A Lightweight Identity Authentication Protocol for Nano-Scale IoT Devices

Batool Mohammed Radhi
Department of Community Health Technologies, Medical Technical Institute, Southern Technical University, Basrah, Iraq
batool.m.radhi@stu.edu.iq

Abdalrahman Fatikhan Ataalla
Department of Computer Engineering Techniques, College of Technical Engineering, University of Al Maarif, Al Anbar, Iraq
engrahumi@uoa.edu.iq

Huda Mohammed Alsayednoor
Shatt Al-Arab University College, Basra, Iraq
huda1994noor@gmail.com

Mahmood A. Al-Shareeda
Department of Information Technology, Management Technical College, Southern Technical University, Basrah, Iraq | College of Engineering, Al-Ayen University, Thi-Qar, Iraq
mahmood.alshareedah@stu.edu.iq (corresponding author)

Mohammed Amin Almaiah
Department of Computer Science, King Abdullah the II IT School, The University of Jordan, Amman, Jordan
m.almaiah@ju.edu.jo

Mansour Obeidat
Applied College, King Faisal University, Al-Ahsa, Saudi Arabia
Mobaydat@kfu.edu.sa

Received: 16 July 2025 | Revised: 14 August 2025 | Accepted: 20 August 2025

 DOI: https://doi.org/10.48084/etasr.13449

ABSTRACT

The nano-scale Internet of Things (nano-IoT) is ushering in a new era of applications in areas such as biomedical sensing, smart dust, and embedded environmental monitoring. Unfortunately, the utilization of nano-devices is barely feasible because of their very limited energy, computation, memory, and communication bandwidth, making existing cryptographic authentication methods infeasible. This study introduces an ultra-lightweight identity authentication protocol designed for nano-IoT systems with limited resources. The proposed protocol uses symmetric key cryptography, one-way hash functions, and XOR operations to achieve mutual authentication with low computational and communication costs. A highly modular architecture is proposed, consisting of 4 main stages: cryptographically secure pre-loading of credentials, a hash-based mutual authentication scheme, a stateless session update mechanism using hash chains and nonces, and a gateway-level revocation enforcement model. In contrast to PUF- or ECC-based protocols, the proposed protocol is extremely resistant to impersonation, replay, man-in-the-middle, desynchronization, and side-channel attacks without requiring special hardware. Simulations in nano-IoT settings show that the proposed protocol is more than 8 times faster and 11 times more energy-efficient than public-key-based algorithms, with high scalability and robust security. This study offers a solid basis for the secure bootstrapping of the forthcoming nano-IoT in dynamic, low-power, and latency-constrained environments.

Keywords-nano-IoT; ultra-lightweight authentication; identity management; low-power cryptography; secure nano-communication; pseudonymous devices; stateless protocols; energy-efficient security; hash-based authentication; mutual verification

I. INTRODUCTION

The explosive growth of IoT has dramatically changed the landscape of modern computing, demanding ubiquitous connections and intelligent controls for a variety of settings [1-3]. As this paradigm continues to develop, macro- and micro-scale devices are being replaced by nano-scale IoT (Nano-IoT) systems—networks of ultra-small, typically embedded, computer nodes that function in highly constrained and sensitive environments [4, 5]. These range from in vivo medical implants to smart dust and from environmental nano-sensors to embedded materials for industrial structures. Apart from being challenging, yet revolutionary, the nano-IoT has extreme limitations on energy, memory, computation, and communication [6, 7]. These quick memory depletions cripple one of the critical components of such systems—secure and efficient identity verification [8, 9].

Classical cryptographic techniques, especially those based on asymmetric cryptography (e.g., RSA, ECC), are computationally and energy-intensive, thus not suitable for nano-devices [10-13]. Even lightweight expressions of cryptographic primitives and mutual authentication schemes designed for traditional IoT often are too computation-intensive and power-hungry for devices with kilobyte-scale memory and microjoule energy capacity. In addition, the dynamic, intermittent, and sometimes lossy communication medium in which nano-IoT systems function contributes to further risks from desynchronization, replay, and session attacks [14-16]. In such situations, the authentication protocols should not only ensure mutual trust and message integrity, but also resist timing drift, energy resets, and passive eavesdropping without overwhelming the device resources [17].

With nano-IoT, attacks are mostly on sensors at the location where the data is generated. Attackers can inject false readings, clone identities, or intercept transmissions before they reach the gateways, without local authentication and integrity checks. Due to their limited resources and the harsh environments in which they are often deployed, nano-devices depend on sensor-level security that is both lightweight and robust enough to enforce trusted data collection and system integrity. In light of such strict requirements, this study proposes an ultra-lightweight identity authentication protocol specifically designed for nano-IoT applications. This protocol is intended to securely work under the heavy computation and power constraints of Nano-IoT devices, using lightweight hash functions and primitive XORs for mutual authentication and session freshness. The system does not depend on computation-heavy PKI operations and uses a method of symmetric key pre-distribution, nonce-based session identifiers, and one-way hash chains for rekeying. This method not only can reduce the load of communication and storage, but can also withstand several popular attacks such as impersonation, replay, Man-In-The-Middle (MITM), and desynchronization. The main contributions of the proposed Nano-IoT ultra-lightweight identity authentication protocol are:

- A four-factor authentication process involving secure pre-loading, lightweight mutual authentication, stateless session refresh, and gateway-initiated revocation, leveraging the resources of ultra-constrained devices such as PRESENT-80 or LFSR-based hash functions.
- Strong session continuity support, including: (i) nonce handling, (ii) hash chain-based key renewal, and (iii) triggered resets. Lightweight but effective revocation mechanisms move the burden of verification to more powerful gateways and save energy on nano-devices.

II. RELATED WORKS

Nano-IoT authentication has become a hot research area based on the demand for security in ultra-constrained environments. Security is undoubtedly the main asset of recent approaches, and resource consumption is the only drawback [18-20]. In [21], a UAV-aided PUF-based authentication and KAP protocol was proposed for unattended IoT scenarios, with an emphasis on both lightweight and physical tamper-proof features. In [22], a PUF-based mutual authentication and key agreement protocol was designed for IoT/IoMT. Based on the ASCON AEAD cipher and formal ProVerif verification, this protocol offers strong security and has low communication (912 bits) and storage (128 bits) overheads. In [23], a three-phase IoT authentication protocol used a hybrid ECC-AES encryption scheme, enhanced by a Self-improved Aquila Optimizer for key generation. In [24], a blockchain-based mutual authentication protocol was proposed for the IoT, using smart contracts on Hyperledger Fabric, BAN logic, and ProVerif validation, and providing secure and efficient communication. In [25], a novel biometric-based and noise-tolerant secure authentication protocol was proposed for IoT, using CRNs to generate the "PUF Phenotype" information, which is different from traditional error correction.

In [26], an ECC mutual authentication protocol was proposed for IoT-Fog-Cloud environments, focusing on energy management and sustainability. In [27], a deep learning-enabled AKA protocol was proposed for IoT-enabled LTE networks, using the DRN-KeyGen technique for dynamic key generation. This protocol provided mutual authentication and protected against active/passive attacks. In [28], a lightweight PUF-based protocol was proposed to provide ongoing and mutual authentication for IoT devices, using only hash, XOR, and symmetric encryption to ensure confidentiality, integrity, and anonymity. In [29], a lightweight key-sharing protocol was proposed for secure IoT applications. REMIDLGKM [30] is a lightweight decentralized group key management and multicast routing approach for IoT networks that improves security, scalability, and efficiency through a cluster-based design. In [31], the PUF-RLA protocol was proposed, showing good resilience against cloning and impersonation attacks, but not suitable for resource-constrained systems, as it requires special hardware to implement PUF, adding overhead to the architecture and increasing cost.

In [32], a PUF and entropy token-based drone-to-drone authentication scheme was proposed. Although this approach is efficient for a UAV-class IoT device, it is not suitable for Nano-IoT devices due to the relatively high energy and space complexity. EBIAS [33] is an ECC-based identity authentication protocol developed over blockchain, providing strong cryptographic security and revocation capabilities at the cost of high computational overhead, much of which is bottlenecked on elliptic curve operations and the process of synchronizing with the blockchain.

The proposed protocol provides a suitable balance of security and efficiency for Nano-IoT based on symmetric keys, lightweight hashes, and XOR operations with the additional property of desynchronization resilience. As of now, its disadvantages, i.e., pre-deployed provisioning, gateway-based revocation, and optional anonymity, reduce the applicability; however, it is still a strong candidate for constrained biomedical and smart dust-like applications.

III. PRELIMINARIES

Figure 1 shows a high-level model of the proposed ultra-lightweight authentication system in the context of Nano-IoT.

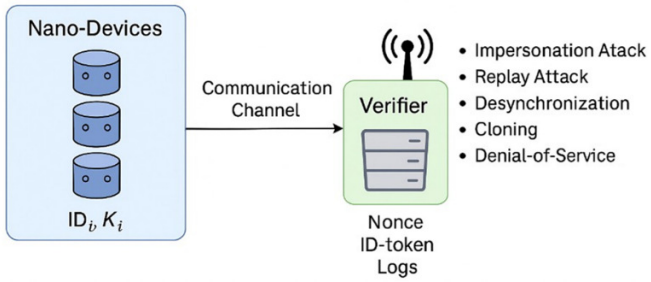

Fig. 1. System model.

A. System Model

The system consists of the following entities:

- Nano-device D_i : A fully-fledged but ultra-constrained computing device that can perform basic computation (bitwise operations, hashing) and low-power wireless communication. Each device is pre-loaded with a unique ID ID_i and a shared secret key K_i.
- Verifier node: A high-resource gateway for verifying nano-devices. It stores the mapping of identity and the token, issuing nonces, validating the response on the way back, and can optionally handle revocation or re-authentication.
- Communication channel: A wireless or near-field communication medium for the exchange of authentication.

Key assumptions: (i) Devices have no space to store large tables or perform complex cryptography (ECC or RSA); (ii) Gateways are semi-trusted and log for anomaly detection and revocation enforcement; (iii) Time synchronization of nano devices is poor or nonexistent with gateways.

B. Threat Model

Adversaries are passive or active and can consist of eavesdroppers, rogue devices, or compromised intermediaries. Specific threats include:

- Impersonation attacks: An attacker tries to cheat by presenting itself as a lifelike D_i to create unauthorized access. Challenge-response verification tied to secret keys and one-time nonces in the protocol counteract this.
- Replay attacks: The attacker uses a valid authentication response that was used earlier. The invalidity of such an attempt is ensured by using nonce-based freshness and session expiration time.
- Man-in-the-Middle (MITM): An adversary directly interferes with the messages exchanged between a device and the verifier. The protocol alleviates this by end-to-end hashing of secrets and nonces.
- Desynchronization attack: Multiple false attempts can introduce a device or verifier to mismatched session states. The protocol is device stateless and relies on verifier-managed recovery tokens to re-synchronize.
- Cloning and device photocopying: An attacker could attempt to clone a device's identity. As the key is unique and never transmitted, and freshness is ensured using hash-chain-based updates, the clones are rejected during authentication.
- Denial of Service (DoS): Chronic requests are used to deplete the resources of a device or its gateway. A rate control applied at the gateway and reduced device-side processes will limit DoS attacks.

IV. PROPOSED AUTHENTICATION PROTOCOL

This framework does not rely on heavy cryptographic operations and provides secure identity verification and mutual trust establishment between nano-devices and their gateways. The protocol relies on a sequence of four main phases:

1. A setup phase for securely pre-loading each device with a symmetric key and an identifier.
2. A mutual authentication phase based on lightweight hash and XOR operations.
3. A refresh mechanism that maintains freshness and mitigates risks of desynchronization.
4. A revocation support strategy that involves key expiry, passive filtering, and detection of behavioral anomalies.

Figure 2 presents the complete authentication flow, involving device bootstrapping, validation, and session refresh, visually capturing the complete protocol logic. Table I presents the formal mathematical model of the proposed Nano-IoT ultra-lightweight identity authentication protocol, covering mutual authentication, session key update, and revocation conditions.

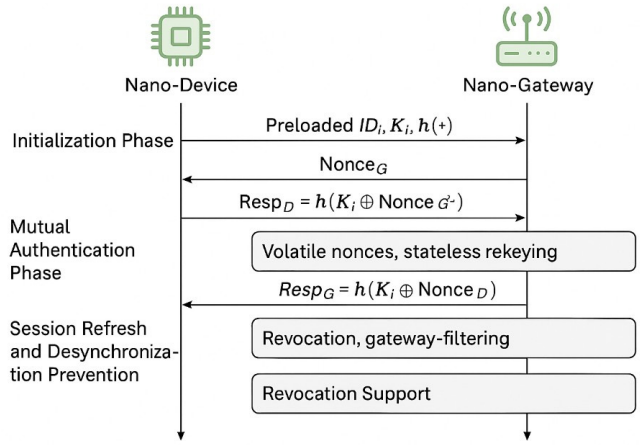

Fig. 2. Diagram illustrating the entire protocol flow.

TABLE I. PROPOSED NANO-IOT ULTRA-LIGHTWEIGHT PROTOCOL

Step	Operation	Expression
1	Device sends ID	$D_i \rightarrow G : ID_i$
2	Gateway sends nonce	$G \rightarrow D_i : N_G$
3	The device computes the response	$R_D = h(K_i \oplus N_G)$
4	Gateway verifies	Verify $R_D = h(K_i \oplus N_G)$
5	Device sends nonce	$D_i \rightarrow G : N_D$
6	Gateway computes the response	$R_G = h(K_i \oplus N_D)$
7	Device verifies	Verify $R_G = h(K_i \oplus N_D)$
8	Session key update	$K_i^{(t+1)} = h(K_i^t)$
9	Revocation check	If $c_i > c_{max}$ or ID_i in RL, revoke D_i

A. Initialization Stage

The initialization state sets out the pre-deployment configuration needed to support the secure authentication of nano-range IoT devices. Due to severe resource limitations in computation, memory, and energy, this phase attempts to minimize the complexity of cryptographic primitives as much as possible while maintaining confidentiality and uniqueness. The following steps are performed as part of secure provisioning, generally during manufacture or trusted enrollment:

1. Assignment of device identifier: Each nano-device D_i is provided with a serial number ID_i that can be programmed either in the factory or during manufacturing. This ID is transmitted when using the handshake to announce the existence of the device.
2. Symmetric key distribution: A small symmetric key K_i and its associated nano-gateway (or verifier) are pre-installed in (or loaded to) the device. This key can be obtained by hashing the device ID or by using a secure random number generator.
3. Parameterization of the hash function: The device is implemented with an ultra-small hash function $h(\cdot)$, such as PRESENT-80 or a hardware-efficient LFSR-based one-way function. This function is used to produce response codes without costly arithmetic operations.
4. Nonce generation setup: The device includes a Pseudorandom Number Generator (PRNG) or a counter to produce new nonces or session randomness that protect against freshness and replay attacks while authenticating.
5. Key validity encoding (optional): To enable revocation and re-authentication mechanisms, an expiration timer or usage counter could be embedded, so that a verifier can determine that the credential has expired or has been too heavily reused, without the need for stateful synchronization. Table II summarizes the primitives employed, their parameters, and the justification for their selection.

TABLE II. PRIMITIVES AND PARAMETERS

Primitive	Parameters	Purpose	Justification for Nano-IoT Use
Symmetric key K_i	80 bits	Shared secret between device D_i and gateway G	80-bit keys provide adequate security for short-lived sessions while requiring minimal memory (10 bytes).
One-way hash $h(\cdot)$	PRESENT-80 or LFSR-based, 80-bit output	Response computation, key updates	PRESENT-80 and hardware-efficient LFSR hash are proven lightweight, with gate count < 2,000 and negligible energy use.
Bitwise XOR $\oplus$	N/A	Mixing key and nonce	Requires only 1 CPU cycle, ideal for constrained devices.
Nonce N_G, N_D	64 bits	Session freshness, replay prevention	64-bit PRNG-generated nonces balance security and minimal transmission overhead.
PRNG	LFSR-based or hardware PRNG	Nonce generation	Provides adequate randomness at extremely low energy cost.

B. Mutual Authentication Phase

The mutual authentication phase ensures that the nano-device D_i and the gateway verifier G authenticate each other without using computationally expensive cryptographic primitives, as shown in Figure 3. With symmetric key operations, one-way hash functions, and reduced communication cost, the protocol realizes a mutual trust relationship between the two sides under scarce resource consumption. The protocol goes like this:

1. Device initiation: The nano-device D_i initiates the session by transmitting its pseudonymous identifier: $D_i \rightarrow G: ID_i$.
2. Verifier challenge: Upon receiving the identifier, the verifier G generates a random nonce $Nonce_G$ and sends it back to the device: $G \rightarrow D_i: Nonce_G$.
3. Device response: The device computes a response using the pre-shared key K_i and the received nonce: $Resp_D = h(K_i \oplus Nonce_G)$ and transmits the result: $Di \rightarrow G: Resp_D$.

4. Verifier authentication: The gateway computes the expected response using its stored key and verifies: $Expected_D = h(K_i \oplus Nonce_G)$. If $Resp_D = Expected_D$, D_i is authenticated.
5. Device challenge (optional): For mutual verification, D_i generates a nonce $Nonce_D$ and sends it: $D_i \rightarrow G: Nonce_D$.
6. Verifier response: The verifier computes and returns: $Resp_G = h(K_i \oplus Nonce_D)$ and $G \rightarrow D_i: Resp_G$.
7. Device verification: The device verifies the response by computing the same hash locally. If matched, mutual authentication is complete.

This phase ensures lightweight bilateral trust without requiring asymmetric operations or excessive communication, making it ideal for highly constrained nano-scale environments.

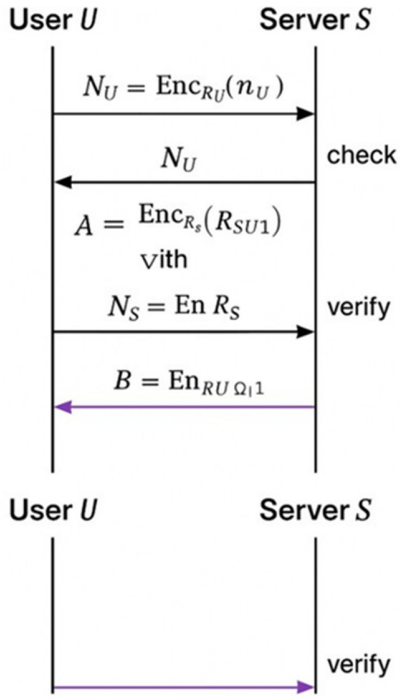

Fig. 3. Mutual authentication phase process.

C. Session Refresh and Desynchronization Avoidance

Since Nano-IoT devices can be extremely sensitive to timing drift, state loss, and even power failures, the protocol introduces resilience against desynchronization and stale session states. The goal is to provide stateless or semi-stateful fresh validation with minimum overhead. To this end, the following mechanisms are used:

1. Volatile nonce memory: A volatile, such as that used at the last nonce received/sent states, is mainly enabled on every device. It is written to the system's temporary volume, which is cleared when the system is rebooted, so that untreated long-term synchronization cannot occur.
2. Session freshness with nonce validity time interval: Verifiers only accept nonces and session tokens if they are within a freshness window, which can be a fixed time ΔT or a sequence window W of messages in the same session. This helps to prevent replay and delayed injection attacks.
3. Hash chain rekeying: Devices that maintain a master key are updated using a one-way hash chain. The stateless nature of this solution enables session keys to progress independently without the need for synchronization, maintaining forward secrecy.
4. Session expiration and stateless rekeying: Both devices and verifiers erase keys after a certain number of sessions or uses. Rekeying is performed implicitly every $cmax$ count, not requiring any dependency on wall-clock or synchronized clocks.
5. Resynchronization by triggered reset (Rg): In the case of an authentication failure or a key inconsistency, the verifier can trigger a reset procedure by sending a recovery nonce: $G \rightarrow Di: RESET\_TOKEN$. Receiving this, the device falls back to a fresher or a default key value kept in protected memory to allow safe rejoining. These mechanisms are used to ensure that the protocol operates even under situations of sporadic communication, energy resets, or timing drift (common in nanoscale settings). The protocol maintains session freshness without the need for long-term state on the nano-devices. When a request is authenticated, the new session key is comprised of:

$$K_i(t+1) = h\big(K_i(t)\big)K_i(t+1)$$

Through a one-way hash chain (guaranteeing forward secrecy), Nonces NGN_GNG and NDN_DND, combined with counters, give session-based randomness that avoids replay as well as desync. As the device holds no history of these session counters or timestamps, it immediately recovers after power loss; the gateway simply rekeys by sending a reset token with an untouched fresh nonce, securing the adopting device. This approach allows for synchronization-free clocks and persistent storage, which is perfect for the transient nano-IoT world.

D. Revocation Support

Revocation is an important and yet hard task in nano-scale IoT because of limited memory, energy, and communication capacities. Conventional revocation mechanisms (e.g., Certificate Revocation List - CLR and blacklists based on blockchain) are infeasible for nanodevices. To mitigate this, the proposed protocol incorporates ultra-lightweight revocation policies, delegating the verification and enforcement duty to gateway-level nodes. The revocation model comprises the following components:

1. Passive revocation with key expiry: Each device key K_i has an associated limit of use or validity counter $cmax$. When the device value is surpassed, the key has expired: if $c_i > c_{max}$, revoke K_i. In this manner, the device does not need to actively communicate for revocation.

2. Gateway-enforced access filter: Gateways keep a local revocation list or anomaly detection filter to refuse access to devices that exhibit unusual behavior (too much traffic, failed authentication). The proposed approach utilizes dynamic filters and does not add any storage requirement for nano-devices.
3. Matching of revocation tags: From time to time, gateways might send hashed revocation tokens to a token revocation service in the form: $Tag_r = h(ID_i)$. Devices that capture a tag matching their ID will self-deactivate or start the re-enrollment process.
4. Timely bounded session keys: Session keys are granted with an implicit timeout value. Devices need to re-auth within this time frame to be kept in a valid state. When a session times out, the nonconvexity verifier simply rejects the expired session without having to perform complicated state maintenance.
5. Behavioral anomaly-based revocation (optional): Regarding NGLPs, compromised or cloned devices can be identified by using statistical models to examine temporal or spatial patterns in systems that use those nano-gateways with machine learning capabilities. Known devices are automatically deauthorized without any on-device revocation logic.

These revocation mechanisms provide defense sustainability and fraud prevention, taking the limited resources of nano-scale devices into account, and ensure robust identity management for high-density nano-IoT deployments. The proposed approach automatically enforces revocation at the gateway level for nano-devices to avoid large-scale computation. Gateways have a local revocation list and use behavioral anomaly detection to detect compromised nodes. The gateways will block any further authentication from the revoked device and might also broadcast a signed revocation notice to neighboring gateways, ensuring network-wide propagation. Gateways can maintain synchronized revocation data to prevent any gateway from being a single point of failure, so other gateways can continue to function even if one is compromised. To scale, the revocation tags are disseminated in a hash form so that only the affected devices need to process them, leveraging this opportunity for efficient bandwidth utilization even in dense nano-IoT deployments.

V. SECURITY THREAT ANALYSIS

A. *Informal Security Analysis*

This examination considers both classical and nano-specific adversarial threats, focusing on the protocol's capacity to ensure confidentiality, availability, and integrity with constrained resources.

- Resistance to side-channel attacks: The proposed protocol was developed as a preliminary design to avoid side-channel leakage by only employing lightweight hash and XOR operations in constant time. The implementation is branch-free, and arithmetic operations are performed in non-constant time, mitigating both timing and simple power analysis attacks. Memory accesses do not deviate from a constant when traversing secret values, making the implementation resilient to both cache and electromagnetic analysis. The narrow code base also relaxes the physical hardening of hardware, which should be optionally masked or noise injected on gateways or more capable devices. The proposed design is thus able to resist many common side-channel vectors due to these design properties, without requiring extra dedicated security hardware.
- Protection against impersonation attacks: Each authentication flow is based on a newly challenged and responded mechanism from a nonce and a pre-shared symmetric key. Since the response is computed as a one-way hash, it is never transmitted or obtainable from public messages, and an adversary cannot forge a correct response. This allows for strong impersonation resistance even in the presence of passive monitoring.
- Replay attack mitigation: To prevent attackers from being able to replay messages that were valid before, the session contains a random nonce, $Nonce_G$, sent by the verifier into the session. Since the responses are tied to this nonce and will be validated against it immediately, an attacker cannot replay it or any other message. Validation is checked against the time window or by expiring based on the retry count.
- Requirement of mutual authentication orderliness: The optional mutual authentication is employed for the nano-device to authenticate the verifier (e.g., a gateway), serving the purpose of preventing MITM attacks. This step uses the same cryptographic primitives but in reverse order, ensuring that both sides authenticate themselves without the use of asymmetric operations.
- Through bypass of synchronized clocks and recourse to nonces, hash chains, and stateless key updates, the protocol is resistant to desynchronization attacks.
- Intermittent power supply, failure-tolerant communication, and fault recovery: Devices can re-establish security in dynamic nano-network environments.
- Anonymity and pseudonymity: Although the initiators are supposed to use a specific identifiers ID_i, the protocol can easily be modified to include privacy protection mechanisms, such as pseudonym rotation, hash identifiers, or group-based pseudonyms, but still the cryptographic primitives remain the same. This is for anonymizing and avoiding a trace across several sessions.
- Bitwise and side-channel attack resistance: All secret-dependent operations use hash functions and XOR operations that are constant-time, not sensitive to secret-dependent branches or memory accesses. Consequently, the protocol reduces the vulnerability of the system to timing and power analysis attacks.

B. *Security Comparison*

The security of the proposed scheme was compared with other recent schemes, including PUF-RLA [31], D2D-MAP [32], and the ECC-based EBIAS protocol [33], as shown in

Table II. EBIAS provides high security against impersonation, replay, and known cryptographic attacks, but comes with computational overhead as it requires elliptic curve operations, making it difficult to use in ultra-constrained nano-IoT nodes. In the proposed protocol, security and efficiency are balanced properly with hash/XOR-based operations and stateless management of session keys. Compared to PUF-based schemes that require dedicated hardware, this method has high scalability and good desynchronization resistance without external support. Moreover, optional pseudonymization and lightweight DoS/KCI attack protection further enhance the privacy guarantees over existing lightweight models; thus, it is capable of inclusion in future nanoscale IoT systems.

TABLE III. SECURITY FEATURE COMPARISON WITH RECENT WORKS

Security feature	**Proposed protocol**	**PUF-RLA [31]**	**D2D-MAP [32]**	**EBIAS [33]**
Mutual authentication	Yes	Yes	Yes	Yes
Replay attack resistance	Yes	Yes	Yes	Yes
MITM	Yes	Yes	Partial	Yes
Forward secrecy	Yes	Partial	Partial	Yes
Desynchronization resilience	Yes	No	No	Yes
PUF hardware dependency	No	Yes	Yes	No
Key freshness/ session update	Yes	Yes	Partial	Yes
Scalability in Nano-IoT	High	Medium	Medium	Medium
Hash/XOR-based simplicity	Yes	No	No	No
Anonymity/ ID obfuscation	Optional	No	No	Yes
Resistance to DoS attacks	Yes	Partial	No	Yes
Resistance to KCI attacks	Yes	No	No	Yes

VI. PERFORMANCE EVALUATION - SECURITY ANALYSIS

The proposed ultra-lightweight authentication protocol was examined in terms of computational efficiency, communication overhead, energy, and scalability, and was also compared with three leading recent lightweight identity schemes, namely PUF-RLA [20], D2D-MAP [21], and the ECC-based EBIAS [22]. The NS-3 and TinyOS simulation frameworks were used for the performance evaluation of the proposed protocol in a WSN constrained nano-IoT environment. The target devices used sub-milliwatt power and were simulated as 8-bit microcontrollers running at 16 MHz, with 4 KB of RAM and 32 KB of flash memory, being representative of biomedical and smart dust applications. The network topology consisted of 100–500 nano-devices using a lossy wireless channel whose packet error rate was set to [0.01, 0.05]. The communication links operate in a narrowband configuration at 250 kbps and a range of up to 10 m.

All baseline protocols (PUF-RLA, D2D-MAP, and EBIAS) were re-implemented according to the original descriptions for fair comparisons. Each test was performed 1000 times, and the mean values were recorded for authentication latency, message size, and energy consumption. To estimate energy use, the number of CPU cycles and transmission bytes were multiplied by per-cycle/bit energy costs from typical nano-device datasheets.

A. Computational Overhead

The proposed protocol showed exceptional computational efficiency, performing 1 full authentication in only 3.6 ms on limited Nano-IoT hardware. In contrast, EBIAS has a much heavier computation due to elliptic curve operations, requiring 29.4 ms. PUF-RLA and D2D-MAP present slightly higher latencies of 12.1 ms and 15.8 ms due to the need for entropy extraction and PUF-based challenge-response exchanges. As shown in Figure 4, the ultralight structure of the proposed scheme, composed of only XOR operations and hash functions, has a speed-up gain of up to 8× compared to ECC-based ones, making it very suitable for energy-limited and real-time nano-IoT scenarios.

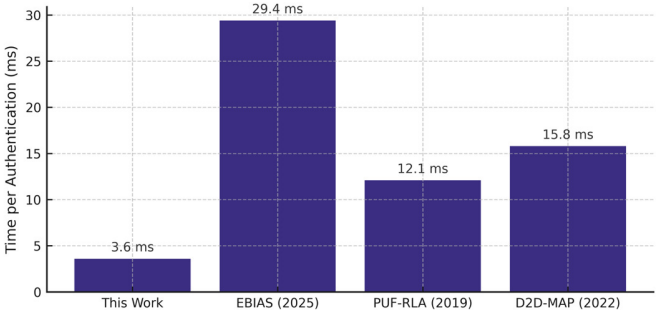

Fig. 4. Comparison of computational overhead.

B. Communication Overhead

The proposed protocol maintains a minimal communication footprint, transmitting just 112 bytes per authentication session. This efficiency stems from the compact challenge-response structure using hashed values and avoids large payloads such as public keys or digital signatures. In contrast, EBIAS transmits 240 bytes per session due to elliptic curve-based payloads. PUF-RLA and D2D-MAP exhibit moderately higher overheads at 160 and 140 bytes, respectively, due to PUF challenge exchanges and entropy disclosures. As shown in Figure 5, this reduction in transmitted data enhances compatibility with narrowband IoT channels and reduces latency in lossy nano-network environments.

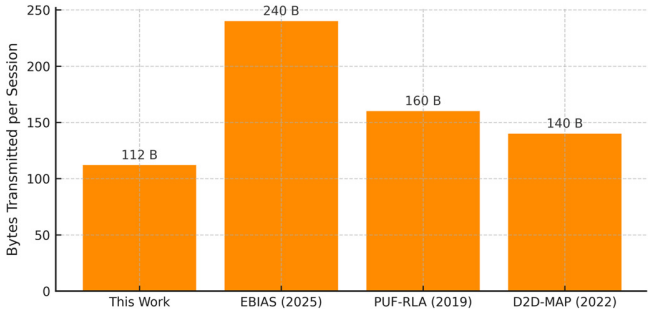

Fig. 5. Comparison of communication overhead.

C. Energy Consumption

The proposed scheme is highly energy efficient and requires only 0.4 µJ for one-time authentication, being suitable for power-limited nano-devices such as biosensors and smart dust. On the other hand, EBIAS needs around 4.5 µJ due to the ECC computation overhead. PUF-RLA and D2D-MAP consume 1.8 and 2.3 µJ, respectively, resulting from PUF hardware activations and multistep handshake operations. As Figure 6 illustrates, the proposed protocol is 11× more energy efficient than public-key-based schemes, thus it can operate in ultra-low-power nano-IoT contexts.

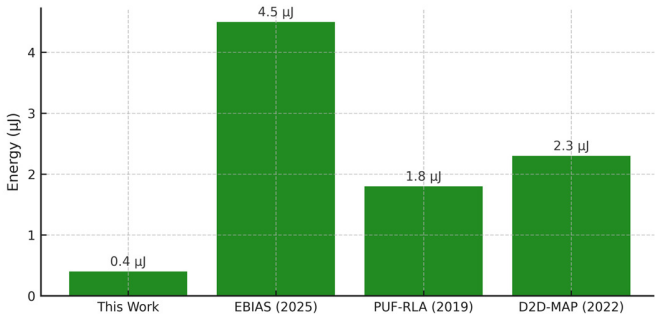

Fig. 6. Energy consumption per authentication session.

VII. CONCLUSION AND FUTURE WORK

This study proposed a new ultra-lightweight identity authentication protocol for nano-scale IoT scenarios. The proposed solution is also efficient under resource constraints, such as low energy and memory resources and limited processing capabilities, using only symmetric key primitives, lightweight hash functions, and XOR. Reliance on computationally expensive methods, such as public-key cryptography or PUFs, was eliminated, allowing realistic deployment to application contexts such as biomedical implants, smart dust, and embedded sensing. The architecture of the protocol consists of the following four basic phases: (i) Secure initialization, (ii) Mutual authentication, (iii) Stateless session refresh, and (iv) Gateway-assisted revocation. All phases are carefully engineered so that security is traded for performance with mutual trust, forward secrecy, desynchronization resilience, and revocation achieved without introducing state or storage requirements to the nano-devices. The incorporation of optional pseudonymity provides additional privacy, and adaptive revocation methods ensure long-term security and protection from cloning and behavioral anomalies. Extensive comparative analysis with existing competitive schemes, namely PUFRSLA, D2D-MAP, and EBIAS, showed that the proposed protocol performs much better in computational delay, communication overhead, and energy consumption, presenting a highly scalable and secure solution for dense, dynamic, and periodically connected nano-IoT networks.

Future work is planned to:

- Introduce a protocol correctness check.
- Include group-based authentication and zero-knowledge proofs for higher degrees of anonymity.
- Verify the protocol behavior in real nano-network emulation environments to test its performance under realistic noise, drift, and packet loss.
- Explore AI-powered gateway-level anomaly detection for more resistant revocation strategies that are context-aware.

The proposed protocol builds the necessary trust base for secure identity management in future generations of nano-IoT systems, supporting secure and sustainable deployment in a plethora of emerging cyber-physical applications.

REFERENCES

[1] K. Vijayvargia, P. Saxena, and D. S. Bhilare, "Context Management Life Cycle for Internet of Things: Tools, Techniques, and Open Issues," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19449–19459, Feb. 2025, https://doi.org/10.48084/etasr.9117.

[2] H. A. Naser, A. T. Lateef, F. A. Bida, and M. Zorah, "Systematic Review of Internet of Nano Things (IoNT) Technology: Taxonomy, Architecture, Open Challenges, Motivation and Recommendations," *Iraqi Journal of Nanotechnology*, no. 2, pp. 7–19, Dec. 2021, https://doi.org/10.47758/ijn.vi2.47.

[3] M. A. Al-Shareeda, A. A. H. Ghadban, A. A. H. Glass, E. M. A. Hadi, and M. A. Almaiah, "Efficient implementation of post-quantum digital signatures on Raspberry Pi," *Discover Applied Sciences*, vol. 7, no. 6, Jun. 2025, Art. no. 597, https://doi.org/10.1007/s42452-025-07201-z.

[4] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," in *2015 Internet Technologies and Applications (ITA)*, Wrexham, United Kingdom, Sep. 2015, pp. 219–224, https://doi.org/10.1109/ITechA.2015.7317398.

[5] K. R. Singh, V. Nayak, J. Singh, and R. P. Singh, "Nano-enabled wearable sensors for the Internet of Things (IoT)," *Materials Letters*, vol. 304, Dec. 2021, Art. no. 130614, https://doi.org/10.1016/j.matlet.2021.130614.

[6] L. H. Mahdi and A. A. Abdullah, "Fortifying Future IoT Security: A Comprehensive Review on Lightweight Post-Quantum Cryptography," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21812–21821, Apr. 2025, https://doi.org/10.48084/etasr.10141.

[7] A. S. Haichour and K. Benfriha, "Empowering Real-Time IoT Applications: A Brief Review on Leveraging GPU Acceleration for Latency Reduction," in *Internet of Things. 7th IFIPIoT 2024 International IFIP WG 5.5 Workshops*, 2025, pp. 107–120, https://doi.org/10.1007/978-3-031-82065-6_8.

[8] S. S. Ahmadpour, A. Heidari, N. J. Navimpour, M. A. Asadi, and S. Yalcin, "An Efficient Design of Multiplier for Using in Nano-Scale IoT Systems Using Atomic Silicon," *IEEE Internet of Things Journal*, vol. 10, no. 16, pp. 14908–14909, Dec. 2023, https://doi.org/10.1109/JIOT.2023.3267165.

[9] A. AlShuaibi, M. W. Arshad, and M. Maayah, "A Hybrid Genetic Algorithm and Hidden Markov Model-Based Hashing Technique for Robust Data Security," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 42–56, May 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.6.

[10] S. Majumder, S. Ray, D. Sadhukhan, M. K. Khan, and M. Dasgupta, "ECC-CoAP: Elliptic Curve Cryptography Based Constraint Application Protocol for Internet of Things," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1867–1896, Feb. 2021, https://doi.org/10.1007/s11277-020-07769-2.

[11] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of Internet of Things using RC4 and ECC Algorithms (Case Study: Smart Irrigation Systems)," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1713–1742, Feb. 2021, https://doi.org/10.1007/s11277-020-07758-5.

[12] Z. G. Al-Mekhlaf *et al.*, "A quantum-resilient lattice-based security framework for internet of medical things in healthcare systems," *Journal of King Saud University Computer and Information Sciences*, vol. 37,

no. 6, Jul. 2025, Art. no. 126, https://doi.org/10.1007/s44443-025-00140-0.

[13] B. A. Mohammed *et al.*, "Taxonomy-Based Lightweight Cryptographic Frameworks for Secure Industrial IoT: A Survey," *IEEE Internet of Things Journal*, 2025, https://doi.org/10.1109/JIOT.2025.3595649.

[14] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2649–2656, Oct. 2022, https://doi.org/10.1109/JIOT.2021.3080461.

[15] R. R. Irshad *et al.*, "IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Blockchain-Based Approach Toward a Trustworthy Cloud Computing," *IEEE Access*, vol. 11, pp. 105479–105498, 2023, https://doi.org/10.1109/ACCESS.2023.3318755.

[16] S. R. Addula, S. Norozpour, and M. Amin, "Risk Assessment for Identifying Threats, vulnerabilities and countermeasures in Cloud Computing," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 37–48, Mar. 2025.

[17] T. Alsalem and M. Amin, "Towards Trustworthy IoT Systems: Cybersecurity Threats, Frameworks, and Future Directions," *Journal of Cyber Security and Risk Auditing*, vol. 2023, no. 1, pp. 3–18, Feb. 2023, https://doi.org/10.63180/jcsra.thestap.2023.1.2.

[18] A. Rana, S. Prajapat, P. Kumar, D. Gautam, and C. M. Chen, "Designing a Security Framework Based on Hybrid Communication in Internet of Nano Things," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 7265–7284, Oct. 2024, https://doi.org/10.1109/JIOT.2023.3315712.

[19] A. Rana, D. Gautam, P. Kumar, and A. Kumar Das, "Architectures, Benefits, Security, and Privacy Issues of Internet of Nano Things: A Comprehensive Survey, Opportunities, and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 2, pp. 1152–1190, Apr. 2025, https://doi.org/10.1109/COMST.2024.3423477.

[20] H. Albinhamad, A. Alotibi, A. Alagnam, M. Almaiah, and S. Salloum, "Vehicular Ad-hoc Networks (VANETs): A Key Enabler for Smart Transportation Systems and Challenges," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 4–15, Feb. 2025.

[21] C. Tian, J. Ma, T. Li, J. Zhang, C. Ma, and N. Xi, "Provably and Physically Secure UAV-Assisted Authentication Protocol for IoT Devices in Unattended Settings," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4448–4463, 2024, https://doi.org/10.1109/TIFS.2024.3379861.

[22] K. Raj, S. Bodapati, and A. Chattopadhyay, "PUF-based Lightweight Mutual Authentication Protocol for Internet of Things (IoT) Devices," in *2024 IEEE International Symposium on Circuits and Systems (ISCAS)*, Singapore, May 2024, pp. 1–5, https://doi.org/10.1109/ISCAS58744.2024.10558672.

[23] A. Munshi and B. Alshawi, "Hybrid Encryption Model for Secured Three-Phase Authentication Protocol in IoT," *Journal of Sensor and Actuator Networks*, vol. 13, no. 4, Aug. 2024, Art. no. 41, https://doi.org/10.3390/jsan13040041.

[24] C. Benrebbouh, H. Mansouri, S. Cherbal, and A. S. K. Pathan, "Enhanced secure and efficient mutual authentication protocol in IoT-based energy internet using blockchain," *Peer-to-Peer Networking and Applications*, vol. 17, no. 1, pp. 68–88, Jan. 2024, https://doi.org/10.1007/s12083-023-01580-z.

[25] H. Fei, O. Millwood, P. Gope, J. Miskelly, and B. Sikdar, "PhenoAuth: A Novel PUF-Phenotype-Based Authentication Protocol for IoT Devices," in *2024 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Tysons Corner, VA, USA, May 2024, pp. 309–319, https://doi.org/10.1109/HOST55342.2024.10545387.

[26] S. P. Satpathy, S. Mohanty, and M. Pradhan, "A sustainable mutual authentication protocol for IoT-Fog-Cloud environment," *Peer-to-Peer Networking and Applications*, vol. 18, no. 1, Dec. 2024, Art. no. 35, https://doi.org/10.1007/s12083-024-01843-3.

[27] A. S. V. Rao, P. K. Roy, T. Amgoth, and A. Bhattacharya, "A deep learning-based authentication protocol for IoT-enabled LTE systems," *Future Generation Computer Systems*, vol. 154, pp. 451–464, May 2024, https://doi.org/10.1016/j.future.2024.01.014.

[28] S. Bhamare, S. Agarwal, and G. S. Kasbekar, "PUF-Based Lightweight and Anonymity-Preserving Continuous Authentication Protocol for IoT Devices," in *2024 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Guwahati, India, Dec. 2024, pp. 1–6, https://doi.org/10.1109/ANTS63515.2024.10898704.

[29] S. Kaganurmath, N. G. Cholli, and M. R. Anala, "DLKS-MQTT: A Lightweight Key Sharing Protocol for Secure IoT Communications," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21532–21538, Apr. 2025, https://doi.org/10.48084/etasr.10216.

[30] S. Othmen, W. Mansouri, and S. Asklany, "Robust and Secure Routing Protocol Based on Group Key Management for Internet of Things Systems," *Engineering, Technology & Applied Science Research*, vol. 14, no. 3, pp. 14402–14410, Jun. 2024, https://doi.org/10.48084/etasr.7115.

[31] M. A. Qureshi and A. Munir, "PUF-RLA: A PUF-Based Reliable and Lightweight Authentication Protocol Employing Binary String Shuffling," in *2019 IEEE 37th International Conference on Computer Design (ICCD)*, Abu Dhabi, United Arab Emirates, Nov. 2019, pp. 576–584, https://doi.org/10.1109/ICCD46524.2019.00084.

[32] K. Lounis, S. H. H. Ding, and M. Zulkernine, "D2D-MAP: A Drone to Drone Authentication Protocol Using Physical Unclonable Functions," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5079–5093, Apr. 2023, https://doi.org/10.1109/TVT.2022.3224611.

[33] W. Wang, B. Yan, B. Chai, R. Shen, A. Dong, and J. Yu, "EBIAS: ECC-enabled blockchain-based identity authentication scheme for IoT device," *High-Confidence Computing*, vol. 5, no. 1, Mar. 2025, Art. no. 100240, https://doi.org/10.1016/j.hcc.2024.100240.