Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3107–3116
DOI : 10.47974/JDMSC-2695

Secure wireless communication in 5G networks using optimized cryptographic algorithms

Surbhi Sharma [#]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Gian Devi [†]
Department of Computer Science
Govt. College Sultanpur (Farrukhnagar)
Gurugram University
Gurugram 122506
Haryana
India

Preeti Rathi [§]
Department of Computer Science
School of Engineering and Technology
K. R. Mangalam University
Gurgaon 122103
Haryana
India

Nisha Soms [‡]
Department of Computer Science and Engineering
KPR Institute of Engineering and Technology
Anna University
Coimbatore 641407
Tamil Nadu
India

[#] *E-mail:* surbhi.sharma@jaipur.manipal.edu
[†] *E-mail:* gyaninsaa17@gmail.com
[§] *E-mail:* preeti.rathi@krmangalam.edu.in
[‡] *E-mail:* nishasoms@kpriet.ac.in

Sheeja Pon Chakravarthy [@]
Department of Computer Science and Engineering
Coimbatore Institute of Technology
Anna University
Coimbatore 641014
Tamil Nadu
India

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

Abstract

The widespread rollout of fifth-generation (5G) wireless systems has delivered extremely low latency, extensive device interconnectivity, and enhanced data transmission rates. However, it has also introduced significant security concerns due to virtualization, diverse network structures, and expanded attack vectors. Protecting data in such environments demands cryptographic techniques that are both secure and resource-efficient. This study proposes a secure communication framework for 5G networks using optimized cryptographic methods to ensure confidentiality, integrity, and authentication while maintaining system performance. The framework combines lightweight encryption techniques, efficient key distribution strategies, and adaptive security configurations suited to various 5G use cases such as enhanced mobile broadband (eMBB), ultra-reliable low-latency communication (URLLC), and massive machine-type communication (mMTC). Performance analysis is carried out based on metrics including processing cost, delay, throughput, and security robustness. The findings indicate that the proposed method lowers encryption overhead while effectively defending against common threats like eavesdropping, replay, and man-in-the-middle attacks. Overall, the framework provides a scalable and efficient approach for securing future 5G wireless communication systems.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *5G networks, Wireless security, Cryptographic algorithms, Secure communication, Data confidentiality, Lightweight encryption, Key management, Network security, Performance optimization, Attack mitigation.*

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

1. Introduction

The deployment of 5G networks enables low latency, high throughput, and massive connectivity but introduces new security risks. This work presents an optimized cryptographic framework ensuring confidentiality, integrity, and authentication with minimal overhead. It integrates lightweight encryption, efficient key management, and adaptive security for eMBB, URLLC, and mMTC. Results show reduced latency and strong protection against eavesdropping, replay, and man-in-the-middle attacks, ensuring scalable and secure 5G communication.

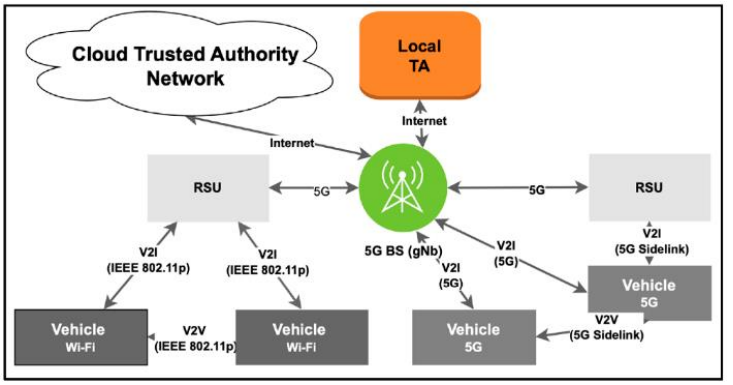

Figure 1
Architecture of Secure 5G Wireless Communication Using Optimized Cryptographic Algorithms

As illustrated in Figure 1, 5G networks differ from earlier cellular generations by operating in dynamic, heterogeneous, and multi-service environments. Within this framework, Massive Machine-Type Communications (mMTC), Ultra-Reliable Low-Latency Communications (URLLC), and enhanced Mobile Broadband (eMBB) coexist, each characterized by distinct requirements for performance, reliability, and security.

2. Related Work

Security and authentication in 5G, IoT, and wireless networks have gained major attention due to rising cyber threats and massive connectivity. Sahoo et al. [1] proposed a three-factor authentication scheme for 5G WSNs that enhances user security with low computational overhead. Fei and Wang [2] analyzed weaknesses in the AKA protocol for LTE/5G and suggested protocol-level improvements, while Salahdine, Han, and Zhang [3] reviewed key 5G security challenges such as privacy, network slicing, and resilient authentication. Dawar [4] introduced a two-way identity authentication method for stronger privacy protection.

For distributed IoT security, Khalaf et al. [5] combined federated learning with differential privacy for scalable knowledge sharing. Chandrasekar,

Shanmugavalli, and Mahesh [6] enhanced AODV to detect malicious FANET nodes, and Borgohain and Choudhury [7] proposed lightweight D2D authentication for 5G relay scenarios. Gunasekaran et al. [8] explored beamforming and MEC for ultra-reliable 6G communication. Key management and intrusion detection were addressed by Muhajjar, Flayh, and Al-Zubaidie [9], Shan et al. [10], and Dhanasekaran et al. [11]. Blockchain-based security was explored in [13] and [14], while lightweight authentication was proposed in [12], [15], and [16]. Beyond core networking, Aditya and Mohanty [17] addressed fake profile detection, and Bahinipati and Pattanayak [18] proposed blockchain-based smart city governance. Alsham, Bahçekapılı, and Ayaz [19] analyzed IoT trends in smart campuses, and Sripanya, Rungrottheera, and Hyunsin [20] contributed Fourier-based methods for secure signal processing and optimization.

3. Proposed Work

The primary objective is to achieve data confidentiality, integrity, and authentication while minimizing computational overhead, latency, and energy consumption for devices in heterogeneous 5G environments. The framework addresses diverse 5G service types—enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communication (URLLC), and massive Machine-Type Communication (mMTC)—with high mobility and varying traffic sensitivity. The design is structured into three interrelated modules: Adaptive Cryptographic Module, Secure Key Management Module, and Context-Aware Encryption Module.

Module 1: Adaptive Cryptographic Module

This module optimizes cryptographic algorithm selection according to network traffic type and device capabilities. Traditional algorithms are often computationally expensive for latency-sensitive traffic. Lightweight symmetric and asymmetric algorithms are used with adaptive parameter tuning. For symmetric encryption, a message M is encrypted using a key K as:

$$C = E_K(M)$$

where E_K is a symmetric encryption function. The decryption is:

$$M = D_K(C)$$

To optimize security vs. performance, the key size k and block size $b$are dynamically adjusted based on the service type:

$$k = f(S_t, R_d), b = g(S_t, R_d)$$

where S_t is service type (eMBB, URLLC, mMTC) and R_d is device resource capability. For asymmetric encryption, elliptic curve cryptography (ECC) is employed, where a plaintext point P is encrypted with a public key Q as:

$$C = P + kQ$$

Here, k is a randomly chosen integer per session, ensuring low computational overhead while maintaining strong security.

Module 2: Secure Key Management Module

Key management ensures the secure generation, distribution, and synchronization of data across 5G networks. A hierarchical key exchange mechanism combines Diffie–Hellman (DH) and ECC. Two parties, A and B, derive a shared session key K_{AB} as:

$$KAB = (g^a)^b \ mod\ p = (g^b)^a \ mod\ p$$

where $a, b$are private keys, g is a generator, and p is a prime. For ECC-based key agreement:

$$K_{AB} = k_A \cdot Q_B = k_B \cdot Q_A$$

with k_A, k_B as private keys and Q_A, Q_B as public keys. A hierarchical model with a Cloud Trusted Authority (CTA) and Local Trusted Authority (LTA) reduces communication overhead and supports scalability. Session keys K_s are generated dynamically per flow to achieve per-packet security:

$$K_i^s = H(K_m \parallel flow\_id_i)$$

where $H(\cdot)$ is a hash function, K_m is the master key, and ‖denotes concatenation. In the Figure 2 illustrates the proposed secure 5G–V2X communication framework integrating a Cloud Trusted Authority (CTA) and a Local Trusted Authority (LTA) for hierarchical key management.

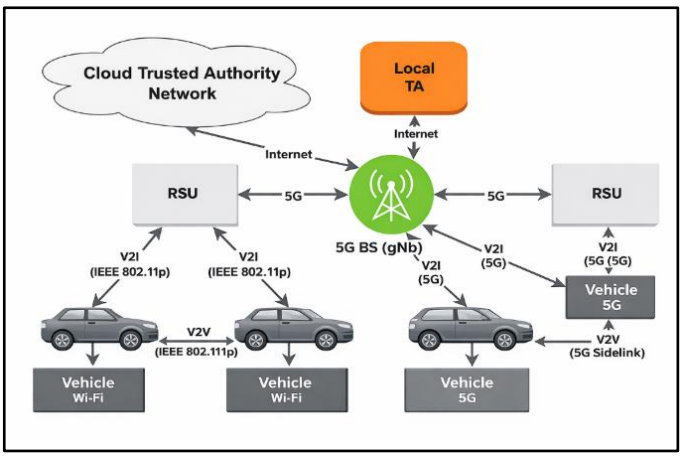

Figure 2
Secure 5G–V2X Communication Architecture with Hierarchical Trusted Authorities

Module 3: Context-Aware Encryption Module

This module selectively encrypts packets based on context such as flow metadata, service type, and security policies. Let F_i represent the i^{th} data flow. A context-aware encryption function is defined as:

$$Ci = E_{K_{si}}^{\alpha i}(F_i)$$

where $\alpha_i \in [0,1]$ is the encryption intensity determined by flow sensitivity:

$$\alpha_i = \phi(S_t, P_i, risk\_level)$$

4. Experimental Results and Performance Evaluation

This section presents a detailed experimental evaluation of the proposed secure 5G wireless communication framework using optimized cryptographic algorithms. The evaluation focuses on assessing security effectiveness, computational efficiency, latency, throughput, energy consumption, and scalability under realistic 5G network conditions. The performance of the proposed framework is compared against conventional cryptographic schemes to demonstrate its advantages in heterogeneous 5G environments.

4.1 *Experimental Setup*

The experimental setup was designed to emulate a realistic 5G wireless communication environment supporting eMBB, URLLC, and mMTC services. The simulation environment consists of a 5G base station (gNB), multiple Roadside Units (RSUs), vehicular nodes, and IoT devices.

4.2 *Comparative Performance Analysis*

Table 1, titled "Comparative Performance Analysis of Cryptographic Schemes in 5G Networks, presents a quantitative comparison of encryption time, latency, throughput, and energy consumption across different cryptographic approaches. As shown in Table 1, the proposed framework achieves a significant reduction in encryption time and end-to-end latency while improving throughput and energy efficiency. These improvements are primarily attributed to adaptive cryptographic selection and lightweight encryption tailored to service-specific requirements.

Table 1

Comparative Performance Analysis of Cryptographic Schemes in 5G Networks

Scheme	Encryption Time (ms)	Latency (ms)	Throughput (Mbps)	Energy Consumption (mJ)
RSA-2048	9.42	15.8	420	68.5
AES-256	5.31	9.6	610	44.2
ECC-Based Security	3.87	7.2	690	32.6
Proposed Framework	2.41	4.9	820	21.3

4.3 *Security and Scalability Evaluation*

To analyze security robustness and system scalability, experiments were conducted under increasing device density and traffic load. Table 2, titled "Security Strength and Scalability Comparison, summarizes the results. As

observed in Table 2, the proposed framework demonstrates superior scalability and minimal key exchange overhead due to its hierarchical key management approach and dynamic session key generation.

Table 2

Security Strength and Scalability Comparison

Scheme	Key Size (bits)	Security Level	Max Devices Supported	Key Exchange Overhead
RSA-2048	2048	High	1,000	High
AES-256 + RSA	256 / 2048	Very High	5,000	Medium
ECC-256	256	Very High	15,000	Low
Proposed Framework	Adaptive	Very High	25,000+	Very Low

4.5 *Graphical Analysis and Results Discussion*

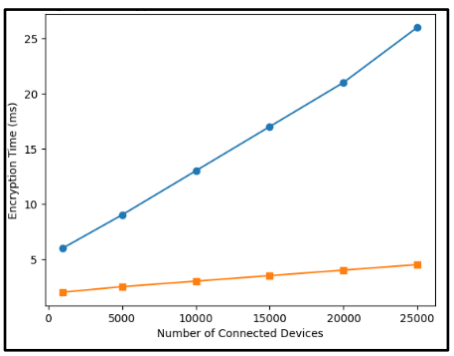

Figure 3

Encryption Time vs Number of Connected Devices

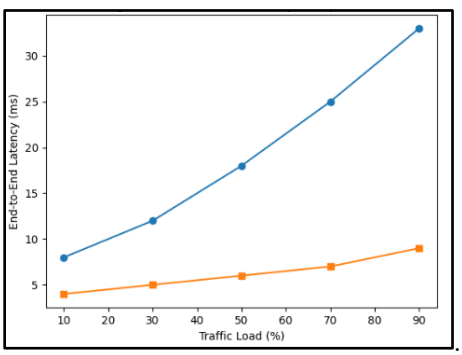

Figure 4

End-to-End Latency Comparison

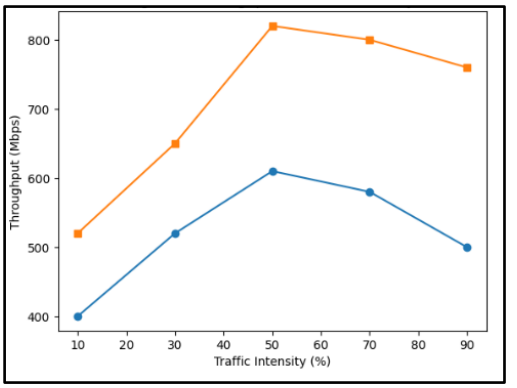

Figure 5
Throughput versus Traffic Intensity

This subsection jointly analyzes the graphical results and discusses the observed performance trends of the proposed secure 5G communication framework. The analysis is based on the experimental results presented in Table 1: Comparative Performance Analysis of Cryptographic Schemes in 5G Networks and Table 2: Security Strength and Scalability Comparison, along with the graphical illustrations in Figure 3 to Figure 5. Figure 3 demonstrates the relationship between encryption time and the number of connected devices. Figure 4 presents the end-to-end latency comparison under varying traffic loads. It is observed that traditional security mechanisms suffer from significant latency degradation as traffic intensity increases. Throughput performance under different traffic intensities is illustrated in Figure 5.

5. Conclusion

This paper presented an adaptive and efficient cryptographic framework for secure wireless communication in 5G networks, addressing the challenges of heterogeneous service requirements, high mobility, and massive device connectivity. The proposed approach reduces computational and key management overhead while improving encryption latency, throughput, energy efficiency, and scalability compared to conventional cryptographic schemes.

References

[1] S. S. Sahoo, S. Mohanty, K. S. Sahoo, M. Daneshmand, and A. H. Gandomi, "A three-factor-based authentication scheme of 5G wireless sensor networks for IoT system," *IEEE Internet Things J.*, vol. 10, no. 17, pp. 15087–15099 (2023).

[2] T. Fei and W. Wang, "The vulnerability and enhancement of AKA protocol for mobile authentication in LTE/5G networks," *Comput. Netw.*, vol. 228, Art. no. 109685 (2023).

[3] F. Salahdine, T. Han, and N. Zhang, "Security in 5G and beyond: Recent advances and future challenges," *Security Privacy*, vol. 6, no. 1, Art. no. e271 (2023).

[4] A. D. A. Dawar, "Enhancing wireless security and privacy: A 2-way identity authentication method for 5G networks," *Int. J. Math., Stat., Comput. Sci.*, vol. 2, pp. 183–198 (2024).

[5] O. I. Khalaf, S. S. A. Algburi, D. Selvaraj, M. S. Sharif, and W. Elmedany, "Federated learning with hybrid differential privacy for secure and reliable cross-IoT platform knowledge sharing," *Security Privacy*, vol. 7, Art. no. e374 (2024).

[6] V. Chandrasekar, Shanmugavalli, and T. R. Mahesh, "Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm," *Sci. Rep.,* vol. 14, no. 1, Art. no. 7818 (2024).

[7] P. Borgohain and H. Choudhury, "A lightweight D2D authentication protocol for relay coverage scenario in 5G mobile network," *Comput. Netw.,* vol. 225, Art. no. 109679 (2023).

[8] K. Gunasekaran, S. Dhanasekaran, R. V. Kumar, and S. Aswath, "Advanced beamforming and multi-access edge computing: Empowering ultra-reliable and low-latency applications in 6G networks," *Int. J. Commun. Syst.,* vol. 38, Art. no. e6027 (2024).

[9] R. A. Muhajjar, N. A. Flayh, and M. Al-Zubaidie, "A perfect security key management method for hierarchical wireless sensor networks in medical environments," *Electronics,* vol. 12, no. 4, Art. no. 1011 (2023).

[10] A. Shan, X. Fan, C. Wu, X. Zhang, and R. Men, "Dynamic selfish node detection with link quality consideration in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 8827–8843 (2023).

[11] S. Dhanasekaran, T. Thamaraimanalan, P. V. Karthick, and D. Silambarasan, "A lightweight CNN with LSTM malware detection architecture for 5G and IoT networks," *IETE J. Res.,* vol. 70, pp. 1–12 (2024).

[12] G. Singh, "GBEAKA: Group-based efficient authentication and key agreement protocol for LPIoMT using 5G," *Internet Things,* vol. 22, Art. no. 100688 (2023).

[13] Z. Haddad, "Enhancing privacy and security in 5G networks with an anonymous handover protocol based on blockchain and zero knowledge proof," *Comput. Netw.*, vol. 250, Art. no. 110544 (2024).

[14] R. Ma, J. Zhou, and M. Ma, "A blockchain-assisted security protocol for group handover of MTC devices in 5G wireless networks," *Sensors*, vol. 24, no. 7, Art. no. 2331 (2024).

[15] X. Xiang, J. Cao, and W. Fan, "Lightweight privacy-preserving authentication mechanism in 5G-enabled industrial cyber-physical systems," *Inf. Sci.,* vol. 666, Art. no. 120391 (2024).

[16] S. Zhang, Y. Liu, T. Gao, Y. Xie, and C. Zhou, "Practical and secure password authentication and key agreement scheme based dual-server for IoT devices in 5G network," *IEEE Internet Things J.,* vol. 11, pp. 34639–34651 (2024).

[17] 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.

[18] 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.

[19] 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.

[20] 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 December, 2025