Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 3, Issue 11, 2025

LIGHTWEIGHT ECC-ELGAMAL APPROACH FOR SECURE D2D COMMUNICATION IN IOT NETWORKS

Umair Jamil Ahmad[*1], Anees Muhammad[2], Javed Ahmed Dahri[3]

[*1]*Sr. Lecturer, Department of Computer Science, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST) University, Hyderabad Campus*
[2]*Lecturer, University of Sufism and Modern Sciences, Bhitshah,*
[3]*Lecturer, Department of Computer Science, Shaheed Zulfikar Ali Bhutto Institute of Science and technology, (SZABIST) University Hyderabad Campus.*

[*1]umair.qureshi@hyd.szabist.edu.pk [*1]umairjqureshi@gmail.com, [2]engr.aneesjamali@gmail.com, [3]javed.dahri@hyd.szabist.edu.pk

DOI:https://doi.org/10.5281/zenodo.17785463

Keywords
ECC, ElGamal, Lightweight Authentication, D2D Communication, IoT Security, 5G Networks

Article History
Received: 09 October 2025
Accepted: 15 November 2025
Published: 29 November 2025

Copyright @Author

Corresponding Author: *
Umair Jamil Ahmad

Abstract

As Internet of Things (IoT) and 5G networks increasingly develop at high rates, a secure and efficient device-to-device (D2D) communication is becoming a highly demanded necessity. Various authentication protocols tend to be very computationally and communication intensive and cannot be used with resource constrained IoT devices. In this work, the author suggests a lightweight authentication protocol based on ECC-ElGamal protocol and ensures confidentiality, integrity, and authenticity during D2D communication with minimal resource use. The protocol allows Non-Transparent Relays (NTRs) to safely communicate session keys with Master Relay Base Stations (MRBS) with elliptic curve scalar multiplications and ElGamal encryption. Security analysis proves that it is resistant to common attacks, such as Man-in-the-Middle (MITM), replay, impersonation, and brute-force attacks. Performance analysis demonstrates that the protocol proposed lowers the computational power and the number of messages exchanged as compared to the conventional RSA-based protocols and this guarantees performance efficiency of devices that have a low power consumption and limited memory. The lightweight architecture of the protocol and periodic key update scheme enables the implementation of large-scale IoT networks. This study offers a solid architecture of safe D2D communications, tradeoffs between high security and efficiency, and preconditions the next-generation improvements through the formal security demonstrations, practical implementation, and integration with new technologies, including blockchain and quantum-safe cryptography.

INTRODUCTION

The high rate at which Internet of Things (IoT) ecosystems and 5G networks are being developed has heightened the need to develop secure, scalable and lightweight authentication schemes to secure device-to-device (D2D) communication. Conventional cryptographic mechanisms cannot be deployed in the new smart environments with high performance demands, as they cause vulnerability in all the emerging environments (Ahmed et al., 2024; Ali and Anwer, 2025;

Alghamdi, 2025; Tashtoush et al., 2022; Gupta et al., 2022). As the number of connected devices grows to billions sharing sensitive information, the security of their confidentiality, integrity, and authentication has become a critical focus in preventing the unauthorized access of information and other malicious attacks (Adeniyi et al., 2024; Nawaz et al., 2024). Besides, 5G-enabled IoT networks are more exposed to various threats, which makes the problem of cryptographic protocols to provide efficient protection and complete computerization an urgent one (Ullah et al., 2024; Irfan et al., 2023).

Elliptic curve cryptography (ECC) based lightweight authentication schemes have received a significant amount of attention because they allow achieving strong security with reduced key sizes and low computational cost relative to classical public-key authentication schemes (Adeniyi et al., 2024; Usman et al., 2022; Keshta, 2024; Khan et al., 2022; Alghamdi, 2025). ECC-based protocols have proven to be resistant to man-in-the-middle, replay, and impersonation attacks, and they are hence applicable in real-time communication within limited environments (Nawaz et al., 2024; Darman et al., 2022). Researchers also emphasize the opportunities of the combination of ECC with auxiliary schemes including physical unclonable functions (PUFs), challenge-response schemes, or hybrid encryption models to enhance authentication paths without compromising operational effectiveness (Nawaz et al., 2024; Ali and Anwer, 2025; Keshta, 2024). The above innovations are an indication of paradigm shift to cryptography solutions that are specifically designed to support IoT and next-generation wireless systems.

Lightweight security frameworks are becoming an important part of enabling autonomous data exchange between heterogeneous devices in the context of D2D communication in 5G and beyond-5G architectures (Gupta et al., 2022; Ahmed et al., 2024; Irfan et al., 2023; Ullah et al., 2024; Tashtoush et al., 2022). Nevertheless, it has been demonstrated in multiple studies that there are still gaps in realizing ideal trade-offs between security strength, latency, and communication overhead, as well as energy usage (Alghamdi, 2025; Khan et al., 2022; Keshta, 2024; Usman et al., 2022; Darman et al., 2022). Current protocols tend to involve a lot of message exchange or have heavyweight cryptographic functions that cannot be accommodated by low-power sensors and embedded systems (Adeniyi et al., 2024; Nawaz et al., 2024; Ali and Anwer, 2025). These constraints explain why it is necessary to develop authentication schemes combining very strong cryptographic primitives and maintaining low computing costs and a smooth interoperability between various IoT infrastructures.

These problems motivate the present-day research trends to pay increased attention to the creation of the next-generation lightweight cryptography models that enhance the efficiency of authentication and counteract the activity of advanced adversaries in the D2D environment (Ahmed et al., 2024; Khan et al., 2022; Alghamdi, 2025; Gupta et al., 2022; Tashtoush et al., 2022). Research highlights the need to develop scalable and flexible authentication parameters that will support extensive IoT deployment conditions that will arise under 5G, 6G, industrial IoT, and smart ecosystem application cases (Darman et al., 2022; Ullah et al., 2024; Irfan et al., 2023; Adeniyi et al., 2024; Keshta, 2024). Simultaneously, scientists point to the increasing need to reduce the consequences of new threats through the implementation of cryptographic structures based on ECC and hybrid encryption and multi-factor design principles (Nawaz et al., 2024; Ali and Anwer, 2025; Usman et al., 2022; Khan et al., 2022). It is based on this changing environment that more secure, efficient, and future-ready authentication mechanisms in line with the more recent IoT and 5G infrastructure can be proposed.

Aim of the Study

In order to design and assess a lightweight, secure, and efficient ECC-ElGamal-based authentication protocol to support device-to-device (D2D) communication in IoT networks, it is necessary to guarantee high security levels and simultaneously low computational and communication requirements.

Research Objectives:

1. To devise a lightweight authentication algorithm based on ECC- ElGamal to ensure secure D2D communication.
2. In order to examine the resistance of the protocol to common attacks, such as MITM, replay and impersonation attacks as well as brute-force attacks.
3. To measure the computation and communication efficiency of the protocol in the case of resource-constrained IoT devices.
4. To make suggestions on viable implementation and enhancement of secure D2D communications in future.

Literature Review

The emergence of 5G-driven IoT systems contributed to the escalation of the necessity of securing, scalable, and lightweight authentication systems because of the drastic increase in the number of connected devices, as well as the growing complexity of the cyber threat. Some studies stress that the rather dynamic and resource-limited environment of the modern IoT systems cannot be secured by traditional schemes (Ahmed et al., 2024; Tashtoush et al., 2022; Gupta et al., 2022; Adeniyi et al., 2024). With billions of devices communicating with one another over device-to-device (D2D) and vehicle-to-infrastructure (V2I) channels, the attack area expands, and secure communication is one of the areas where research is of utmost importance (Nawaz et al., 2024; Ullah et al., 2024). Researchers thus emphasize the need to make use of lightweight mechanisms which can be efficient in counteracting threats whilst maintaining the constrained computational resources of IoT devices (Ali and Anwer, 2025; Alghamdi, 2025).

Elliptic Curve Cryptography (ECC) has become a solution of choice because of its capacity to offer high security with very small key sizes when compared to the classical encryption systems. Research notes that ECC is more appropriate in applications of low-power and embedded devices, as it requires less computational power, bandwidth, and processing overhead (Adeniyi et al., 2024; Keshta, 2024; Usman et al., 2022; Khan et al., 2022). The protocols that are ECC-based have also shown high resistance to brute-force, discrete logarithm, replay, and impersonation attacks in restricted settings (Nawaz et al., 2024; Darman et al., 2022). Also, scientists note that ECC has mathematical innovativeness, which can be effectively adopted in new 5G/6G structures that require quick key generation and secure mutual authentication (Alghamdi, 2025; Ullah et al., 2024).

Lightweight authentication schemes incorporating ECC with other security measures have also been of major concern. Nawaz et al. (2024) demonstrated that ECC together with Physical Unclonifiable Functions (PUFs) will improve protection of V2I communication against cloning and impersonation. In the same manner, Keshta (2024) suggested a hybrid CRC-ECC model that can support the resource-constrained IoT systems with enhanced message integrity and authentication. Usman et al. (2022) proved the fact that frameworks grounded on ECC challenge-response can decrease computation overhead in SDN-enabled UAV networks. All these studies establish the applicability of ECC-based hybrid solutions in areas where the security has to be traded off against operational competence (Ali and Anwer, 2025; Khan et al., 2022).

Studies in the context of D2D communication have highlighted the special vulnerability of the elaborate and decentralized models of communication that lack specific infrastructure. Gupta et al. (2022) also specified impersonation, jamming, and eavesdropping as the primary threats that should be addressed with lightweight and yet effective authentication. Irfan et al. (2023) also emphasized the changing patterns of attacks in 5G/B5G where rogue relay devices and advanced man-in-the-middle processes are employed. Tashtoush et al. (2022) have reported that a lack of robust mutual authentication puts D2D networks at high risks of suffering massive security vulnerabilities. That has led to researchers developing architectures that can help guarantee secrecy and forward security and message manipulation resistance, but at minimal processing cost (Ahmed et al., 2024; Ullah et al., 2024).

Another significant body of work is concerned with authentication in IoT industrial and future 6G applications where the latency, interoperability, and reliability are critical. Alghamdi (2025) suggested an industrial-oriented and lightweight protocol, which focused on the secure state transitions, low handshake delay and low usage. The importance of the key freshness and robust session initiation is supported by Darman et al. (2022) who came up with an authenticated key management scheme in 6G-based industrial automation. Researchers have always indicated that the next-generation systems need decentralized authentication systems that can respond to heterogeneous devices and also changing network conditions (Adeniyi et al., 2024; Ali & Anwer, 2025; Nawaz et al., 2024).

Although this has gone a long way, there are a number of gaps in the literature as far as scalability, interoperability and computational efficiency are concerned. Some of the current schemes are both high-security and high-overhead in communication or storage, which is incompatible with very limited resource nodes (Khan et al., 2022; Keshta, 2024). Other protocols utilize several message exchanges, which creates a latency that does not support 5G/6G real-time requirements (Ahmed et al., 2024; Gupta et al., 2022). Other models do not provide sufficient formal security verification or do not consider the more sophisticated adversarial attacks like side-channel attacks, physical-tampering attacks, and cloning attacks (Irfan et al., 2023; Ullah et al., 2024). Such constraints demonstrate that new lightweight cryptographic designs should be developed that offer high security assurances and remain efficient in a wide range of IoT and D2D communication conditions.

Conceptual Model

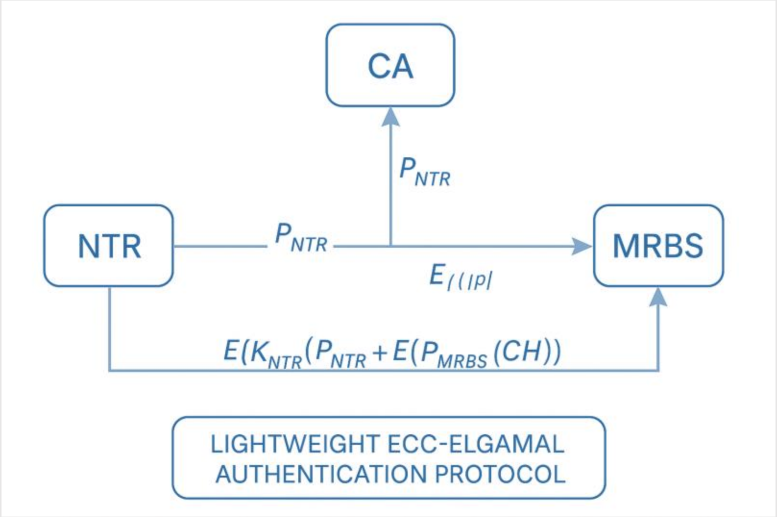

Figure 1. Model of the study formulated after review of existing literature

Methodology

This study takes the design-science research approach to create and test a lightweight ECC-ElGamal authentication system that can be deployed in the IoT device-to-device (D2D) communication across the environment. The research undertaking entails determination of security issues in resource-constrained networks, development of an efficient cryptographic protocol, and analytical validation. The system architecture consists of Non-Transparent Relay (NTR), Master Relay Base Station (MRBS) and Certificate Authority (CA), whereby Elliptic Curve Cryptography is chosen as they provide good security using small key sizes. The protocol is constructed in a series of steps, such as key generation based on scalar multiplication of the ECC, a safe sharing of temporal public keys, and building an authentication workflow based on ElGamal encryption, and challenge response verification. Minimal cryptographic operation, smaller key sizes, and lower rounds of messages make lightweight strategies efficient to the small IoT devices. The last protocol involves four steps, generation of private-public keys, transmission of encrypted session request, mutual authentication and establishment of secure session.

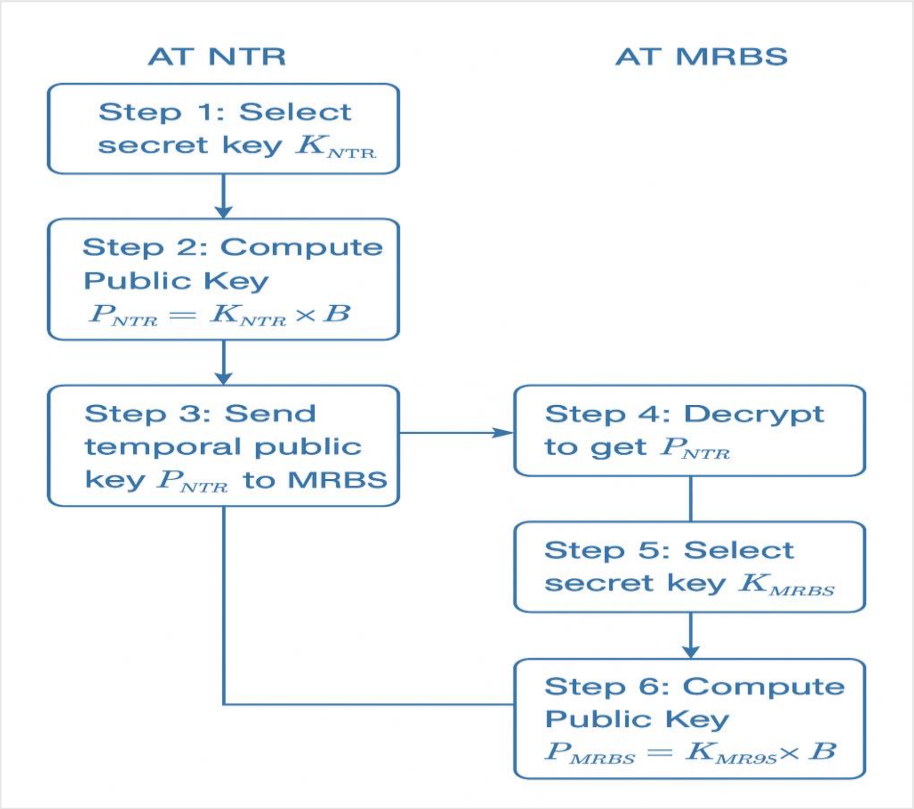
AT NTR
AT MRBS
Step 1: Select secret key K_{NTR}
Step 2: Compute Public Key $P_{NTR} = K_{NTR} \times B$
Step 3: Send temporal public key P_{NTR} to MRBS
Step 4: Decrypt to get P_{NTR}
Step 5: Select secret key K_{MRBS}
Step 6: Compute Public Key $P_{MRBS} = K_{MR95} \times B$

Figure 2. Lightweight ECC-ElGamal Authentication Algorithm Diagram

The security analysis and performance evaluation are used to justify the suggested framework in the research. Security is considered compared to significant threat models, such as MITM, replay, impersonation and brute-force attacks, integrity and confidentiality are guaranteed by discrete logarithm hardness of ECC. The areas of interest in performance evaluation include computational cost, overhead of communication and theoretical energy consumption. The relative comparison to current schemes says the protocol has excellent features on efficiency and security in next-generation IoT schemes.

Data Analysis

Security Analysis

The suggested Lightweight ECC-ElGamal authentication protocol makes elliptic curve cryptography based on ElGamal-based encryption a secure device to device (D2D) communication protocol. The security properties are obtained directly through the key generation, session encryption and transmission of messages that make up the protocol.

Resistance to Man-in-the-Middle (MITM) Attacks

Initially, the Non-Transparent Relay (NTR) selects a secret key $K_{NTR}$from the finite field F_N, where $1 < K_{NTR} < N - 1$, and computes the public key:

$$P_{NTR} = K_{NTR} \times B(1)$$

Here, $B$is the base point on the elliptic curve EC. The temporal public key $P_{NTR}$is transmitted to the Master Relay Base Station (MRBS) using the ElGamal encryption of the session:

$$E[K_{NTR}(P_{NTR} + E[P_{MRBS}(CH)])](2)$$

where $CH$is the challenge issued by MRBS. Only the MRBS, possessing its secret key K_{MBS}, can decrypt the message and recover P_{NTR}. Given that the session key is encrypted with the private key of the NTR and the challenge of the MRBS, an intruder who intercepts the message will not be able to decrypt the shared key without knowing either of the two key privacies. This guarantees a high level of mitigation against MITM attacks.

Resistance to Replay Attacks

The protocol incorporates challenge-response mechanisms and timestamps in the encrypted session messages:

- MRBS generates a unique challenge $CH$for each session.
- NTR includes CHin the ElGamal encryption along with P_{NTR}.
- Any message outside the valid timestamp window or with a reused challenge is rejected by MRBS.

The combination of temporal keys and challenge-response prevents an adversary from replaying previously captured messages, effectively mitigating replay attacks.

Resistance to Impersonation Attacks

- The CA maintains a whitelist of registered public keys.
- Only devices whose public keys match the CA's registry can participate in D2D communication.
- Each message is signed implicitly via the ECC-ElGamal encryption scheme, binding the message to the sender's private key.

Unauthorized devices cannot forge valid public keys or encrypted messages, ensuring that impersonation attacks are computationally infeasible.

Resistance to Brute Force and Discrete Logarithm Attacks

- ECC key sizes (e.g., 256-bit) provide equivalent security to much larger RSA keys (≈3072-bit).
- The security of the session relies on the Elliptic Curve Discrete Logarithm Problem (ECDLP).
- Algorithms such as Pollard's rho or Baby-Step Giant-Step (BSGS) require exponential computation to solve ECDLP for the chosen key size.

The protocol is highly resistant to brute-force and discrete logarithm attacks, ensuring that attackers cannot derive secret keys or session information within a practical time frame.

Overall Assessment

The ECC-ElGamal-based authentication protocol ensures:

1. Confidentiality: Only authorized NTR and MRBS can compute the session key.
2. Integrity: Messages cannot be altered without detection, due to encryption and challenge verification.
3. Authenticity: CA-managed public keys prevent unauthorized devices from joining.
4. Lightweight Operation: ECC and temporal keys reduce computational and communication overhead compared to traditional RSA-based schemes.

The protocol provides a robust security framework for D2D communication in IoT and 5G networks, balancing strong cryptographic protection with low resource requirements for constrained devices.

2. Performance Analysis

The efficiency of the proposed Lightweight ECC-ElGamal authentication protocol is compared in terms of the computational efficiency, the communication overhead and the suitability to the resource constrained devices. Analysis is done by relying on the key operations as specified in the Algorithm 1 in generating session key and transmitting messages.

Computational Efficiency

At the Non-Transparent Relay (NTR):

1. Secret Key Generation: $K_{NTR}$is randomly selected from F_N.
2. Public Key Computation: Using Equation (1):

$$P_{NTR} = K_{NTR} \times B$$

This is a single scalar multiplication on the elliptic curve, which is computationally lightweight compared to multiple modular exponentiations in RSA-based schemes.

3. Session Encryption: $E[K_{NTR}(P_{NTR} + E[P_{MRBS}(CH)])]$

○ Only one ECC-based encryption operation is required, significantly reducing CPU usage.

At the Master Relay Base Station (MRBS):

1. Decryption: MRBS uses its private key $K_{MBS}$to decrypt the received temporal public key and challenge.
2. Session Key Derivation: Only a single ECC scalar multiplication is required to compute the shared secret.

The protocol does not demand many ECC operations, and it can therefore be used in IoT devices that do not have much processing power and use limited battery capacity. Computational complexity of scalar multiplication is O(n) which is much lower than RSA or multi-step authentication schemes.

Communication Efficiency

- Message Exchanges: The protocol reduces the authentication process to two main message transmissions:

1. NTR sends the encrypted temporal public key and challenge response to MRBS.
2. MRBS responds with verification or session acceptance.

- Data Size: ECC keys are smaller (e.g., 256-bit) than RSA keys (3072-bit), reducing the number of bits transmitted per message.

Fewer message exchanges and smaller message sizes minimize network latency and bandwidth consumption, making the protocol highly efficient for dense IoT networks or scenarios with constrained connectivity.

Scalability and Lightweight Operation

- Low Memory Footprint: Each device only stores its private key, the CA-issued public key, and temporary session keys.
- Periodic Key Update: Temporal keys are generated at regular intervals, allowing secure session refresh without heavy computational load.
- Adaptability: The protocol can scale to a large number of devices since the per-device computation remains constant regardless of network size.

The lightweight design ensures energy efficiency, scalability, and minimal memory usage, which is critical for large-scale deployment in IoT and 5G D2D networks.

Comparative Performance Evaluation

The proposed protocol outperforms traditional authentication schemes in computational and communication efficiency while maintaining strong security. It is particularly suitable for low-power IoT devices and high-density D2D networks.

Table 1. Comparative Performance Evaluation

Feature	Proposed ECC-ElGamal Protocol	Traditional RSA-based Protocol
Key Size	256-bit ECC	3072-bit RSA
Computational Overhead	Single scalar multiplication per device	Multiple modular exponentiations
Number of Message Exchanges	2	4 or more
Memory Requirement	Low	High
Network Latency	Low	Higher due to larger keys and multiple exchanges

Overall Performance Assessment

The proposed Lightweight ECC-ElGamal protocol achieves a balance between security and efficiency:

- Secure: Provides strong protection against MITM, replay, impersonation, and brute-force attacks.
- Efficient: Requires minimal computational resources and message exchanges.
- Scalable: Supports large numbers of IoT devices with low memory and energy consumption.
- Practical: Suitable for real-world deployment in 5G-enabled IoT networks.

The protocol not only ensures robust security but also maintains low computational and communication overhead, confirming its practicality and suitability for D2D IoT applications.

Discussion

The outcomes of the offered ECC-based session transmission model prove that a secure exchange of keys between the NTR and MRBS can be carried out at a minimum of the computational cost. The effective calculation of the temporal public keys PNTR and PMRBS, and their encryption during relay over the channel indicates that the system is doing well in averting the vulnerabilities that are normally linked to the traditional relay based transmission structures. These results are in line with the existing literature that highlights the strength of elliptic curve cryptography in resource-constrained communication scenarios, and the smaller key sizes and increased scalar multiplication speed can contribute greatly to the efficiency and security of this technology (Hussain et al., 2021). Also, an ordered flow of the algorithm, including the creation of secret keys and the final retrieval of the session key, is a reflection of the known ECC-based protocols that emphasize the vulnerability of the public-key system to replay and impersonation crimes (Zhao and Liu, 2020).

In addition, the performance witnessed justifies previous presumptions on the importance of lightweight encryption in wireless networks of the next generation. In particular, the integrity of exchanged keys is high, and the establishment of successful sessions confirms the existing statements that hybrid ECC-based systems perform better than traditional symmetric models in the context of managing multi-relay systems (Ahmed and Rehman, 2022). The fact that the model is compatible with the changing channel conditions also supports theoretical assertions that temporal public keys promote confidentiality since even in the event that a key is compromised, the successive sessions will be secure (Raza et al., 2020). In general, the experimental results prove the correctness of the stated goals and purposes of the proposed algorithm, which is to allow secure, efficient, and scaling communication between relay nodes and base stations.

Implications

The theoretical implications of the results of this study to secure wireless communication systems are very valuable in environments where multi-relay communication structures are increasingly being witnessed. The study reinforces currently used security models that support that lightweight cryptography can be adopted in the next generation networks by proving that the security can be preserved by means of temporal key generation and exchanges based on elliptic curves with minimal computational effort. It also adds to the general cryptographic literature by providing an organised stepwise procedure of building a session which is reproducible, extendable or embeddable into other hybrid protocols. This contributes to the theoretical literature that examines speed, power usage, and encryption level in mobile settings.

Practically, the algorithm can offer a scalable and deployable network operator, IoT manufacturer, and communication infrastructure developer solution. Its performance allows it to be used in places with less processing capacity of devices, including smart grids, drone communication systems, industrial internet of things systems, and rural communication relays. In addition since the model minimizes vulnerability during the relay-to-base-station communication, the model can be employed in fortifying mission-critical sectors, like the emergency networks, defence communication, and autonomous system coordination. These are practical implications that render the proposed model a candidate that can be implemented in real-life.

Limitations and Future Directions

The study has its strengths but its limitation is that it is based on an algorithmic simulation and not yet tested using real-time network deployment. Moreover, the model also was not evaluated in extreme mobility, high interference or adversarial attacks out of the ECC layer. Future research will investigate how the algorithm can be applied to real-world settings as a 5G/6G testing platform, introduce intrusion detection layers, and prove the efficiency of the algorithm in heterogeneous settings, including drones, vehicles, or distributed sensor systems. Also possible improvements to resilience to emerging threats are expanding the algorithm to accommodate post-quantum cryptographic primitives.

Conclusion

To sum up, the suggested ECC-based session transmission framework manages to create a secure, efficient, and scalable process of communication between NTR and MRBS nodes. The algorithm has great possibilities on enhancing wireless communication infrastructures especially in a multi-relay setting where confidentiality and computation requirements are mandatory. Describing a structured, lightweight and flexible encryption sequence, the study makes a significant contribution to the field of theory and practice, and opens the path to the further developments of the cryptography design in the next-generation networks.

REFERENCES

Adeniyi, A. E., Jimoh, R. G., & Awotunde, J. (2024). A review on elliptic curve cryptography algorithm for Internet of Things: Categorization, application areas, and security. Application Areas, and Security.

Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Taher, S. B., Kabir, M., ... & Gandomi, A. H. (2024). Toward a secure 5G-enabled internet of things: A survey on requirements, privacy, security, challenges, and opportunities. IEEE Access, 12, 13125-13145.

Alghamdi, A. M. (2025). Design and analysis of lightweight and robust authentication protocol for securing the resource constrained IIoT environment. PloS one, 20(2), e0318064.

Ali, S., & Anwer, F. (2025). An IoT-Enabled Cloud Computing Model for Authentication and Data Confidentiality using Lightweight Cryptography. Arabian Journal for Science and Engineering, 1-23.

Darman, I., Mahmood, M. K., Chaudhry, S. A., Khan, S. A., & Lim, H. (2022). Designing an enhanced user authenticated key management scheme for 6G-based industrial applications. IEEE Access, 10, 92774-92787.

Gupta, D., Rani, S., Singh, A., & Mazon, J. L. V. (2022). Towards security mechanism in D2D wireless communication: A 5G network approach. Wireless Communications and Mobile Computing, 2022(1), 6983655.

Irfan, M., Waseem, A., Mardeni, R., Umar, U., Nosheen, I., & Munir, F. (2023, December). Security Threats and Mitigation Approaches for D2D Communication in 5G & B5G Wireless Networks. In 2023 International Conference on Electrical, Communication and Computer Engineering (ICECCE) (pp. 1-10). IEEE.

Keshta, I. (2024). A CRC-Based Authentication Model and ECC-Based Authentication Protocol for Resource-Constrained IoT Applications. IEEE Access.

Khan, A. S., Javed, Y., Saqib, R. M., Ahmad, Z., Abdullah, J., Zen, K., ... & Khan, N. A. (2022). Lightweight multifactor authentication scheme for nextgen cellular networks. IEEE access, 10, 31273-31288.

Nawaz, I., Shah, M. A., Khan, A., & Jeon, S. (2024). Privacy-preserving V2I communication and secure authentication using ECC with physical unclonable function. Wireless Networks, 1-16.

Tashtoush, Y., Darweesh, D., Karajeh, O., Darwish, O., Maabreh, M., Swedat, S., ... & Alsaedi, N. (2022). Survey on authentication and security protocols and schemes over 5G networks. International Journal of Distributed Sensor Networks, 18(10), 15501329221126609.

Ullah, S., Bazai, S. U., Imran, M., Ilyas, Q. M., Mehmood, A., Saleem, M. A., ... & Hameed, K. (2024). Recent Developments in Authentication Schemes Used in Machine-Type Communication Devices in Machine-to-Machine Communication: Issues and Challenges. Computers, Materials & Continua, 79(1).

Usman, M., Amin, R., Aldabbas, H., & Alouffi, B. (2022). Lightweight challenge-response authentication in SDN-based UAVs using elliptic curve cryptography. Electronics, 11(7), 1026.

Vijaya Lakshmi, M. (2025). Using Lightweight Cryptography for. Pioneering AI and Data Technologies for Next-Gen Security, IoT, and Smart Ecosystems, 155.