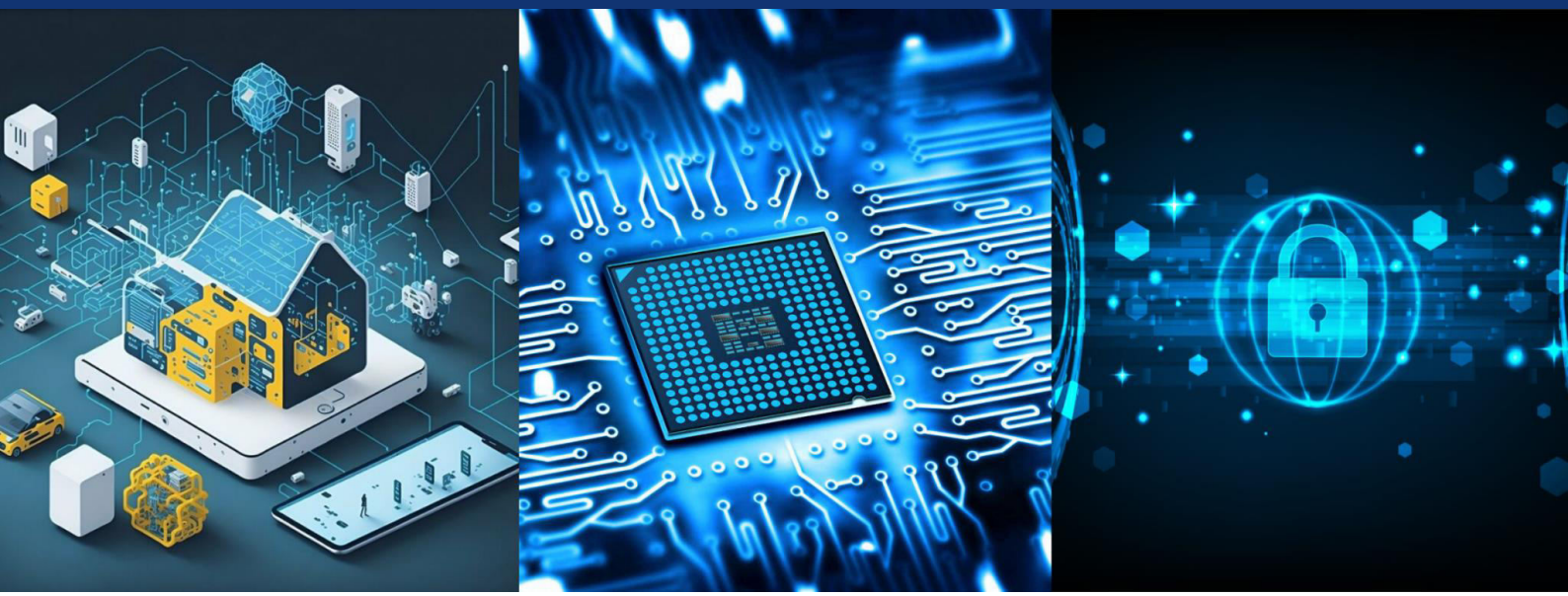
IJIRCCE

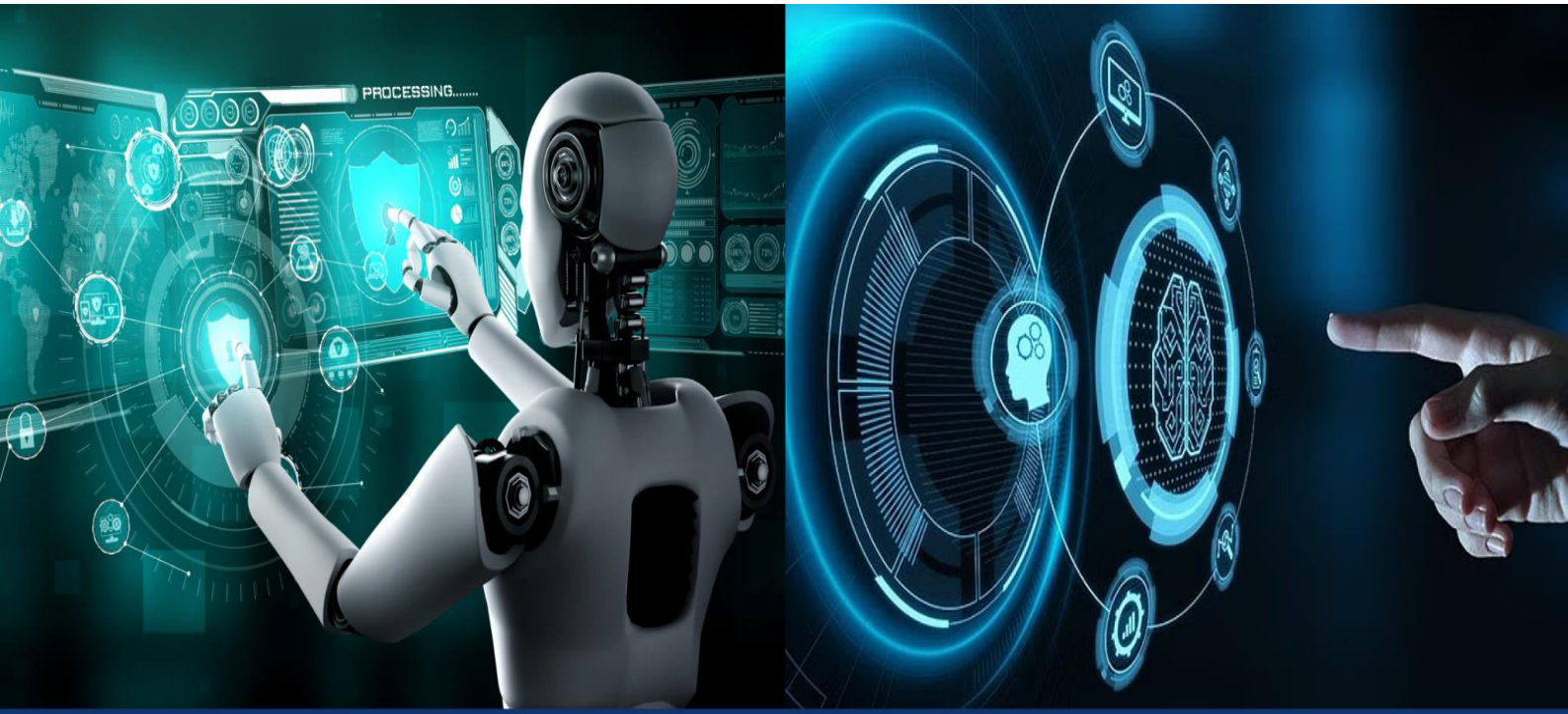
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 5, May 2026

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405026

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Wireless Network Security in Smart Device

Vikas K S[1], Dr Puja Shashi[2]

PG Student, Dept. of MCA, City Engineering College, Bengaluru, Karnataka, India[1]

Professor & HOD, Dept. of MCA, City Engineering College, Bengaluru, Karnataka, India[2]

ABSTRACT: Smart devices like smartphones, wearables, smart home appliances, and industrial IoT endpoints increasingly rely on wireless networks for connectivity and service delivery. However, their resource-constrained nature and heterogeneous communication stacks make them vulnerable to a wide range of wireless attacks. In this paper, an efficient and secure wireless communication framework is proposed for smart-device-based networks. The framework optimizes energy-efficient data transmission while enforcing multi-layer security mechanisms to protect against eavesdropping, spoofing, and denial-of-service attacks. A trust-based authentication scheme is introduced to validate the legitimacy of smart-device nodes and to detect malicious entities attempting to emulate legitimate users. The framework is assessed using standard simulation tools, and performance metrics such as throughput, end-to-end delay, and packet-delivery ratio are analysed under normal and attack scenarios. Findings indicate that the suggested scheme improves secure communication reliability with minimal overhead on energy-constrained smart devices.

KEYWORDS: Smart Devices, Wireless Network Security, IoT Security, Trust-Based Authentication, Secure Communication, Energy Efficiency.

I. INTRODUCTION

With the proliferation of smart devices in homes, industries, and cities, wireless networks have become the backbone of modern digital ecosystems. These devices typically operate over Wi-Fi, Bluetooth, Zigbee, or cellular-based IoT protocols, which expose them to a broad attack surface at the physical, link, network, and application layers. Traditional security protocols such as WPA2/WPA3 and TLS are often either too heavy for low-power smart devices or not consistently enabled, leaving many devices exposed to passive and active attacks.

In this paper, an efficient and secure wireless communication framework is proposed for smart-device networks. The framework aims to achieve three main objectives: (i) reduce the amount of energy used for transmitting data, (ii) preserve the integrity and confidentiality of data over wireless links, and (iii) detect and mitigate malicious or compromised smart-device nodes. A trust-based authentication algorithm is integrated into the communication stack to evaluate the behavioural credibility of each node and to control access to the wireless network. This approach allows smart devices to communicate securely while adapting to dynamic network conditions such as node mobility, channel congestion, and intermittent connectivity.

II. SYSTEM MODEL AND ASSUMPTIONS

The system model considers a heterogeneous network of N smart-device nodes, including mobile phones, sensors, actuators, and home gateways, that communicate over a shared wireless medium. The network is assumed to operate in the presence of licensed primary systems (e.g., cellular base stations) and unlicensed secondary services (e.g., Wi-Fi access points and IoT gateways). The wireless spectrum is partition into M non-overlapping channels with different bandwidths and time-slot structures.

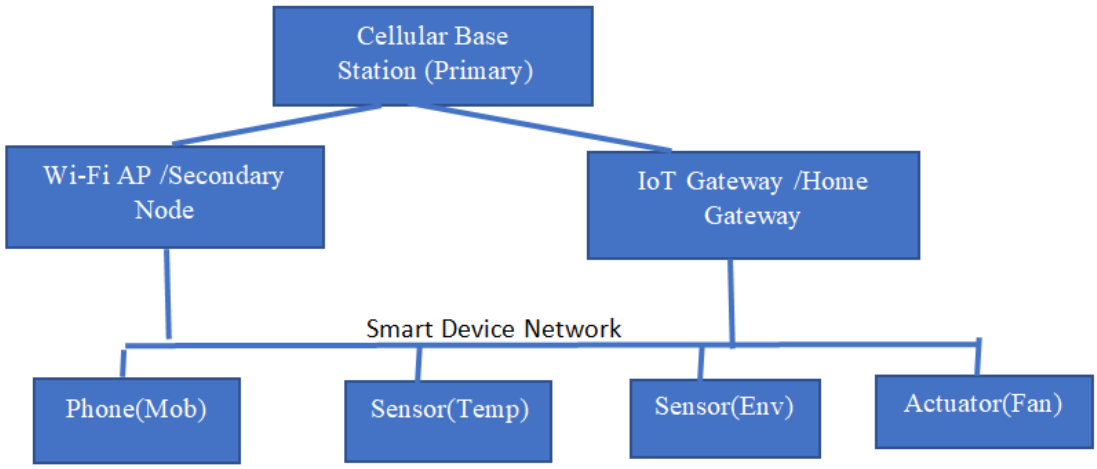
Each smart-device node is equipped with a wireless transceiver capable of switching between multiple channels and communication protocols. All nodes are assumed to follow a given mobility model and to periodically exchange beacon or hello messages to maintain neighbour information. A secure control channel or frequency-hopping sequence (FHS) is used for initial node discovery and key exchange, ensuring that sensitive control packets are protected from eavesdropping and tampering. The communication protocol stack includes lightweight encryption and integrity-checking mechanisms adapted to the processing and energy constraints of smart devices.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405026

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



III. EFFICIENT WIRELESS COMMUNICATION

For smart-device networks, reducing energy consumption while maintaining acceptable latency and throughput is critical. In the proposed framework, each transmitting node first evaluates possible next-hop nodes based on a node-selection criterion that balances energy cost and path reliability. The node-selection metric considers residual battery level, link quality, and historical packet-delivery ratio for each candidate relay.

A channel-selection scheme is also introduced to increase spectrum utilization while reduce interference with primary and neigh boring systems. The available licensed channels are periodically sensed, and a channel-quality metric is computed as the product of bandwidth and idle duration, $tc=y \cdot x$, where y is the channel bandwidth and x is the observed idle time. Channels with higher tc are preferred for data transmission, whereas channels frequently occupied by primary users are avoided. If primary-user signals are detected, the node switches to an alternative channel or enters a low-power sensing mode to reduce interference and energy waste.

This combination of node and channel selection enables smart-device nodes to dynamically choose optimal paths and frequencies, thereby improving end-to-end latency and throughput without significantly increasing energy consumption.

IV. SECURITY IN SMART DEVICE NETWORKS

Multi-Layer Security Mechanisms

To address these challenges, the proposed framework integrates security at multiple layers:

Link-layer security: Use of WPA2/WPA3-based mutual authentication and encryption for Wi-Fi connections, and secure pairing for Bluetooth-based smart devices.

Network-layer security: Implementation of lightweight secure routing protocols that incorporate message authentication and integrity checks to prevent routing-table poisoning and sinkhole attacks.

Wireless Threat Landscape

Smart-device networks face a variety of wireless attacks, including man-in-the-middle (MitM) attacks, replay attacks, spoofing, rogue access points, and eavesdropping. Due to weak or absent encryption, many consumer-grade smart devices leak sensitive sensor data or authentication tokens. In industrial and critical-infrastructure settings, attackers may inject false commands or disrupt service through denial-of-service flooding.

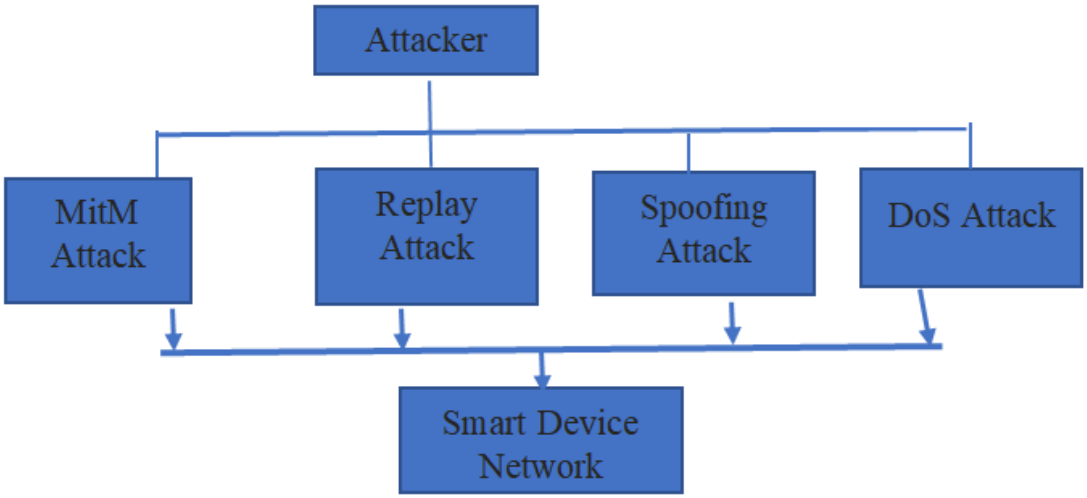
Moreover, compromised devices can be recruited into botnets that launch coordinated attacks on other network segments. These threats are exacerbated by the lack of consistent security updates, default credentials, and limited onboard cryptographic capabilities in many low-end smart devices.

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405026

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Wireless Threat Landscape

Transport-and application-layer security: Employment of TLS/DTLS or similar lightweight secure protocols for data-in-transit protection, particularly for cloud-connected smart devices.

Trust-Based Authentication Scheme

A trust-based authentication algorithm is introduced to evaluate the credibility of each smart-device node. Each node is assigned a dynamic trust score that is updated based on:

- Successful and timely packet delivery,
- Consistency of spectrum-sensing decisions (for spectrum-aware devices),
- Absence of suspicious behaviour such as repeated failed authentication attempts or unexpected channel switches.

When a node requests to join the network, its trust score is checked against a predefined threshold. Nodes with scores below the threshold are either isolated or subjected to stricter monitoring and limited privileges. This trust framework helps detect selfish or malicious nodes that attempt to emulate legitimate users or degrade network performance.

V. RESULT AND DISCUSSION

Simulation Setup

The proposed framework is implemented and evaluated using a standard network simulator (e.g., NS-2 or NS-3), modelling a network of smart-device nodes with varying mobility patterns and power constraints. Several scenarios are considered: normal operation, MitM attacks, spoofing attempts, and denial-of-service flooding. Performance metrics such as throughput, end-to-end delay, packet-delivery ratio, and energy consumption are recorded under each scenario.

Key Observations

Throughput vs. Simulation: Figure 1 shows that the secure framework maintains a stable throughput over time, even under attack conditions, due to the trust-based filtering of malicious nodes. In contrast, an unprotected baseline configuration exhibits significant throughput degradation once attacks are introduced.

Throughput vs. End-to-End: Delay illustrates the trade-off between throughput and end-to-end delay. The proposed scheme achieves a higher throughput at a moderate increase in delay compared with strict security-only configurations, indicating a balanced design suitable for latency-sensitive smart-device applications.

Throughput vs. Jitter: In Figure 3, jitter is measured as the variation in packet arrival time. The secure framework reduces jitter under normal conditions by avoiding unstable or congested channels, while still maintaining acceptable performance under active attacks.

These results demonstrate that the proposed secure wireless communication framework improves reliability and trustworthiness with only marginal overhead on low-power smart devices.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. CONCLUSION

In this paper, an efficient and secure wireless communication framework for smart-device networks is proposed. The framework combines energy-aware node and channel selection with multi-layer security and a trust-based authentication scheme to protect against a wide range of wireless attacks. Simulation results show that the scheme enhances secure throughput, maintains reasonable end-to-end delay, and reduces jitter under both normal and attack conditions. The framework can be practically deployed in smart-home, industrial-IoT, and urban-sensor networks to improve the confidentiality, integrity, and availability of smart-device communications. Future work may explore integrating AI-based anomaly detection and blockchain-assisted identity management to further strengthen wireless security in smart-device ecosystems.

REFERENCES

1. Gupta et al., "AI-Driven Intrusion Detection for Smart IoT Wireless Networks," *IEEE Internet of Things Journal*, vol. 12, no. 2, pp. 1450–1463, Jan. 2025.
2. L. Zhang and H. Wang, "Lightweight Authentication Protocols for Resource-Constrained Smart Devices," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 980–993, Mar. 2025.
3. M. Al-Hawawreh et al., "Secure Federated Learning for Wireless Edge-Enabled Smart Devices," *IEEE Wireless Communications*, vol. 32, no. 1, pp. 76–83, Feb. 2025.
4. S. R. Pokhrel and J. Choi, "Physical Layer Security in 6G-Enabled Smart Device Networks," *IEEE Communications Magazine*, vol. 63, no. 4, pp. 102–108, Apr. 2025.
5. Y. Liu et al., "Blockchain-Based Secure Data Sharing in Smart Home Wireless Networks," *Future Generation Computer Systems*, vol. 150, pp. 250–262, 2025.
6. T. Nguyen and D. B. Rawat, "Privacy-Preserving Communication in Smart Healthcare IoT Systems," *IEEE Access*, vol. 13, pp. 31045–31058, 2025.
7. R. Sharma et al., "Zero-Trust Architecture for Wireless Smart Device Ecosystems," *Computer Networks*, vol. 245, 110234, 2025.
8. J. Kim and S. Park, "Quantum-Resistant Cryptography for IoT Wireless Security," *IEEE Transactions on Network Science and Engineering*, vol. 12, no. 3, pp. 2101–2114, 2025.
9. E. Baccarelli et al., "Energy-Efficient Secure Communication in Edge-Based Smart Device Networks," *IEEE Transactions on Green Communications and Networking*, vol. 9, no. 1, pp. 88–101, 2025.
10. F. A. Aoudia and M. Hoydis, "Machine Learning for Secure Wireless Communications in Smart Devices," *IEEE Journal on Selected Areas in Communications*, vol. 43, no. 6, pp. 1550–1565, Jun. 2025.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details