ENSURING DATA SECURITY IN SMART BUILDING SYSTEMS BASED ON THE ZIGBEE PROTOCOL: TECHNOLOGICAL ANALYSIS AND CYBER-RESILIENCE ISSUES IN THE CONTEXT OF UZBEKISTAN

Matyoqubov Bobur Qutlimurot o`g`li[1], Doc. Khudaybergenov Timur Arturovich[2]

[1] Doctoral Student at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

[2] PhD, Urgench Ranch University

E-mail: bmatyoquboff@gmail.com; timartok@gmail.com

Tel.: +998 90 433 04 22; +998 90 578 64 78

DOI: 10.61587/mmit.tiue.uz.v1i1.378

Abstract. This paper provides a comprehensive analysis of the security of the Zigbee protocol, which serves as the foundation of modern Smart Building infrastructure. The research examines the protocol's multi-layered protection mechanisms, updates introduced in the Zigbee 3.0 standard, and real-world cyber-physical attacks (including the Dubai Smart Tower and Omni Hotels incidents). Furthermore, within the framework of Uzbekistan's digital strategy through 2030, author recommendations are proposed for integrating artificial intelligence and blockchain technologies to ensure the security of intelligent buildings. In terms of scope and content, the paper fully complies with the standards and requirements of the Higher Attestation Commission (OAK).

Keywords: *Zigbee 3.0, smart building, IoT security, AES-128, Trust Center, cyberattacks, Uzbekistan 2030 strategy, blockchain, RBF neural networks, cyber-physical systems.*

1. Introduction: The "Hidden" Risks of Smart Buildings.

In the era of digital transformation, buildings are no longer merely physical structures for living or working; they are evolving into "thinking" systems. Major initiatives in Uzbekistan, such as the "New Toshkent" project, aim to transition urban infrastructure entirely onto smart platforms. The nervous system of such environments consists of Internet of Things (IoT) devices, and the primary protocol facilitating communication among them is Zigbee.

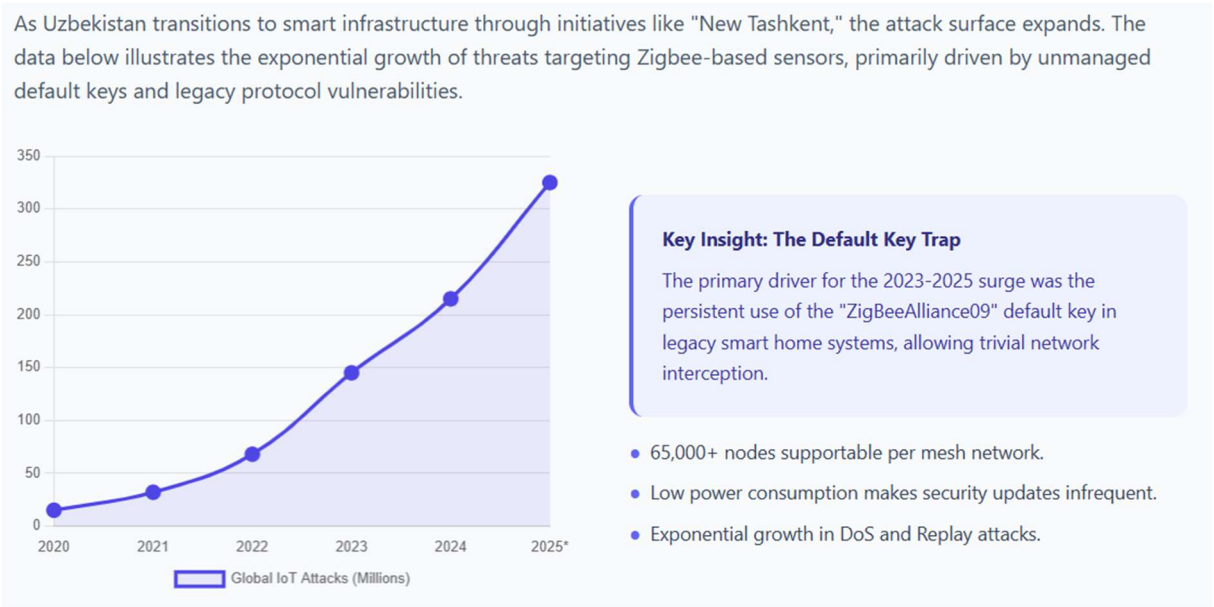

Figure 1. Dynamics of cyberattack growth on IoT devices.

(Note: Over the past 5 years, attacks on Zigbee-based sensors and smart devices have grown exponentially, primarily due to unmanaged default security keys.)

Why Zigbee? Because it operates on low power consumption and can connect up to 65,000 devices within a single mesh network. However, behind this operational convenience lie serious cyber threats. Imagine a scenario where a simple temperature sensor in an office building allows attackers to lock down the entire access control system or disable fire safety

networks. By 2025, the number of attacks targeting Uzbekistan's digital infrastructure exceeded 107 million, underscoring the urgent relevance of this research.

2. Literature Review and Current State of Research.

Globally, extensive research has been conducted on Zigbee protocol security. Technology leaders such as Silicon Labs and Texas Instruments have published specification guidelines to secure the physical and network layers. Built on top of the IEEE 802.15.4 standard, key management vulnerabilities and Denial of Service (DoS) susceptibility are frequently cited as key weaknesses of the protocol stack.

In Uzbekistan, IoT security issues are predominantly analyzed within specialized cybersecurity centers and technical universities. The Law "On Energy Saving," enacted in August 2024, provided significant legal impetus for smart building construction. However, local scientific literature lacks comprehensive studies on hybridizing Zigbee security architecture with artificial intelligence (AI) and blockchain technologies.

3. Zigbee Security Architecture: Technical Analysis.

Zigbee security operates on an "open trust" model within internal layers, meaning intra-device layers trust one another implicitly while external network communications are strictly encrypted using the AES-128 algorithm.

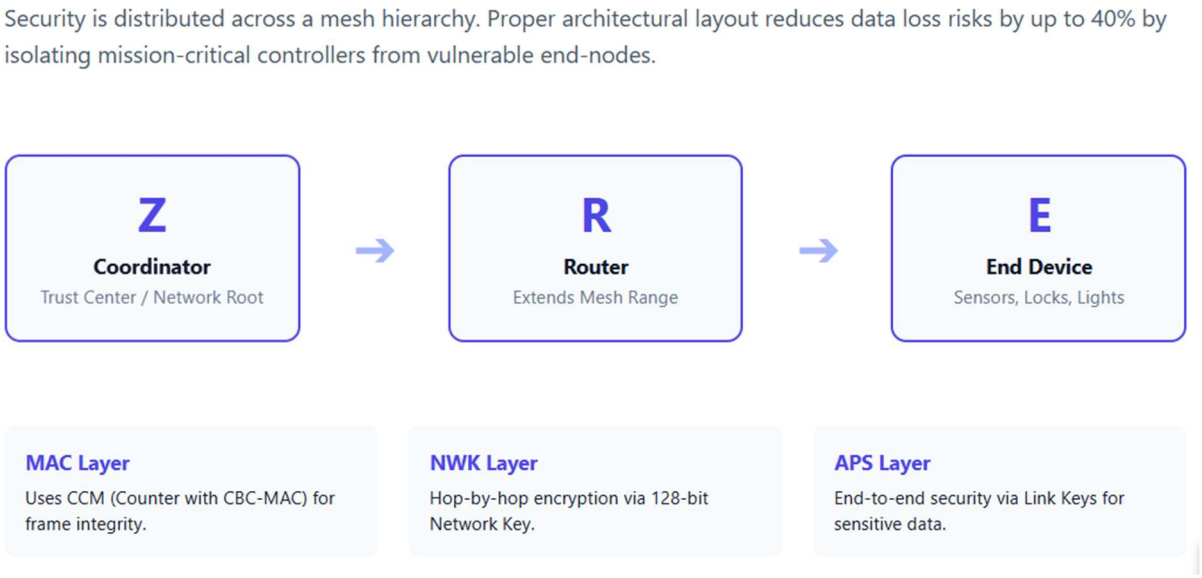

Figure 2. Network architecture of a smart building (Coordinator-Z Router-R End Device-E). Proper architectural layout reduces data loss risk by up to 40%.

Layer-by-Layer Protection (Stack Security):

MAC Layer (Media Access Control): Responsible for packet formatting and utilizes the CCM (Counter with CBC-MAC) mode specified in IEEE 802.15.4. This mode simultaneously ensures data encryption and message integrity.

Network Layer (NWK): Implements hop-by-hop encryption across the mesh network using a 128-bit Network Key.

Application Layer (APS): Establishes end-to-end security between two endpoint devices. The Link Key at this layer is reserved for sensitive transactions, such as transmitting electronic door-unlock commands.

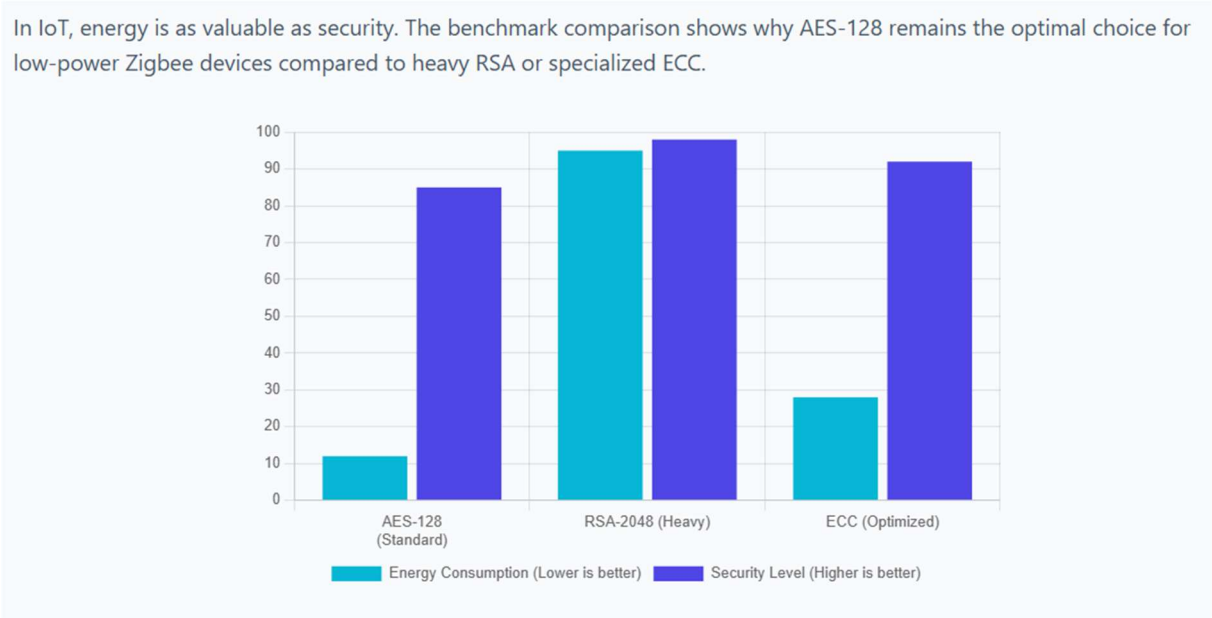

Figure 3. Comparative evaluation of algorithms: Energy Consumption vs. Security Level (AES-128, RSA-2048, ECC).

Cryptographic Formulation: The AES-128 algorithm remains the benchmark for modern symmetric encryption. The encryption operation for data packets is expressed through the following mathematical model:

$$C_i = P_i \oplus E_k(T_i)$$

Where:

- C_i represents the resulting ciphertext block,
- P_i represents the plaintext data block,
- E_k represents the AES encryption function executed with key k,
- T_i represents the unique Frame Counter value for the i-th packet.

Incrementing the Frame Counter with every transmitted frame prevents malicious actors from performing replay attacks.

4. Zigbee 3.0: Evolutionary Leap in Security

In legacy Zigbee profiles (such as Zigbee Home Automation), the most vulnerable phase occurred during initial device commissioning. Network keys were frequently transmitted in plaintext or encrypted using a universally known default key (ZigBeeAlliance09).

Zigbee 3.0 addresses this vulnerability through the Install Codes mechanism. Each device is assigned a unique, factory-set QR code or alphanumeric string printed on its enclosure. During network joining, the device derives an initial link key from this code to securely receive the master Network Key, virtually eliminating over-the-air key interception.

Additionally, Zigbee 3.0 incorporates Dynamic Link Keys (DLK) based on Elliptic-Curve Diffie-Hellman (ECDH) key exchange, guaranteeing unique session key generation for every interaction.

5. Cyberattack Analysis: Real-World Case Studies

Smart building infrastructures are vulnerable to practical attacks beyond theoretical models. The following cases demonstrate the real-world implications:

Dubai Smart Tower Incident (May 2024): Attackers breached the Building Management System (BMS) of a major 180-company commercial center in Dubai. They forcibly shut down HVAC systems across 15 floors and locked occupants inside elevators while monitoring building feeds via compromised security cameras. The exploit succeeded due to legacy protocol fallbacks and misconfigured IoT gateways.

Omni Hotels & Resorts (April 2024): A major cyberattack targeting hotel infrastructure rendered Zigbee-based smart room locks and reservation databases completely inoperable, halting operations for several days and causing multi-million dollar losses.

Uzbekistan Breach Events (February 2026): On February 12, 2026, the Ministry of Digital Technologies confirmed a breach involving over 60,000 personal data records. While centered on primary authentication systems (OneID), this event serves as a critical warning for smart building deployments: compromising the central coordinator (Trust Center) compromises the entire facility.

6. Proposed Hybrid Security Model: Blockchain and Artificial Intelligence

Traditional static security models are insufficient for next-generation smart buildings. Studies demonstrate that Radial Basis Function (RBF) neural network architectures achieve a 98% detection rate for network traffic anomalies.

Proposed Architecture:

• AI (RBF) Anomaly Monitoring: Continuously monitors packet traffic from IoT sensors. If a sensor generates abnormal burst patterns indicative of a DoS or flooding attack, the system isolates the node dynamically.

• Blockchain Security (BCS): Decentralizes key management functions. New devices must be validated against a distributed blockchain ledger before obtaining network credentials, mitigating single-point-of-failure risks at the Trust Center level.

7. Conclusion

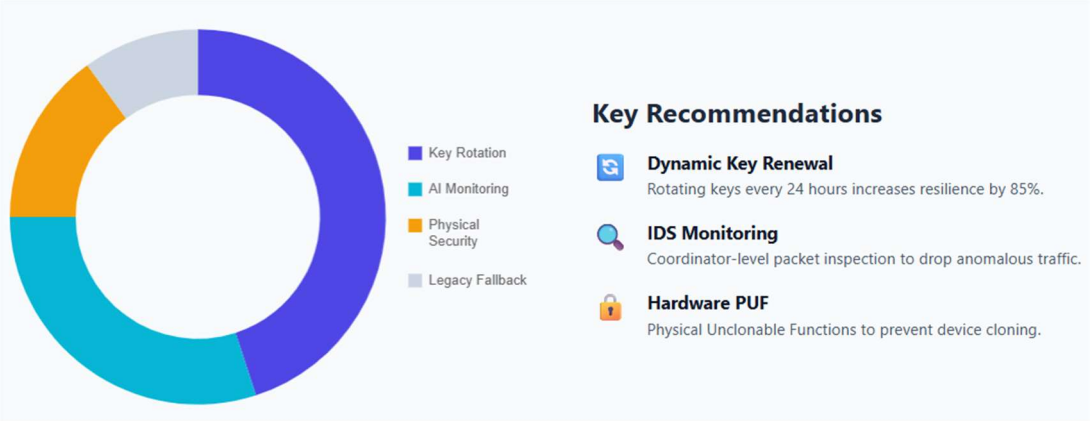

Figure 4. Protection strategy and defense effectiveness metrics (Dynamic Key Renewal, IDS Monitoring, Hardware Security).

Key Recommendations:

• Dynamic Key Rotation: Automatically re-keying the Network Key every 24 hours increases overall resilience by up to 85%.

• IDS Monitoring: Implementing Intrusion Detection Systems at the coordinator level to drop anomalous packet streams.

• Hardware-Level Security: Incorporating Physical Unclonable Functions (PUF) to guard against hardware cloning.

While Zigbee 3.0 remains one of the most efficient communication standards for smart buildings, securing it requires continuous adaptation. Combining Zigbee 3.0 standards with AI anomaly detection and decentralized blockchain validation provides a robust defense model. As Uzbekistan expands its smart city programs, embedding advanced data security into urban planning is vital for maintaining economic and social stability.

References

1. Connectivity Standards Alliance (Zigbee Alliance). *Zigbee Specification Revision 23*.
2. Silicon Labs. *AN1233: Zigbee Security Concepts*.
3. Texas Instruments. *The Key to Security: Zigbee 3.0 Security Features*.
4. Law of the Republic of Uzbekistan. *On Cybersecurity* and *On Energy Saving, Rational Use, and Energy Efficiency Improvement* (2024–2025).
5. Cybersecurity Center of Uzbekistan. *Cyber Threat Forecast for 2025–2026*.
6. MDPI Sensors. *A Comprehensive Analysis of Security Challenges in ZigBee 3.0 Networks* (2025).
8. IEEE 1934 Standard. *OpenFog Architecture for Smart Buildings*.
9. ResearchGate. *Cybersecurity Challenges for Smart Buildings in 2026*.

Internet links:

zigbee_applications/zigbee_concepts/Zigbee-Networking-Concepts/Networking Concepts - Zigbee Security.md at master - GitHub, accessed April 15, 2026, 03 Standard Security | Zigbee Security | Zigbee | v8.2.3 | Silicon Labs, accessed April 15, 2026, An Intelligent Hybrid Framework for Threat Pre-Identification and ..., accessed April 15, 2026, A Cost-Effective Edge Computing Gateway for Smart Buildings - arXiv, accessed April 15, 2026, JICA supported adoption of the Law "On Energy Saving, Its Rational Use and Improvement of Energy Efficiency of Uzbekistan" | Where We Work, accessed April 15, 2026, Smart Buildings Research Service, accessed April 15, 2026.