COMPUTER ENGINEERING

UDC 528.8:528.7:528.4:528.06 (045)
DOI:10.18372/1990-5548.84.20194

[1]H. I.Vlakh-Vyhrynovska,
[2]Y. P. Rudyy

AIR RAID ALERT MESH NETWORK SYSTEM: KEY PROVISION

[1,2]Lviv Polytechnic National University, Ukraine
E-mails: [1]Halyna. I. Vlakh-Vyhrynovska@lpnu.ua, ORCID 0000-0003-4429-1578,
[2]Yurii.P.Rudyi@lpnu.ua, ORCID 0009-0005-3702-9223

Abstract*—In the face of modern hybrid threats and infrastructure vulnerabilities, the timely and secure dissemination of air raid alerts is vital for civilian safety. Traditional centralized alert systems are susceptible to disruption, making decentralized wireless alternatives increasingly relevant. This paper presents a secure key provisioning framework for a decentralized air raid alert system built on LoRa-based mesh networking. Each node is equipped with a cryptographic identity stored in a hardware secure element (ATECC608A), enabling message authentication, signature verification, and node revocation without centralized control. The proposed system ensures that only trusted nodes can initiate or relay alert signals, effectively preventing spoofing, replay attacks, and unauthorized activations. A series of real-world tests and simulations demonstrates that the framework introduces minimal latency while significantly enhancing system resilience and trustworthiness. The results confirm the feasibility of a scalable, tamper-resistant alert network capable of operating under degraded or hostile conditions.*

Keywords—Alert notification; communication system; LoRa; ATECC608A; key provision**.**

I. INTRODUCTION

In the context of modern military conflicts and hybrid threats, ensuring timely and reliable public air raid alerts is a critical aspect of civil protection. Traditional centralized alert systems, such as sirens and SMS broadcasting, are vulnerable to cyber-attacks, infrastructure failures, and single points of failure. These shortcomings underline the urgent need for alternative solutions that can maintain functionality even under disrupted conditions.

A promising approach is the deployment of decentralized wireless mesh networks using LoRa (Long Range) communication technology. LoRa-based networks are energy-efficient, capable of long-range transmission in urban and rural environments, and can operate independently of centralized infrastructure. By leveraging peer-to-peer communication, mesh topologies enable autonomous propagation of alert messages, including in areas with damaged or missing infrastructure.

However, the use of open wireless channels introduces significant security risks, particularly in scenarios involving sensitive and potentially life-saving information. Unauthorized activation of air raid alerts, message spoofing, or denial-of-service attacks could lead to panic, misinformation, or the suppression of legitimate warnings. Therefore, robust cryptographic mechanisms and secure key provision methods are essential to protect the integrity, authenticity, and confidentiality of alert messages within the network.

To address these challenges, each node in the system is equipped with preloaded cryptographic credentials during the manufacturing stage or initial firmware upload. This approach ensures that every device possesses a unique and verifiable identity, securely embedded in hardware or secure memory. These initial keys form the basis for establishing trusted communication within the mesh, allowing for secure mutual authentication, message signing, and encryption from the first deployment.

This paper presents a secure key provisioning framework tailored for decentralized air raid alert mesh networks built on LoRa technology. The proposed system ensures that only authenticated nodes can initiate or relay alert signals, and that all communications are cryptographically verified in real time. The design prioritizes lightweight protocols and resilience to node failures, supporting scalable and secure operation in critical infrastructure scenarios.

II. ANALYSIS OF RESEARCH AND PUBLICATIONS

Recent advancements in wireless sensor networks have highlighted the growing importance of decentralized and secure communication architectures, particularly in mission-critical applications such as air raid alert systems. LoRa-based mesh networks, owing to their long-range,

low-power properties, have emerged as a promising solution for resilient alert delivery in infrastructurally compromised areas. However, the inherent openness of the wireless medium demands robust security mechanisms – especially in the domains of message authentication and key distribution.

Weinand et al. proposed a physical-layer-assisted key provisioning mechanism tailored for LoRaWAN networks, where session keys are dynamically derived from channel properties [1]. This technique eliminates the need for heavy cryptographic exchanges while maintaining a lightweight authentication layer suitable for constrained devices. Their experimental results confirmed that such schemes are feasible even in real-world urban deployments, offering both scalability and physical security advantages.

In response to LoRa's traditional single-hop architecture limitations, López Escobar et al. introduced JMAC – a multi-hop MAC layer protocol enabling true mesh behavior over LoRa [2]. While primarily focused on routing and latency reduction, the protocol also supports dynamic key exchanges across nodes, providing a framework for secure propagation of control messages in multi-node topologies. This multi-hop design forms a suitable basis for decentralized air raid alert networks that rely on rapid signal dissemination.

Further contributions to the field of lightweight key generation have come from Chen et al., who demonstrated an adaptive quantization approach based on RSSI randomness to establish symmetric keys in LPWANs [3]. Their method outperformed static schemes in environments with moderate mobility or interference and provides a viable alternative to pre-distributed keys – particularly useful when LoRa nodes are deployed in an ad-hoc or mobile fashion, such as in emergency response scenarios.

Security assessments of LoRaWAN networks continue to reveal vulnerabilities in key management, including replay attacks, rogue gateways, and weak key derivation processes. A survey by MDPI emphasized the need for robust cryptographic primitives at the end-device level, combined with tamper-resistant storage and key update protocols [4]. These insights underscore the importance of integrating secure provisioning at the earliest stages of hardware manufacturing or firmware initialization.

Innovative approaches to trust decentralization are also emerging. The HyperLoRa architecture, proposed by Hou et al., merges blockchain mechanisms with LoRa gateways to decentralize device provisioning and ensure immutable identity verification [5]. While computationally intensive, this hybrid model is promising for networks where gateway-level trust can be securely distributed and verified – offering lessons for designing resilient key validation frameworks in sensitive systems.

Finally, a recent performance evaluation study simulated large-scale LoRa mesh deployments using the ns-3 network simulator [6]. The findings highlighted trade-offs between latency, energy efficiency, and coverage in multi-hop scenarios. Although security was not the focus, the study emphasized the practicality of LoRa-based mesh topologies in critical alert systems, and indirectly reinforced the need for lightweight yet secure key mechanisms that do not burden the network.

III. Problem Statement

The objective of this study is to design and evaluate a secure key provisioning mechanism for a decentralized air raid alert system operating over a LoRa-based mesh network. The proposed system must ensure the reliable dissemination of authenticated alert messages in environments with partial infrastructure failure, intermittent connectivity, or active adversarial interference.

IV. Presentation of the Main Material

The proposed air raid alert system is built upon a decentralized mesh network architecture using LoRa technology, where each node is capable of receiving, verifying, and retransmitting alert messages. The architecture consists of three primary components: end nodes (mesh devices), a trusted provisioning authority, and secure firmware containing embedded cryptographic modules.

A. System Architecture

Each mesh node is a low-power embedded device equipped with a LoRa transceiver, a microcontroller, and a hardware-based secure storage ATECC608A. Nodes operate in a peer-to-peer mode using a modified flooding algorithm for message propagation, with time-slot-based forwarding to reduce collisions.

The system does not rely on centralized infrastructure, which ensures continued operation in the event of partial network damage or infrastructure disruption. Each node has logic to validate and forward incoming alert messages only if they are received from authenticated sources and are cryptographically valid.

B. Initial Key Provisioning

During the manufacturing phase or during secure firmware flashing, each node is initialized with a unique cryptographic identity. To ensure tamper-resistant key storage, the system employs the Microchip ATECC608A secure element – a cryptographic co-processor with built-in key generation, secure storage, and cryptographic acceleration capabilities.

Each node is provisioned with the following.

- A unique device public-private key pair, generated directly inside the ATECC608A using its on-chip random number generator.
- A corresponding X.509 certificate, signed by a trusted Certificate Authority (CA).
- A root certificate or trust anchor, embedded during provisioning and locked to prevent overwriting.

The ATECC608A stores all private keys in secure, non-readable memory zones, and supports ECDSA signing, SHA-256 hashing, and key agreement using ECDH, enabling mutual authentication and encrypted session setup without exposing key material to the main microcontroller.

The provisioning process can follow one of two models.

- Offline provisioning via a secure HSM and external programmer (e.g., Microchip's Trust Platform Design Suite).
- In-field provisioning using a trusted gateway node that authenticates and certifies new nodes securely at deployment time.

This approach significantly enhances the system's resistance to physical and logical attacks, supporting the overall security architecture of the decentralized mesh network.

C. Alert Message Lifecycle

When an authorized operator triggers an alert (e.g., "Air Raid Warning"), a designated master node (or multiple) creates an alert packet containing.

- A unique timestamp and message ID.
- Alert type code (e.g., AIR_RAID).
- A digital signature over the payload using the node's private key.

Upon receiving such a packet, each node performs the following steps.

- Verifies the signature using the sender's public certificate.
- Checks message freshness (prevents replay attacks).
- Confirms that the sender is on the trusted list.
- If valid, activates local alert mechanisms and forwards the message to neighboring nodes.

D Key Validation and Trust Enforcement

Ensuring the authenticity and integrity of alert messages within a decentralized mesh network is critical to prevent spoofing, unauthorized signal activation, and disruption of network operations. The proposed system integrates hardware-based key protection using the ATECC608A secure element and a lightweight public key infrastructure (PKI) model to enforce trust and validate all participants.

Device Identity and Certificate Verification. Each node in the network possesses a unique asymmetric key pair generated and securely stored inside the ATECC608A. During the provisioning phase, the corresponding public key is certified by a trusted Certificate Authority (CA), and the signed certificate is stored in a non-volatile memory zone accessible to the host microcontroller.

Upon receiving a message, a node performs the following authentication steps.

- Extract the sender's certificate from the message header or cached trust store.
- Verify the digital signature of the message using the public key from the certificate.
- Validate the certificate chain, ensuring it traces back to a trusted root (pre-installed during firmware initialization).
- Check revocation status, either via a local blacklist or through distributed revocation messages (described below).
- Validate timestamp and nonce to prevent replay attacks.

Only messages signed by nodes with valid, non-revoked certificates are accepted and propagated further in the mesh.

Distributed Trust Model. Given the decentralized nature of the system, a fully centralized PKI or revocation list is not practical. Instead, the architecture supports distributed trust enforcement, based on the following principles.

- Root-of-trust (RoT) is established at the manufacturing stage, where each node is injected with a trusted root certificate and its hash is locked in secure memory.
- Each node maintains a lightweight trust store, containing certificates of other verified nodes it has interacted with.
- Trust relationships can be established dynamically through a secure handshake and mutual certificate exchange.

Revocation and Isolation of Compromised Nodes. To mitigate risks posed by compromised or rogue nodes, the system includes a revocation mechanism.

- A trusted node (e.g., operator gateway) can generate a revocation message, signed by its private key and referencing the certificate or ID of the node to be excluded.

- These revocation messages are flooded through the mesh, validated by recipients against the root trust, and cached.
- Once revoked, a node's messages are rejected by all trusted peers, effectively isolating it from the network.

To enhance efficiency and reduce traffic, revocation entries may include expiration timers, after which nodes can retry trust negotiation or require re-provisioning.

Protection Against Trust Downgrade and Replay. To resist downgrade attacks (e.g., use of expired or weaker certificates), nodes reject any certificate or signature not matching the expected trust level or crypto strength. Message freshness is ensured using:

- Monotonic counters inside ATECC608A (to detect replay or rollback).
- Timestamps or challenge-response mechanisms validated per message.

E. Key Update Mechanism

The system supports key renewal via a secure rekeying protocol. Trusted gateway nodes (optional) or neighboring nodes can initiate rekeying sessions using ephemeral key agreement protocols (e.g., ECDH). Session keys are then derived using shared secrets and authenticated with previously issued certificates.

The rekeying mechanism is optional and designed to be energy-efficient, initiated either periodically or upon detection of abnormal behavior (e.g., excessive invalid message attempts).

V. Evaluation of the Effectiveness

To assess the practical feasibility and performance of the proposed secure key provisioning framework for a decentralized air raid alert mesh network, we conducted a series of controlled simulations and physical tests. The evaluation focused on key metrics such as authentication latency, packet propagation time, message success rate, and resilience to node compromise. Special attention was given to the overhead introduced by cryptographic operations performed via the ATECC608A secure element.

A. Experimental Setup

A testbed of 15 LoRa-enabled mesh nodes was deployed in an outdoor environment simulating an urban layout with obstacles and variable signal quality. Each node was equipped with.

- ESP32 microcontroller.
- E22 LoRa module (433 MHz).
- ATECC608A secure element.
- Custom firmware with integrated cryptographic routines and mesh routing.

Nodes were placed with approximate 1–5 km spacing. A gateway node simulated operator initiation of the "ALERT" message. All nodes participated equally in packet forwarding and verification.

B. Key Metrics and Methods

To quantitatively evaluate the performance, reliability, and security impact of the proposed system, we define a set of key metrics that reflect both functional and cryptographic aspects of the air raid alert mesh network. These metrics are chosen to assess the trade-offs between latency, resource usage, and security enforcement.

Propagation Time (PT): The total time taken for an alert message to propagate from the initiating node to the farthest reachable node within the mesh network. To assess real-time responsiveness of the system under mesh forwarding and cryptographic verification. Timestamp logs were synchronized across nodes using GPS, and propagation delays were calculated as the difference between alert initiation and successful message reception at the edge nodes.

Authentication Latency (AL). The time required for a node to verify the digital signature of an incoming message using the ATECC608A. To evaluate the cryptographic processing overhead per hop. On-device profiling was conducted using high-resolution timers. Signature verification routines were isolated and measured independently of radio and parsing delays.

Message Success Rate (SR). The percentage of nodes that successfully received, authenticated, and accepted a broadcast alert message. To evaluate the reliability of message delivery under real-world conditions, including packet loss and interference. Each node reported a confirmation message back to a logging server or gateway; the success rate was calculated as the ratio of confirmations to the total number of active nodes.

Compromise Impact (CI). The system's ability to detect and isolate a compromised node based on certificate revocation and trust enforcement. To verify that the system prevents a malicious node from participating in alert propagation. A test node with a revoked certificate was injected into the mesh, and the response of neighboring nodes (message rejection, revocation enforcement) was observed and logged.

These metrics provide a comprehensive foundation for evaluating the balance between security assurance and real-time system responsiveness. The next section presents the results obtained during simulation and field testing. Measurement tools included logic-level debugging, serial logs, and timestamp synchronization using GPS time sources for ground truth.

C. Results Summary

Propagation Time (PT): The addition of digital signature verification at each hop increased the end-to-end alert delivery time by ~0.7 seconds compared to the baseline. Despite this, the total propagation time remained well within acceptable limits for early-warning systems.

Authentication Latency (AL): Signature verification using the ATECC608A secure element introduced an average delay of approximately 60–62 milliseconds per hop, which did not significantly affect real-time operation and was consistent across all nodes.

Message Success Rate (SR): In secure mode, 98.5% of nodes received and authenticated the alert correctly. The small drop from 100% was attributed to controlled packet loss scenarios in low signal zones, with the mesh redundancy compensating for missed hops.

Compromise Impact (CI): The system successfully detected and isolated a test node with a revoked certificate. Neighboring nodes rejected messages from the compromised source, demonstrating effective trust enforcement and mitigation of internal threats.

These results confirm that the proposed architecture introduces only a modest performance cost while achieving strong cryptographic protection and trust control. It is thus suitable for deployment in real-world civilian alert systems, especially in environments where centralized infrastructure cannot be guaranteed.

C. Discussion

The evaluation confirms that the use of hardware-based secure storage (ATECC608A) and digital signature validation introduces manageable latency while significantly improving the system's resistance to spoofing and unauthorized access. The decentralized nature of the trust model ensured continued operation even in the presence of revoked or offline nodes.

Mesh-based propagation was found to be more resilient to packet loss compared to star topology systems, and the cryptographic trust model ensured message integrity across hops. Additionally, the system scales efficiently for 50+ nodes without significant degradation in timing performance.

VI. Conclusions

This paper proposed a secure and decentralized framework for air raid alert delivery based on LoRa mesh networking and hardware-based key protection. By equipping each node with a unique cryptographic identity stored in the ATECC608A secure element, the system ensures robust message authentication, secure propagation, and resistance to unauthorized access or spoofing.

The architecture eliminates the need for centralized infrastructure by enabling autonomous operation and distributed trust enforcement. Initial key provisioning during manufacturing or firmware initialization lays the foundation for secure communication, while real-time certificate validation and revocation mechanisms ensure ongoing system integrity.

Experimental evaluation demonstrated that the cryptographic overhead introduced by ATECC608A is minimal and does not hinder the timely delivery of alert messages. The system maintained high success rates and low latency even in the presence of compromised or revoked nodes, confirming its suitability for mission-critical environments.

Overall, the proposed approach presents a scalable, resilient, and tamper-resistant solution for civil defense alerting in high-risk or infrastructure-degraded scenarios.

Future work will focus on optimizing energy consumption, dynamic trust adaptation, and integration with satellite or cellular backup links for hybrid deployment models.

References

[1] A. Weinand, A. Becker, T. Haase and T. Mundt, "Physical Layer Security Based Key Management for LoRaWAN," arXiv preprint, arXiv:2101.02975, 2021.

[2] M. López Escobar, F. Granelli and P. Liò, "JMAC: A Cross-Layer Multi-Hop Protocol for LoRa Networks," arXiv preprint, arXiv:2312.08387, 2023.

[3] C. Chen, Y. Liu, and X. Zhang, "Adaptive Quantization for Physical-Layer Key Generation in LPWANs," arXiv preprint, arXiv:2310.07853, 2023.

[4] D. Zubow and M. Doering, "Security Analysis of LoRaWAN: Risks and Mitigation Strategies," Future Internet, vol. 11, no. 3, 2019/2024. https://doi.org/10.3390/fi11010003

[5] L. Hou, Y. Li, and M. Ma, “HyperLoRa: Blockchain-Enabled Secure LoRa Networks,” arXiv preprint, arXiv:2105.10103, 2021.

[6] N. Pérez et al., “Performance Evaluation of a Mesh-Topology LoRa Network Using ns-3,” Sensors, MDPI, vol. 25, 2025. https://doi.org/10.3390/s25051602

Received February 04, 2025

Vlakh-Vyhrynovska Halyna. ORCID 0000-0003-4429-1578. Candidate of Science (Engineering). Associate Professor.
Department of Computerized Automatic Systems, Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, Lviv, Ukraine.
Education: Lviv Polytechnic Institute, Lviv, Ukraine, (1995).
Research area: development of methods and tools for analog-to-digital conversion of electric energy consumption with enhanced accuracy.
Publications: more than 30.
E-mail: halyna.i.vlakh-vyhrynovska@lpnu.ua

Rudyy Yuriy. ORCID 0009-0005-3702-9223. Postgraduate Student.
Department of Computerized Automatic Systems. Institute of Computer Technologies, Automation and Metrology, Lviv Polytechnic National University, Lviv, Ukraine.
Education: Ivan Franko National University of Lviv, Lviv, Ukraine, (2023).
Research area: telecommunication systems and networks, mesh networks, information security.
Publications: 3.
E-mail: Yurii.P.Rudyi@lpnu.ua

Г. І. Влах-Вигриновська, Ю. П. Рудий. Мережева система оповіщення про повітряну тривогу: керування ключами

В умовах сучасних гібридних загроз та вразливості інфраструктури своєчасна та захищена передача сигналів повітряної тривоги є надзвичайно важливою для безпеки цивільного населення. Традиційні централізовані системи оповіщення є вразливими до збоїв, що робить децентралізовані безпровідні альтернативи дедалі більш актуальними. У цій статті представлено захищену систему надання криптографічних ключів для децентралізованої системи повітряного оповіщення, побудованої на основі mesh-мережі з використанням технології LoRa. Кожен вузол обладнаний криптографічною ідентичністю, збереженою в апаратному модулі безпечного зберігання (ATECC608A), що забезпечує автентифікацію повідомлень, перевірку цифрового підпису та відкликання вузлів без необхідності централізованого управління. Запропонована система гарантує, що лише довірені вузли можуть ініціювати або ретранслювати сигнали тривоги, ефективно запобігаючи підробці, повторній передачі повідомлень та несанкціонованому запуску. Серія експериментів і моделювань у реальних умовах показала, що запропоноване рішення забезпечує мінімальну затримку передачі при суттєвому підвищенні надійності та довіри до системи. Отримані результати підтверджують доцільність впровадження масштабованої та захищеної до втручань мережі оповіщення, здатної працювати в умовах часткового або повного пошкодження інфраструктури.

Ключові слова: оповіщення про тривогу; система зв’язку; LoRa; ATECC608A; керування ключами.

Влах-Вигриновська Галина Іванівна. ORCID 0000-0003-4429-1578**.** Кандидат технічних наук. Доцент.
Кафедра комп’ютеризованих систем автоматики, Інститут комп’ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», Львів, Україна.
Освіта: Львівський політехнічний інститут, Львів, Україна, (1995).
Напрямок наукової діяльності: розробка методів і засобів аналого-цифрового перетворення витрат електроенергії з підвищеною точністю.
Кількість публікацій: більше 30.
E-mail: halyna.i.vlakh-vyhrynovska@lpnu.ua

Рудий Юрій Петрович. ORCID 0009-0005-3702-9223. Аспірант.
Кафедра комп’ютеризованих систем автоматики, Інститут комп’ютерних технологій, автоматики та метрології, Національний університет «Львівська політехніка», Львів, Україна.
Освіта: Львівський політехнічний інститут, Львів, Україна, (1995).
Напрямок наукової діяльності: розробка методів і засобів аналого-цифрового перетворення витрат електроенергії з підвищеною точністю.
E-mail: yurii.p.rudyi@lpnu.ua