and X25519 for ECDH, meticulously calibrated to maximize execution velocity while minimizing memory consumption on the Cortex-M4 architecture. Operationally, the client functions as a deterministic finite state machine (FSM), navigating through distinct operational phases including IDLE, HANDSHAKE_INIT, HANDSHAKE_PROVE, and CONNECTED, a design choice that guarantees resilient recovery and re-synchronization in the presence of network instability.

To comprehensively validate the performance parameters of the proposed security paradigm, an exhaustive benchmarking methodology was applied, combining a high-concurrency client simulator for macroscopic system

metrics with the physical Arduino hardware for precise micro-benchmarking. Profiling of the cryptographic execution costs on a standard x64 server architecture revealed exceptional operational efficiency, with small-payload Ascon-128a encryption executing in approximately 305 ns, ECDH shared secret derivation requiring roughly 67 µs, TESLA MAC generation consuming 330 ns, and HKDF key derivation completing in 936 ns. These granular metrics definitively prove the server's capacity to simultaneously process thousands of device handshakes without inducing latency bottlenecks. Corresponding micro-benchmarks on the Arduino Uno R4 client demonstrated that Ascon encryption for a standard 16-byte payload necessitates approximately 1.2 ms, a processing duration that easily satisfies the operational constraints of nodes transmitting periodic telemetry. At the macroscopic level, system-wide evaluations driven by a Go-based concurrent simulator indicated a median (p50) end-to-end data packet latency of 0.28 ms, excluding physical network propagation, alongside a 95th percentile (p95) latency of 0.54 ms. Furthermore, continuous stream testing verified a sustained throughput capacity of approximately 8.2 packets per second for each simulated connection, while the complete three-way ECDH negotiation sequence demanded an average of merely 4.57 ms in server-side processing time.

The stark contrast in computational overhead between asymmetric and symmetric operations is visually corroborated in figure 2, which demonstrates the microsecond-level latency of Ascon and TESLA compared to the heavier ECDH operations.

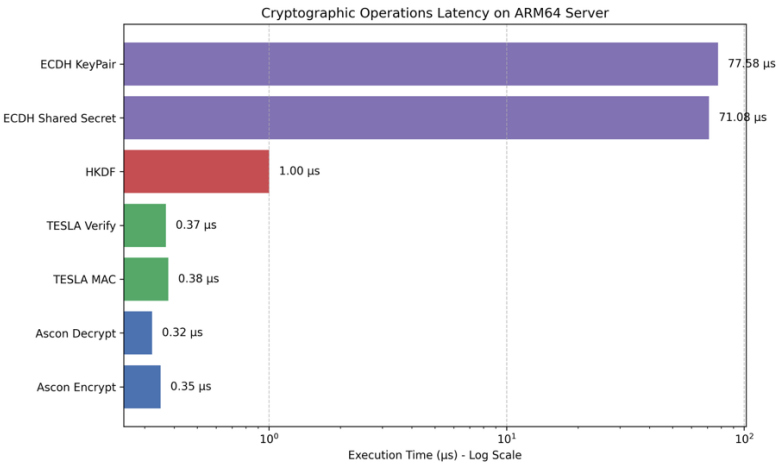


Fig. 2. Cryptographic operations latency on the ARM64 server

Furthermore, the macroscopic scalability of the proposed architecture is illustrated in figure 3, confirming the server's capability to sustain high throughput even as the number of concurrent IoT devices scales to 1000.

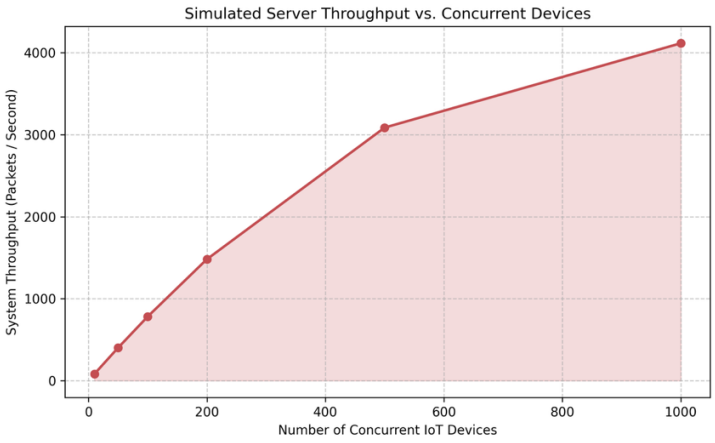


Fig. 3. Simulated server throughput versus concurrent devices

Finally, the architectural resilience was subjected to a battery of automated security validations to rigorously assess threat mitigation capabilities. The implemented sliding window mechanism demonstrated absolute efficacy against replay attacks, successfully rejecting 100 % of injected packets carrying duplicate sequence numbers. The protective capacity of the RFF module was confirmed through the deliberate injection of transmission vectors deviating from established baselines; anomalies exceeding the ThresholdWarm parameter were systematically discarded during the

HELLO_PROVE stage before expensive ECDH/HKDF operations, validating the physical layer's role as a highly efficient, energy-preserving gatekeeper. Similarly, any attempts to introduce modified MAC tags or manipulated ciphertexts were instantly identified and neutralized by the TESLA verification and Ascon decryption routines, confirming robust tamper resistance. Analysis of the computational footprint further corroborated the protocol's suitability for constrained environments: the entirety of the compiled client firmware, encompassing the SDK, cryptographic primitives, and the LoRa library, consumed approximately 48 KB of Flash memory. Simultaneously, the runtime SRAM utilization was restricted to roughly 6 KB out of the available 32 KB on the Arduino Uno R4, thereby preserving substantial computational resources for the execution of the primary IoT application logic.

Conclusions and Future Research. The widespread deployment of IoT ecosystems throughout critical infrastructure is intrinsically dependent on the capabilities of Low-Power Wide-Area Networks (LPWAN). Despite this reliance, the profound operational limitations characterizing «Arduino-class» microcontrollers specifically regarding their computational throughput and energy reserves render conventional cryptographic standards like DTLS fundamentally impractical [2; 4; 5]. To resolve this systemic vulnerability, the present investigation successfully formulated and empirically substantiated a multi-tiered, cross-layer security architecture specifically optimized for resource-deprived environments. The central accomplishment of this dissertation lies in the articulation of a defense-in-depth framework that spans three primary network strata, thereby guaranteeing that the exploitation of a single layer does not precipitate a catastrophic failure of the entire communication infrastructure [18]. This proposed methodology systematically neutralizes both digital intrusions and physical exploitation vectors without violating the stringent resource parameters mandated by LPWAN edge deployments.

Operating at the foundational hardware level, the proposed system introduces a Radio Frequency Fingerprinting Gate, which functions as a highly optimized, preemptive barrier against physical device cloning [16]. By computing the Euclidean distance between the extracted analog signal metrics namely the Frequency Error, Signal-to-Noise Ratio, and Received Signal Strength Indicator and an established Exponentially Weighted Moving Average profile, the architecture decisively intercepts unauthorized transmissions prior to the initiation of energy-intensive cryptographic operations. Subsequently, the Transport Layer establishes a secure communication conduit through a highly refined Elliptic Curve Cryptography [21] negotiation, specifically relying upon the Curve25519 (X25519) algorithm [22; 23]. This phase enforces perfect forward secrecy via the dynamic generation of ephemeral keys and the subsequent derivation of session parameters utilizing HKDF [24], while concurrently mitigating DOS vulnerabilities through the implementation of stateless server cookies [13]. Advancing to the Application Layer, the framework incorporates the Ascon-128a cipher to facilitate lightweight authenticated encryption, thereby strictly preserving the confidentiality and integrity of telemetry data [25]. Parallel to this, the architecture circumvents the massive computational burden typically associated with per-packet asymmetric signatures by integrating an adapted TESLA mechanism, which leverages a delayed-disclosure strategy to execute resource-efficient broadcast authentication [19].

To rigorously evaluate the theoretical constructs of this security paradigm, an exhaustive empirical analysis was conducted utilizing a comprehensive full-stack prototype. This experimental setup featured an Arduino Uno R4 WiFi edge node, powered by a Cortex-M4 processor, interfacing over a LoRa physical layer with a centralized server engineered in the Go programming language. The resulting benchmarking metrics definitively validated the architecture's suitability for profoundly constrained operational contexts. From a memory utilization perspective, the complete client-side firmware required a remarkably minimal footprint of only 48 KB of Flash memory and approximately 6 KB of runtime SRAM, thereby preserving a substantial capacity for the execution of primary IoT business logic. Furthermore, cryptographic micro-benchmarking revealed outstanding processing velocities, evidenced by client-side Ascon encryption executing in merely 1.2 ms. Concurrently, the central server demonstrated the capacity to process thousands of simultaneous connections without introducing systemic latency, as highlighted by Ascon encryption times of approximately 305 ns and ECDH shared secret derivations requiring only 67 µs. The system also exhibited robust macroscopic network performance, sustaining a throughput of 8.2 packets per second per individual connection and maintaining a median end-to-end packet latency of just 0.28 ms, thereby confirming that the imposition of rigorous security protocols does not intrinsically degrade network agility.

The theoretical integrity of the proposed framework was further corroborated through a series of automated security validations and comprehensive threat modeling scenarios. During these evaluations, the implemented sliding window mechanism achieved a 100 % success rate in identifying and discarding sequence-manipulated replay attempts. In parallel, the hardware-centric RFF module proved highly reliable in consistently isolating and rejecting anomalous analog transmission vectors. Moreover, the integrated Ascon and TESLA verification routines successfully intercepted and neutralized all simulated instances of ciphertext tampering and MAC manipulation. Ultimately, the cumulative findings of this dissertation firmly establish that the provision of comprehensive, enterprise-level security within LPWAN topologies does not necessitate the deployment of computationally burdensome, traditional cryptographic suites. By synergistically combining physical-layer attributes with advanced, lightweight cryptographic primitives, the proposed cross-layer paradigm effectively establishes a novel and highly resilient standard for defending heavily constrained IoT infrastructures against complex, multi-vector adversarial campaigns.

Building upon the foundational framework established in this paper, future research endeavors will focus on advancing the scalability, adaptability, and long-term resilience of the proposed architecture. As a primary trajectory for future work, the integration of lightweight machine learning algorithms specifically TinyML paradigms into the Radio Frequency Fingerprinting module will be rigorously investigated. While recent studies have demonstrated the efficacy of Siamese neural networks for RFF authentication in IoT environments [17], their deployment on profoundly constrained «Arduino-class» microcontrollers remains an open challenge that requires further optimization of model architectures and inference engines.

References:

1. LoRa Alliance (2020), *LoRaWAN 1.0.4 Specification (TS001-1.0.4)*, [Online], available at: https://resources.lora-alliance.org/technical-specifications/ts001-1-0-4-lorawan-l2-1-0-4-specification
2. Alimi, O.A., Ouahada, K., Abu-Mahfouz, A.M. and Rimer, S. (2020), «A Survey on the Security of Low Power Wide Area Networks: Threats, Challenges, and Potential Solutions», *Sensors*, Vol. 20, No. 20.
3. Torres, N., Pinto, P. and Lopes, S.I. (2021), «Security Vulnerabilities in LPWANs—An Attack Vector Analysis for the IoT Ecosystem», *Applied Sciences*, Vol. 11, No. 7.
4. Rescorla, E., Tschofenig, H. and Modadugu, N. (2022), *RFC 9147: The Datagram Transport Layer Security (DTLS) Protocol Version 1.3*, Internet Engineering Task Force (IETF), doi: 10.17487/RFC9147.
5. Perrig, A., Szewczyk, R., Tygar, J.D. et al. (2002), «SPINS: Security Protocols for Sensor Networks», *Wireless Networks*, Vol. 8, No. 5, pp. 521–534.
6. Roman, R., Zhou, J. and Lopez, J. (2013), «On the features and challenges of security and privacy in distributed internet of things», *Computer Networks*, Vol. 57, No. 10, pp. 2266–2279, doi: 10.1016/j.comnet.2012.12.018.
7. Granjal, J., Monteiro, E. and Silva, J.S. (2015), «Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues», *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 3, pp. 1294–1312, doi: 10.1109/COMST.2015.2388550.
8. Sicari, S., Rizzardi, A., Grieco, L.A. and Coen-Porisini, A. (2015), «Security, privacy and trust in Internet of Things: The road ahead», *Computer Networks*, Vol. 76, pp. 146–164, doi: 10.1016/j.comnet.2014.11.008.
9. *Advanced Encryption Standard (AES)*. Series. *NIST Federal Information Processing Standards Publication (FIPS 197)* (2001), National Institute of Standards and Technology.
10. Aras, E., Ramachandran, G.S., Lawrence, P. and Hughes, D. (2017), «Exploring the Security Vulnerabilities of LoRa», *3rd IEEE International Conference on Cybernetics (CYBCONF)*, pp. 1–6, doi: 10.1109/CYBConf.2017.7985777.
11. Eldefrawy, M., Butun, I., Pereira, N. and Gidlund, M. (2019), «Formal Security Analysis of LoRaWAN», *Computer Networks*, Vol. 148, pp. 328–339, doi: 10.1016/j.comnet.2018.11.017.
12. Ntshabele, K., Isong, B., Gasela, N. and Abu-Mahfouz, A.M. (2022), «A Comprehensive Analysis of LoRaWAN Key Security Models and Possible Attack Solutions», *Mathematics*, Vol. 10, No. 19, doi: 10.3390/math10193421.
13. Pathak, G., Gutierrez, J., Ghobakhlou, A. and Ur Rehman, S. (2022), «LPWAN Key Exchange: A Centralised Lightweight Approach», *Sensors*, Vol. 22, No. 13, doi: 10.3390/s22135065.
14. Sravan, S.S., Mandal, S. and Alphonse, P.J.A. (2025), «SDSMS-LoRa: secure dynamic session key management scheme for LoRaWAN v1.1», *The Journal of Supercomputing*, Vol. 81, 371 p., doi: 10.1007/s11227-024-06802-6.
15. *Lightweight Cryptography Standardization Process: NIST Selects Ascon* (2023), National Institute of Standards and Technology (NIST), [Online], available at: https://www.nist.gov/news-events/news/2023/02/lightweight-cryptography-standardization-process-nist-selects-ascon
16. Soltanieh, N., Norouzi, Y., Yang, Y. and Karmakar, N.C. (2020), «A Review of Radio Frequency Fingerprinting Techniques», *IEEE Journal of Radio Frequency Identification*, Vol. 4, No. 3, pp. 222–233, doi: 10.1109/JRFID.2020.2968369.
17. Dhakal, R., Kandel, L.N. and Shekhar, P. (2025), «Radio Frequency Fingerprinting Authentication for IoT Networks Using Siamese Networks», *IoT*, Vol. 6, No. 3, doi: 10.3390/iot6030047.
18. Mustafa, R., Sarkar, N.I., Mohaghegh, M. and Pervez, S. (2024), «A Cross-Layer Secure and Energy-Efficient Framework for the Internet of Things: A Comprehensive Survey», *Sensors*, Vol. 24, No. 22, doi: 10.3390/s24227209.
19. Perrig, A., Canetti, R., Tygar, J.D. and Song, D. (2002), «The TESLA Broadcast Authentication Protocol», *RSA CryptoBytes*, Vol. 5, No. 2, pp. 2–13.
20. Garcia, J.C.P., Benslimane, A., Braeken, A. and Su, Z. (2023), «μTesla-based Authentication for Reliable and Secure Broadcast Communications in IoD using Blockchain», *IEEE Internet of Things Journal*, Vol. 10, No. 20, pp. 18400–18413, doi: 10.1109/JIOT.2023.3280124.
21. Koblitz, N. (1987), «Elliptic Curve Cryptosystems», *Mathematics of Computation*, Vol. 48, No. 177, pp. 203–209, doi: 10.2307/2007884.
22. Bernstein, D.J. (2006), «Curve25519: New Diffie-Hellman Speed Records», *Public Key Cryptography – PKC 2006*, Lecture Notes in Computer Science, Vol. 3958, pp. 207–228, doi: 10.1007/11745853_14.
23. Langley, A., Hamburg, M. and Turner, S. (2016), *RFC 7748: Elliptic Curves for Security*, Internet Engineering Task Force (IETF), doi: 10.17487/RFC7748.
24. Krawczyk, H. and Eronen, P. (2010), *RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*, Internet Engineering Task Force (IETF), doi: 10.17487/RFC5869.
25. Dobraunig, C., Eichlseder, M., Mendel, F. and Schläffer, M. (2021), «Ascon v1.2: Lightweight Authenticated Encryption and Hashing», *Journal of Cryptology*, Vol. 34, No. 3, 33 p., doi: 10.1007/s00145-021-09398-9.

Чернявський Богдан Вадимович – аспірант Дніпровського національного університету імені Олеся Гончара.

https://orcid.org/0009-0006-3933-1423.

Наукові інтереси:

– легковагова криптографія в IoT та LPWAN;
– апаратна безпека;
– вбудовані системи та периферійні обчислення.

Чернявський Б.В.

Міжрівнева безпека IoT з використанням радіочастотних відбитків та легковагової криптографії

У роботі розглянуто результати дослідження протоколу безпеки для IoT пристроїв у LPWAN середовищі. Для перевірки гіпотези було розроблено і верифіковано гібридний протокол з використанням радіочастотних відбитків (RFF), TESLA та легковагового методу шифрування Ascon-128a. Отримано експериментальні результати на 8 та 32-бітних контролерах, arm64 платформі. Цей підхід до захисту передачі даних забезпечує належний рівень комплексного захисту за умови мінімальних обчислювальних ресурсів і незначних затримок передачі. Архітектурний підхід демонструє здатність ефективно протистояти атакам на клонування і повторного відтворення, ще без сумнівів є критично важливим у бездротових мережах. Особливу увагу приділено проблемі обмеженості ресурсів у LPWAN-системах, де застосування традиційних протоколів DTLS є недоцільним та ресурсним, а в деяких випадках технічно неможливим, оскільки використовуються складні операції на базі RSA алгоритму для узгодження AES ключів. Такий підхід використовує майже всі ресурси на узгодження мережі і спонукає використовувати більш дорогі контролери для досягнення потрібного рівня безпеки в промислових рішеннях. Практична реалізація була побудована на платформі Arduino Uno R4 WIFI з використанням бібліотеки LoRa та серверним компонентом, розробленим мовою Go для обчислювальної архітектури ARM64, що підтвердило гіпотезу. На етапі системної інтеграції було спроєктовано специфічні методи синхронізації, спрямовані на запобігання часової девіації в роботі протоколу TESLA, а також алгоритми деривації радіочастотних відбитків із залученням рівня абстракції бази даних. Профілювання на платформі Arduino доводить високу ефективність підходу з мілісекундними транзакціями та мінімальними споживаннями пам’яті, а використання радіочастотних відбитків дозволяє надійно блокувати зловмисний трафік ще до початку роботи ресурсних криптографічних перевірок.

Ключові слова: безпека IoT; LPWAN; радіочастотні відбитки; Ascon; TESLA; міжрівнева безпека.

The article was sent to the editorial board on 30.12.2025.