Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3167–3176
DOI : 10.47974/JDMSC-2744

Lightweight elliptic curve cryptography for SDN-managed secure communication in 6G wireless sensor networks

Ashok Kumar Saini [#]
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Manoj Wadhwa [†]
Department of Computer Science & Engineering
University Institute of Engineering
Chandigarh University
Mohali 140413
Punjab
India

Richa Rawal [§]
Department of Information Technology
Swami Keshvanand Institute of Technology, Management & Gramothan
Jaipur 302017
Rajasthan
India

Sanat Jain [‡]
Department of Computer Science & Engineering
School of Computing Science & Engineering
VIT Bhopal University
Sehore 466114
Madhya Pradesh
India

[#] *E-mail:* ashok.saini@jaipur.manipal.edu
[†] *E-mail:* manojkw11@yahoo.com
[§] *E-mail:* richarawal@skit.ac.in
[‡] *E-mail:* sanatjain@vitbhopal.ac.in

Reenu Batra [@]
Department of Computer Science and Engineering
School of Engineering & Technology
K. R. Mangalam University
Gurugram 122103
Haryana
India

Prashant Vats *
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

Sixth-generation (6G) wireless communication is anticipated to support massive sensor connectivity, real-time intelligence, and ultra-reliable services, thereby intensifying security requirements in Wireless Sensor Networks (WSNs). Conventional cryptographic solutions often impose excessive computational and energy overhead on sensor nodes, limiting their applicability in 6G environments. In this work, a lightweight security framework based on Elliptic Curve Cryptography (ECC) is presented for Software-Defined Networking (SDN)–controlled 6G Wireless Sensor Networks. The proposed framework exploits discrete elliptic curve structures over finite fields to provide secure key establishment and data confidentiality with minimal resource consumption. SDN is employed to decouple control and data planes, enabling centralized policy enforcement, adaptive key distribution, and programmable security management.

Subject Classification: *Primary 94A60, Secondary 94A62.*

Keywords: *6G wireless sensor networks, Software-defined networking (SDN), Elliptic curve cryptography (ECC), Lightweight cryptography, Secure communication, Programmable data plane, SDN-based firewall, P4-enabled switches, Key management, Energy-efficient security.*

1. Introduction

The rapid evolution of sixth-generation (6G) wireless communication is expected to significantly transform Wireless Sensor Networks (WSNs) by enabling ultra-low latency, massive connectivity, and intelligent data-driven services. These capabilities support emerging applications such as smart cities, autonomous systems, industrial automation, and advanced healthcare. However, large-scale sensor deployment in 6G environments introduces serious security challenges related to data confidentiality, authentication, key management, and

[@] *E-mail:* **reenubatra88@gmail.com**
* *E-mail:* **prashant.vats@jaipur.manipal.edu (Corresponding Author)**

network scalability. The resource constraints of sensor nodes, including limited energy, memory, and computational capacity, further complicate the implementation of robust security mechanisms. Traditional cryptographic approaches such as RSA impose high computational and communication overhead, making them unsuitable for resource-constrained WSNs. In contrast, Elliptic Curve Cryptography (ECC) provides equivalent security with significantly smaller key sizes by exploiting algebraic properties of elliptic curves over finite fields, making it well-suited for lightweight secure communication. Despite these advantages, efficient management of cryptographic operations in dynamic 6G WSN environments remains challenging. Figure 1 presents an SDN-based programmable firewall architecture where a centralized controller analyzes network traffic and dynamically installs security rules on P4-enabled switches. The switches perform line-rate packet inspection to block malicious traffic and forward legitimate flows. This approach enables scalable, adaptive, and efficient security enforcement for SDN-managed 6G Wireless Sensor Networks.

2. Related Work

Recent studies on next-generation communication networks emphasize secure, efficient, and scalable data transmission across IoT, cloud, and optical infrastructures. Trust-based frameworks improve reliability in IoT-enabled edge–fog–cloud environments [1], while SDN/NFV technologies enhance network flexibility and service management [2, 6]. Optical and elastic networks address high bandwidth demands through advanced routing, modulation, and spectrum allocation techniques [3, 5, 7, 9, 10]. Security-focused approaches such as blockchain-based communication frameworks and intelligent detection mechanisms further strengthen network protection [4, 11, 12]. Additionally, IoT-driven applications and data-driven analysis support smart infrastructures and communication systems [8, 13, 14]. However, integrating lightweight cryptographic schemes with SDN-based control for secure 6G wireless sensor networks remains limited, motivating this study.

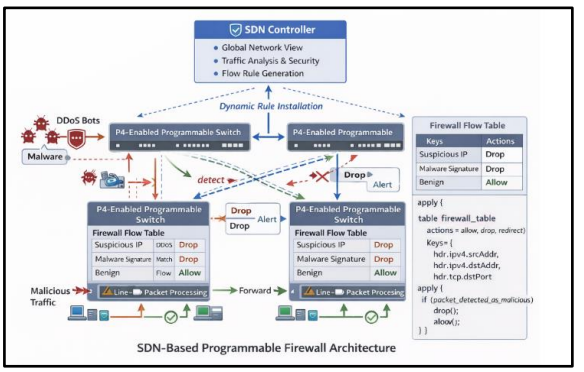

Figure 1

SDN-Based Programmable Firewall Architecture for Secure Traffic Management.

3. Proposed Work

3.1 *Three-Tier SDN-Managed Lightweight ECC Framework*

In this section, we propose a three-tier secure communication framework for 6G Wireless Sensor Networks (WSNs) that integrates lightweight Elliptic Curve Cryptography (ECC) with Software-Defined Networking (SDN) to achieve secure, scalable, and energy-efficient data transmission. The architecture consists of the sensor layer, SDN control layer, and application/cloud layer, enabling centralized security orchestration while preserving lightweight operations at resource-constrained sensor nodes.

Security is established using elliptic curves over discrete finite fields. Let the elliptic curve Eover a prime field $\mathbb{F}_p$ be defined as

$$E: y^2 \equiv x^3 + ax + b(\mathrm{mod}p),$$

where $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \equiv /0(\mathrm{mod}p)$. Let G be the base point of prime order $n$on E.

Each sensor node S_i selects a private key $d_i \in [1, n-1]$ and computes its public key

$$Q_i = d_i G.$$

The SDN controller authenticates nodes, verifies public keys, and maintains secure key-to-identity mappings.

For secure communication between nodes S_i and S_j, a shared session key is derived using Elliptic Curve Diffie–Hellman (ECDH):

$$K_{ij} = d_i Q_j = d_j Q_i.$$

A symmetric session key is generated using a lightweight hash function:

$$K_s = H(K_{ij}).$$

Sensor data M_i is encrypted as

$$C_i = E_{K_s}(M_i),$$

where $E_{K_s}(\cdot)$ denotes lightweight symmetric encryption.

The SDN controller dynamically installs secure flow rules expressed as

$$F = \{S_i, S_j, K_s, T_{exp}\},$$

where T_{exp} is the session of a lifetime.

Algorithm 1: SDN-Managed Lightweight ECC-Based Secure Communication
Input: Elliptic curve parameters (E, G, n), sensor nodes S_i, S_j **Output:** Secure ciphertext C_i
Step 1: SDN controller initializes elliptic curve parameters $(E, G, n)$and broadcasts them to all sensor nodes.
Step 2: Each sensor node S_i randomly selects a private key $d_i \in [1, n-1]$.
Step 3: Sensor node S_i computes its public key $Q_i = d_i G$ and registers it with the SDN controller.

Step 4: SDN controller verifies Q_i, authenticates S_i, and stores the key mapping.
Step 5: When S_i intends to communicate with S_j, the SDN controller retrieves $Q_j$and distributes it securely.
Step 6: Both nodes compute the shared secret using ECDH:
$K_{ij} = d_i Q_j = d_j Q_i.$
Step 7: The session key is derived as $K_s = H(K_{ij})$.
Step 8: Sensor node S_i encrypts sensed data M_i using symmetric encryption:
$C_i = E_{K_s}(M_i).$
Step 9: SDN controller installs flow rule $F = \{S_i, S_j, K_s, T_{exp}\}$ and forwards encrypted data.
Step 10: Upon expiration of T_{exp}, the SDN controller triggers key renewal.

3.2 *Security Game for Key Establishment (AKE Model)*

Define the Authenticated Key Exchange (AKE) experiment $\text{Exp}_{\mathcal{A}}^{\text{AKE}}(\lambda)$.

1. Setup:
   Challenger selects curve parameters (E, G, n).
2. Queries:
   $\mathcal{A}$may issue:
   - Execute(i, j): Obtain honest protocol transcript
   - Send(i, j, m): Inject message m
   - Reveal(i): Reveal session key
   - Corrupt(i): Reveal long-term key d_i
3. TestQuery:
   Challenger selects a random bit b:
$$K_b = \begin{cases} K_{\text{session}}, & b = 1 \\ U \xleftarrow{R} \{0,1\}^{\lambda}, & b = 0 \end{cases}$$
4. Goal:
   Adversary outputs b'.

Define advantage:

$$\text{Adv}_{\mathcal{A}}^{\text{AKE}}(\lambda) = |\Pr[b = b'] - \tfrac{1}{2}|.$$

3.3 *Perfect Forward Secrecy (PFS) Model*

Session $s$uses ephemeral secrets:

$$r_S^{(s)}, r_{BS}^{(s)} \xleftarrow{R} [1, n-1].$$

Session key:

$$K^{(s)} = \text{KDF}(x(r_S^{(s)} r_{BS}^{(s)} G)).$$

Even after Corrupt(S), Corrupt(BS):

$$\Pr\left[\mathcal{A}(T_S, T_{BS}) = K^{(s)}\right] \leq \epsilon_{\text{ECDLP}}.$$

3.4 *Signature Security Model (EUF-CMA) & Resistance to Replay Attacks*

Define experiment $\text{Exp}_{\mathcal{A}}^{\text{EUF-CMA}}(\lambda)$.

- $\mathcal{A}$obtains signatures:

$$\sigma_i = \text{Sign}(d, m_i)$$

- Adversary outputs (m^*, σ^*)

  Forgery is successful if:

$$\text{Verify}(Q, m^*, \sigma^*) = 1 \wedge m^* \notin \{m_i\}.$$

4. Experimental Results and Performance Evaluation

To evaluate the effectiveness of the proposed SDN-managed lightweight ECC framework, extensive simulations were conducted to analyze latency, energy consumption, scalability, and SDN control-plane stability. The proposed ECC-based approach was compared against a conventional RSA-based security scheme under increasing network scale. Performance metrics were recorded by varying the number of sensor nodes from 50 to 500, reflecting realistic 6G WSN deployment scenarios.

4.1 *End-to-End Latency Analysis*

End-to-end latency represents the total time required for secure data transmission, including key establishment, encryption, forwarding, and SDN flow setup. Figure 2 compares ECC and RSA as the number of sensor nodes increases. Results show ECC consistently achieves lower latency due to smaller key sizes and faster operations, making it suitable for delay-sensitive 6G WSN applications.

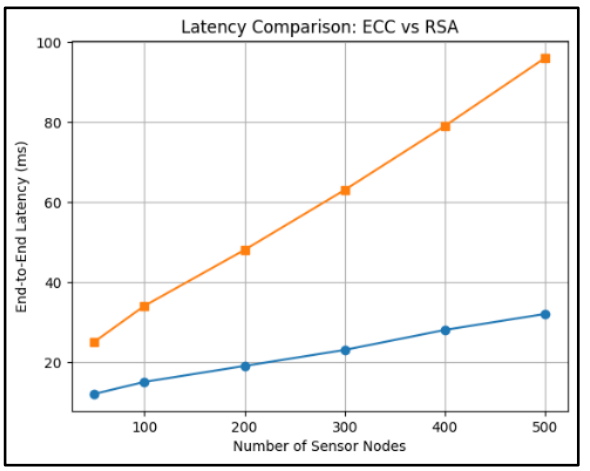

Figure 2
End-to-end latency comparison of ECC and RSA under varying sensor node density.

4.2 *Energy Consumption Evaluation*

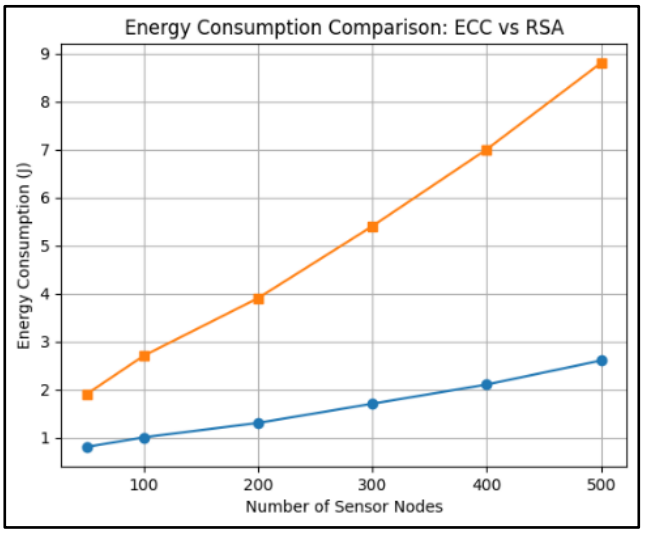

Figure 3
Energy consumption comparison between ECC and RSA schemes.

Energy efficiency is critical for resource-constrained sensor nodes. Figure 3 compares the average energy consumption of ECC and RSA-based security mechanisms. Results show that ECC consumes significantly less energy, while RSA incurs higher computational overhead, leading to faster energy depletion at higher node densities.

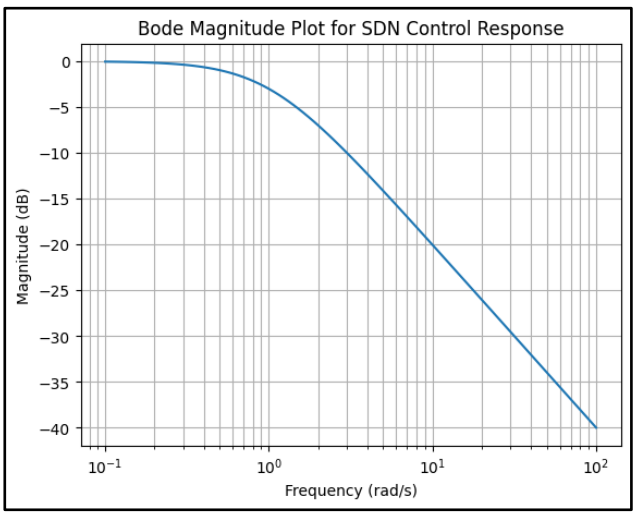

Figure 4
Bode magnitude plot representing SDN control-plane response.

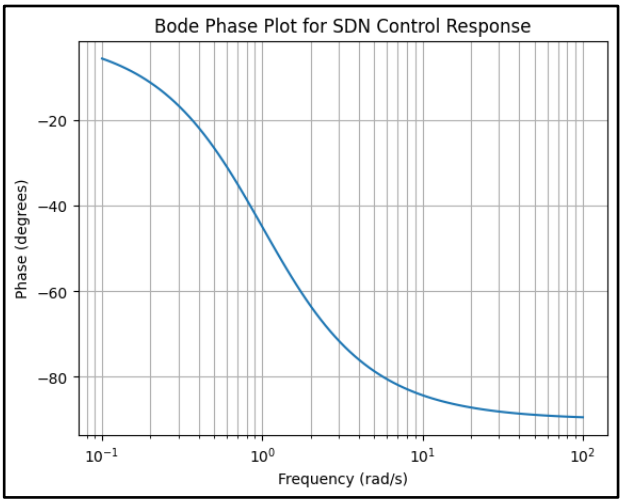

Figure 5
Bode phase plot illustrates SDN controller stability.

4.3 *SDN Control-Plane Stability Analysis Using Bode Plots*

The dynamic behavior and stability of the SDN control plane were analyzed using frequency-domain analysis. Figure 4 shows the Bode magnitude plot of the SDN controller response, indicating stable gain characteristics at low frequencies and controlled attenuation at higher frequencies. This behavior confirms the controller's ability to handle increasing traffic and security policies without oscillations or instability. The corresponding Bode phase plot is depicted in Figure 5, illustrating a smooth phase transition with no abrupt shifts. The absence of phase discontinuities confirms stable control-plane operations, even under frequent flow updates and key renewals.

5. Conclusion

This paper proposes a lightweight ECC-based security framework for 6G WSNs using an SDN-managed three-tier architecture. The approach ensures strong security with low computational overhead, improves energy efficiency and latency, and enables scalable key management and adaptive security enforcement for next-generation sensor networks.

References

[1] P. Karthikeyan and K. Brindha, "Smart data flow: A trust-driven hybrid fragmentation framework for optimizing data transmission in IoT-enabled edge–fog–cloud systems," *Computing*, vol. 107, Art. no. 250 (2025), doi: 10.1007/s00607-025-01491-2.

[2] I. Araújo, A. Brízido, and S. R. Lima, "Virtual network function development for NG-PON access network architecture," *J. Netw. Syst. Manage.* (2023), doi: 10.1007/s10922-023-09765-w.

[3] C. Kumar, "Performance investigation of 400 × 100 Gb/s ultra-dense WDM system using different modulation techniques with varying channel spacing," *Wireless Pers. Commun.*, vol. 134, no. 4, pp. 2203–2233 (2024), doi: 10.1007/s11277-024-11008-3.

[4] O. M. A. El-Hamed, F. E. A. El-Samie, W. Badawy, and S. M. A. El-Atty, "Blockchain-based framework for secure communication in vehicular ad hoc network (VANET)," *J. Opt.* (2025), doi: 10.1007/s12596-025-02760-1.

[5] B. S. Heera, A. Sharma, V. Lohani, and Y. N. Singh, "Routing, modulation, core and spectrum assignment techniques for crosstalk management in multi-core fiber based spatially multiplexed elastic optical networks," *Photon. Netw. Commun.*, vol. 48, nos. 1–3, pp. 35–50 (2024), doi: 10.1007/s11107-024-01021-8.

[6] F. A. Silva, F. A. Trinta, M. S. Bonfim, J. A. F. de Macedo, P. A. Rego, and V. Lagrota, "Performance evaluation of cloud native applications: A systematic mapping study," J*ournal of Network and Systems Management*, vol. 33, Art. no. 98 (2025), doi: 10.1007/s10922-025-09937-w.

[7] S. Chandra, K. Mondal, and S. Singha, "Protective and fragmentation-aware routing of unicast data centre traffic in disaster-prone online SDM-EONs," *Discover Applied Sciences*, vol. 7, Art. no. 264 (2025), doi: 10.1007/s42452-025-06739-2.

[8] S. Pandiaraj, R. Krishnamoorthy, S. Ushasukhanya, J. V. N. Ramesh, R. A. Alsowail, and S. Selvarajan, "Optimization of IoT circuit for flexible optical network system with high speed utilization," *Optical and Quantum Electronics*, vol. 55, Art. no. 1206 (2023), doi: 10.1007/s11082-023-05452-x.

[9] D. Prakash and M. Managuli, "An optimization approach to DWDM network reconfiguration through reinforcement learning," *SN Computer Science*, vol. 5, Art. no. 1069 (Nov. 2024), doi: 10.1007/s42979-024-03438-4.

[10] N. Chen, W. Yue, Y. Xu, W. Guo, Y. Xiao, Z. Ren, X. Ding, M. Li, Y. Xu, T. Wu, and C. Liu, "Design and simulation of a compact polarization beam splitter based on dual-core photonic crystal fiber with elliptical gold layer," *Scientific Reports*, vol. 14, no. 1, Art. no. 18017 (2024), doi: 10.1038/s41598-024-68995-3.

[11] B. L. V. S. Aditya and S. N. Mohanty, "Design of an efficient model for fake profile detection on social media using advanced feature engineering and deep learning techniques," *J. Inf. Optim. Sci.*, vol. 46, no. 6, pp. 1803–1810 (2025), doi: 10.47974/JIOS-2009.

[12] S. D. Bahinipati and B. K. Pattanayak, "A novel blockchain-enabled smart contract for smart city e-governance ecosystem," *J. Inf. Optim. Sci.*, vol. 46, no. 6, pp. 1831–1840 (2025), doi: 10.47974/JIOS-2012.

[13] Z. S. Alsham, E. Bahçekapılı, and A. Ayaz, "Trends in IoT applications in smart campuses: A topic modeling approach," *COLLNET J. Scientom. Inf. Manage.*, vol. 19, no. 1, pp. 21–40 (2025), doi: 10.47974/CJSIM-2024-017.

[14] W. Sripanya, W. Rungrottheera, and P. Hyunsin, "Fourier series analysis and computation based on function characteristics," *J. Interdiscip. Math.*, vol. 28, no. 6, pp. 2109–2120 (2025), doi: 10.47974/JIM-2352.

Received January, 2026