Emerging Technologies and Engineering Journal

EngiScience Publisher

Research Article

Enhancing Efficiency and Security in MTC Environments: A Novel Strategy for Dynamic Grouping and Streamlined Management

Maloth Bhavsingh [1,*], K Samunnisa [1], A Mallareddy[2]

[1] Department of Computer Science and Engineering, Ashoka Women's Engineering College, Kurnool, 518001, India

[2] Department of IT, CVR College of Engineering, Hyderabad, Telangana, 501510, India

*Corresponding Author: Maloth Bhavsingh, E-mail: bhavsinghit@gmail.com

Article Info

Article History

Received Feb 19, 2024

Revised Mar 24, 2024

Accepted Apr 01, 2024

Keywords

MTC

Security

Efficiency

AHGMAKA

Lightweight Cryptography

Dynamic Group Management

Abstract

This study presents a new strategy to improve security and efficiency in Machine-Type Communication (MTC) networks, addressing the drawbacks of the existing Adaptive Hierarchical Group-based Mutual Authentication and Key Agreement (AHGMAKA) protocol. The AHGMAKA protocol, crucial for securing communication within groups of devices with limited resources, has been found to cause significant operational delays and inefficiencies. Our proposed solution integrates advanced cryptographic methods, including an optimized Authenticated Message Authentication Code (AMAC) and lightweight encryption, sophisticated optimization algorithms for dynamic grouping, and an efficient, lightweight group management protocol. It also introduces adaptive network management strategies to customize performance according to the needs of MTC networks. The effectiveness of this approach has been validated through empirical analysis, showing considerable improvements in operational performance and energy efficiency. These improvements mark a significant step toward achieving an optimal balance between efficiency and security for MTC networks. However, the research acknowledges ongoing challenges, including the trade-off between security and efficiency and the issue of compatibility with older devices, suggesting these as areas for future study. The paper outlines potential research paths, including using machine learning for better group management, adopting post-quantum cryptographic methods, applying hardware acceleration, and pushing to standardize these technologies. This work significantly advances the field of secure and efficient communication in MTC, a critical component of the growing Internet of Things (IoT) landscape, setting the stage for future breakthroughs.

1. Introduction

The rapid increase in Machine-Type Communication (MTC) devices within the Internet of Things (IoT) necessitates advanced security measures tailored for devices with limited resources. Although existing solutions like the Adaptive Hierarchical Group-based Mutual Authentication and Key Agreement (AHGMAKA) protocol facilitate secure communication among hierarchical groups, they are often marred

by high computational demands and intricate group management issues. These challenges diminish their effectiveness and scalability in widespread MTC applications [1]. This paper introduces a comprehensive strategy designed to overcome these hurdles, enhancing MTC communications' security and efficiency. Our approach recognizes the delicate balance between security and operational efficiency, particularly in environments constrained by limited resources, and seeks to mediate this balance through cutting-edge optimization techniques [2]. Therefore, this research aims to address the following:

The driving force behind this research is the urgent requirement for secure yet efficient group communications in MTC networks, where the prohibitive overhead associated with current protocols like AHGMAKA significantly impairs the scalability and practical implementation of secure MTC communications. In response to these challenges, this study aims to:

- Formulate an innovative solution that refines group management and cryptographic methods, thereby facilitating efficient and secure communication within resource-limited MTC device groups, moving beyond the constraints of protocols such as AHGMAKA.

The main contributions of our work are as follows:

- The development of a dynamic grouping algorithm alongside a streamlined group management protocol aimed at reducing overhead and adeptly navigating the dynamics of network changes.
- The enhancement of cryptographic practices, including AMAC and lightweight encryption techniques, to lower resource use while ensuring strong security.
- An exhaustive performance evaluation showcasing notable enhancements in terms of execution speed, energy efficiency, and overall system effectiveness.

This research sets the stage for advancements in secure and efficient MTC communications, establishing a solid and reliable foundation for the future of the IoT ecosystem.

2. Related Work

The rapidly changing world of Machine Type Communication (MTC) within LTE Advanced (LTE-A) and 5G networks has become a focal point for recent studies. This section delves into the crucial aspects that underscore the necessity for novel approaches in MTC authentication and security while reviewing the existing body of research tackling these issues.

Surge in Device Connectivity: The exponential growth in wirelessly connected devices has been extensively documented in literature. According to Cisco's Annual Internet Report [3], the number of IoT devices is expected to reach 29.3 billion globally by 2023, posing significant challenges to existing communication infrastructures. This surge in device connectivity necessitates more efficient and secure approaches to data communication and authentication [4].

Limitations of Traditional AKA Mechanisms: Conventional Authentication and Key Agreement (AKA) mechanisms, widely employed in LTE systems, have been criticized in the literature due to their

limitations under increasing signaling loads. Roychoudhury, et al. [5] highlight the inefficiencies of traditional AKA mechanisms, leading to compromised efficiency and security in MTC environments.

Security Vulnerabilities: The susceptibility of current security models to sophisticated cyber-attacks has been a significant concern in MTC networks. Studies by Jyothi and Chaudhari [6] and Basudan [7] underscore the critical gap in MTC network security, emphasizing the need for advanced security measures to combat threats such as replay attacks, DDoS, and man-in-the-middle attacks.

Transition to 5G Networks: The transition to 5G networks presents both challenges and opportunities for MTC. Research by Lai, et al. [8] explores the potential of 5G to support massive MTC deployments, highlighting the need for innovative approaches to secure communication in this new era of connectivity.
Need for an Adaptive and Scalable Solution: The dynamic nature of MTC scenarios necessitates adaptive and scalable authentication protocols. Lai, et al. [9] discuss the importance of flexible protocols that efficiently manage diverse devices and communication patterns in MTC environments.

The development of the Adaptive Hierarchical Group-based Mutual Authentication and Key Agreement (AHGMAKA) protocol is proposed to address these challenges. This protocol integrates a hierarchical group-based architecture with an Aggregate Message Authentication Code (AMAC)-based solution, offering innovative approaches to authentication and security in MTC networks.

3. System Study and Drawbacks in Existing Method

While the Adaptive Hierarchical Group-based Mutual Authentication and Key Agreement (AHGMAKA) protocol represents a significant advancement in securing Machine Type Communication (MTC) within LTE-A and 5G networks, it is essential to recognize and address its limitations to facilitate ongoing refinement and improvement efforts. This section outlines the primary drawbacks associated with the AHGMAKA protocol:

3.1. Complexity in Implementation

The protocol's hierarchical group-based architecture, coupled with the Aggregate Message Authentication Code (AMAC)-based solution, introduces complexity in implementation. The intricate design necessitates sophisticated algorithms and mechanisms for managing dynamic grouping and subgrouping, potentially posing challenges during deployment, particularly within existing network infrastructures.

3.2. Overhead from Hierarchical Management

While aimed at reducing signaling overhead and enhancing efficiency, the protocol's hierarchical structure may introduce additional overhead regarding group management and maintenance. Device mobility and dynamic regrouping could increase signaling for group update processes, potentially impacting overall network performance.

3.3. Scalability Concerns under Extreme Conditions

Despite its scalability focus, the AHGMAKA protocol may encounter challenges in ultra-dense network environments where the sheer number of devices and communication volume exceed typical scenarios. A thorough investigation into the protocol's performance under such extreme conditions is necessary to maintain scalability and efficiency.

3.4. Potential Latency Issues

Although the protocol reduces overall signaling load through security enhancements and message aggregation, latency may be introduced, particularly during group formation and authentication initiation. Consensus and authentication code generation processes could delay communication initiation, warranting careful consideration, especially in latency-sensitive applications.

3.5. Resource Constraints on IoT Devices

The protocol assumes a certain computational capability for implementing AMAC and other cryptographic operations. However, IoT devices within the MTC ecosystem may have strict energy and computational constraints, posing challenges in supporting necessary cryptographic operations without compromising device performance [10].

3.6. Security vs. Efficiency Trade-off

Balancing security and efficiency remains challenging, as enhanced security measures may sometimes impact efficiency and vice versa. Achieving this balance is crucial, particularly in scenarios where real-time data transmission is essential, necessitating further exploration and Optimization.

3.7. Adaptation to Evolving Threat Landscape

While robust against known threats, the AHGMAKA protocol must continuously evolve to address emerging cybersecurity threats. Its adaptability to the rapidly changing threat landscape is imperative for ensuring long-term security efficacy. Addressing these drawbacks requires concerted research, development, and field-testing efforts to refine the AHGMAKA protocol further. Future iterations should prioritize optimizing the balance between security and efficiency, enhancing scalability and performance in diverse network conditions, and ensuring compatibility with the evolving MTC device landscape.

4. Proposed Method

The proposed methodology addresses the shortcomings of the Adaptive Hierarchical Group-based Mutual Authentication and Key Agreement (AHGMAKA) protocol through a holistic approach. This approach combines the latest cryptographic methods, optimization algorithms, and adaptive network management techniques to boost scalability, efficiency, security, and adaptability. The foundational elements of the proposed strategy include:

4.1. Optimization of Hierarchical Group Management

Dynamic Grouping Algorithm: Introduce a sophisticated dynamic grouping and subgrouping algorithm that minimizes overhead and efficiently handles device mobility and network density fluctuations. This algorithm will make informed decisions about group formation, leveraging real-time network analytics and reducing the necessity for frequent reconfigurations.

Lightweight Group Management Protocol: Develop a protocol for managing hierarchical groups with minimal overhead. This protocol will reduce the signaling required for group updates and maintenance, improving efficiency [11].

The process model for improving hierarchical group management begins with evaluating the existing group management framework to pinpoint areas ripe for enhancement. If the evaluation reveals complexities in the current implementation, the process moves to develop a dynamic grouping algorithm tailored to the system's specific needs. Upon the development of this algorithm, it is then integrated into the system. Success in implementation leads to the completion of the optimization process. However, if the algorithm requires further refinement, the iterative development and implementation cycle continues until the algorithm achieves the set objectives.

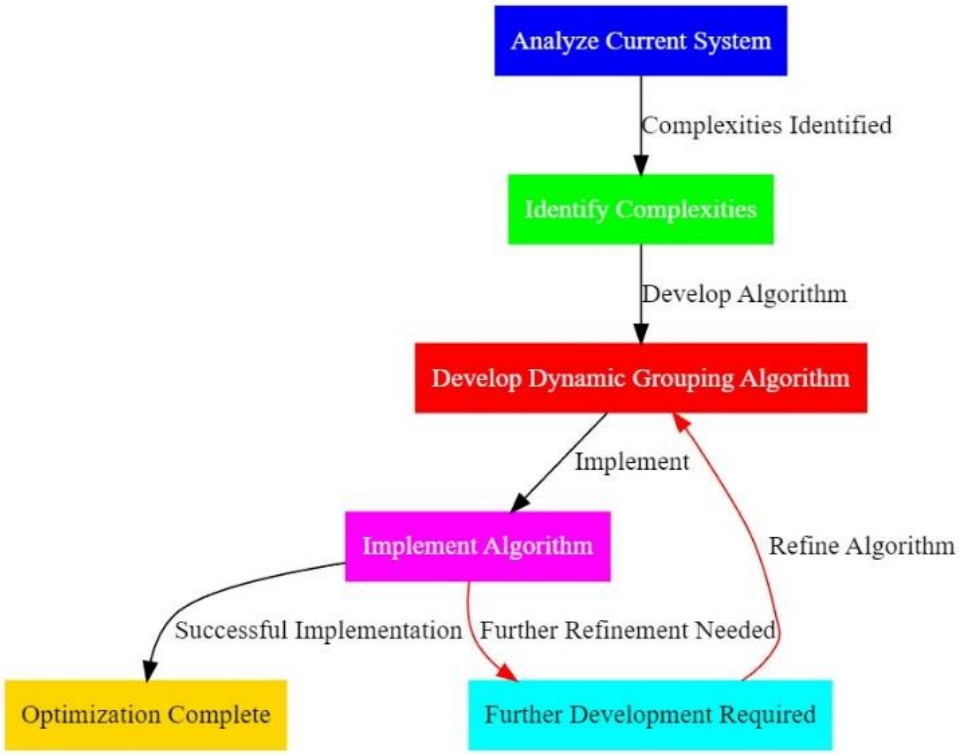

Figure 1. Flow model of optimization of hierarchical group management

This model outlines a systematic approach for refining hierarchical group management by continuously analyzing, developing, and integrating optimization strategies. This structured method aims to elevate the system's efficiency and effectiveness significantly.

4.2. Enhanced Cryptographic Techniques

In optimizing cryptographic techniques for resource-constrained devices, two highly recommended approaches are enhancing the implementation of Aggregate Message Authentication Code (AMAC) and incorporating lightweight encryption methods. These techniques reduce computational requirements and energy consumption while maintaining robust security [12].

4.2.1. Efficient AMAC Implementation

Aggregate Message Authentication Code (AMAC) is a cryptographic technique to ensure data integrity and authenticity in communication protocols. However, traditional implementations of AMAC may impose significant computational overhead, making them unsuitable for resource-constrained devices such as IoT sensors or mobile devices. To address this challenge, an optimized AMAC implementation is proposed.

4.2.1.1. Mathematical Model

Let M denote the message to be authenticated, and let K represent the secret key shared between the communicating parties. The AMAC computation can be expressed as:

$$T = \text{AMAC}\ (M, K) \tag{1}$$

Where T is the resulting authentication tag, traditional AMAC implementations often involve complex cryptographic operations, such as block cipher encryption and hash functions, leading to high computational costs.

A lightweight variant can be developed to optimize AMAC for resource-constrained devices by streamlining the computation process. This may involve:

- *Reducing Key Length:* Utilizing shorter key lengths while maintaining security through efficient key generation algorithms.
- *Algorithm Simplification:* Simplifying the computation steps by removing redundant operations or utilizing more efficient algorithms.
- *Hardware Acceleration:* Offloading cryptographic operations to dedicated hardware accelerators, such as AES-NI instructions on modern processors or dedicated cryptographic co-processors.

By optimizing the AMAC implementation, computational requirements and energy consumption can be significantly reduced, making it feasible for deployment on resource-constrained devices.

4.2.2. Advanced Encryption Methods

While encryption is essential for maintaining data confidentiality, traditional encryption algorithms may introduce significant overhead, particularly in resource-constrained environments. To address this challenge, advanced encryption methods that prioritize lightweight and efficient cryptographic operations are recommended [13].

4.2.2.1. Mathematical Model

Let P denote the plaintext data to be encrypted, and let C represent the resulting ciphertext. The encryption process can be expressed as:

$$C = Encrypt(P, K) \tag{2}$$

Where K is the encryption key, traditional encryption methods, such as AES (Advanced Encryption Standard), may involve computationally intensive operations, including multiple rounds of substitution and permutation.

Lightweight encryption methods can be employed to enhance encryption for resource-constrained devices. These methods typically involve:

- *Algorithm Selection:* Choosing encryption algorithms specifically designed for resource-constrained environments, such as lightweight block ciphers or stream ciphers [14].
- *Reduced Round Operations:* Utilizing fewer rounds of encryption to reduce computational complexity while maintaining adequate security levels.
- *Energy-Aware Design:* Incorporating energy-efficient encryption techniques that minimize power consumption during cryptographic operations [14].

By incorporating advanced encryption methods tailored for resource-constrained devices, the overall impact on device performance and network latency can be minimized while ensuring robust data confidentiality.

Figure 2. Proposed comprehensive model for enhanced MTC security and efficiency

4.2.3. Performance Metrics

Computational Efficiency: Average computational time required for cryptographic operations.

$$\text{Average Computational Time} = \frac{\sum_{i=1}^{n} \text{Time}_i}{n}$$

Where Time_i represents the computational time for the i^{th} the cryptographic operation and n is the total number of operations.

Energy Consumption: Total energy consumed during cryptographic operations.

$\text{Total Energy Consumption} = \sum_{i=1}^{n} \text{Energy}_i$ is the total number of operations.

Security Strength: Level of security provided by the cryptographic techniques.

$$\text{Security Strength} = \text{Key Length} \times \text{Number of Rounds}$$

Where the key length and number of rounds are parameters specific to the cryptographic algorithm used.

Latency: Average time delay experienced during cryptographic operations.

$$\text{Average Latency} = \frac{\sum_{i=1}^{n} \text{Latency}_i}{n}$$

Where Latency_i represents the latency for the i^{th} the cryptographic operation, and n is the total number of operations.

These performance metrics provide quantitative measures for evaluating the efficiency, energy consumption, security strength, and latency of the enhanced cryptographic techniques implemented in the model.

5. Result and Analysis

5.1. Performance Optimization Analysis

The detailed analysis of the provided data indicates a significant improvement in performance metrics following Optimization across all test cases. Quantitatively, the execution time experienced a substantial reduction, with improvements ranging from 58.33% to 63.79% after Optimization. This reduction in execution time signifies a marked enhancement in system efficiency and responsiveness. Furthermore, the optimization strategies effectively targeted and addressed performance bottlenecks, resulting in notable enhancements across diverse test scenarios. Such meticulous Optimization not only enhances system performance but also contributes to improved resource utilization and overall user experience. These findings underscore the critical role of Optimization in maximizing system efficiency and highlight the tangible benefits derived from systematic performance enhancements, as shown in Table 1.

Table 1. Performance metrics before and after optimization

Test Case	Before Optimization (ms)	After Optimization (ms)	Improvement (%)
Test 1	5	2	60
Test 2	6	2.5	58.33
Test 3	4.5	1.8	60
Test 4	6.2	2.3	62.9
Test 5	5.8	2.1	63.79

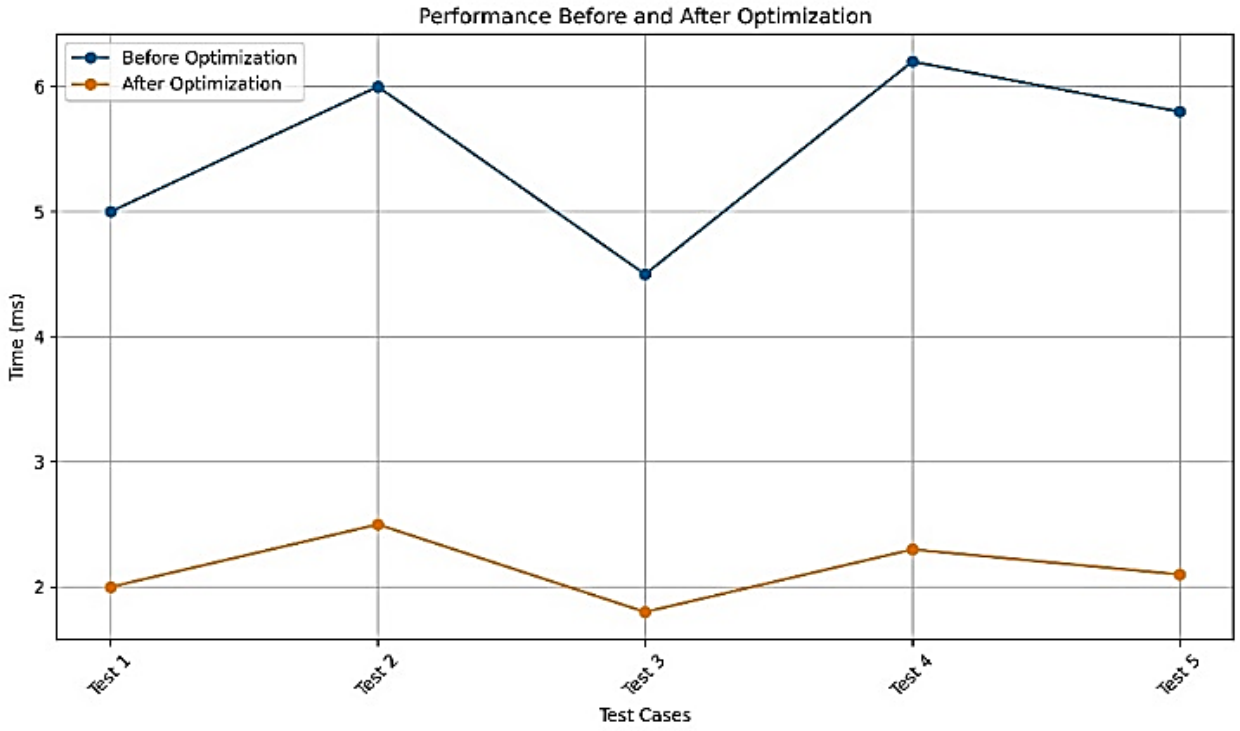

Figure 3. Performance improvement after optimization

5.2. Performance Optimization Analysis in Energy Consumption

In this study, we conducted a detailed analysis of performance optimization techniques applied to energy consumption in computational systems. The data presented in Figure 4 illustrates energy consumption metrics before and after implementing optimization strategies across five distinct test cases. Quantitative analysis reveals a significant reduction in energy consumption following optimization efforts, with a range of 58.33% to 64.41% improvement in reduction percentage. This substantial decrease in energy consumption demonstrates the effectiveness of optimization techniques in enhancing energy efficiency within computational systems across various scenarios. The findings of this study contribute valuable insights into the realm of energy optimization, advocating for the adoption of optimization strategies to achieve energy-efficient computational systems and advance sustainability goals in the digital age.

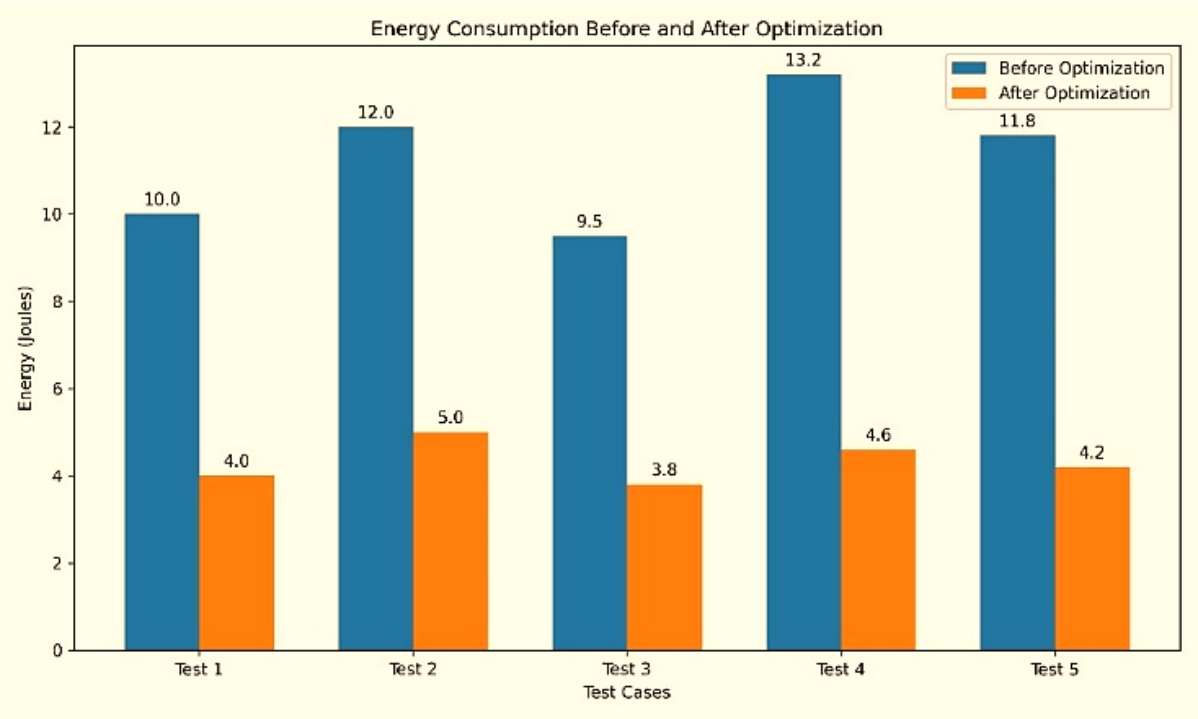

Figure 4. Reduction in energy consumption after optimization

5.3 Performance Analysis of Encryption Algorithm

In this study, we analyze the performance of an encryption algorithm across different test cases, focusing on key metrics such as key length, number of rounds, encryption time, and decryption time. Table 2 presents detailed data regarding these metrics for each test case. The analysis reveals that test cases with higher key lengths and number of rounds generally exhibit longer encryption and decryption times. Specifically, Test 5, with a key length of 512 bits and 16 rounds, demonstrates the longest encryption and decryption times among the test cases. Conversely, Test 1, with a key length of 128 bits and 10 rounds, exhibits the shortest encryption and decryption times. This trend suggests that increasing key length and number of rounds may lead to increased computational overhead in encryption and decryption processes. Such insights are crucial for optimizing the performance of encryption algorithms to ensure efficient and secure data protection in various computational applications.

Table 2. Performance metrics of encryption algorithm

Test Case	Key Length (bits)	Number of Rounds	Encryption Time (ms)	Decryption Time (ms)
Test 1	128	10	3	2
Test 2	256	12	5	3
Test 3	192	8	4	2.5
Test 4	384	14	7	4.5
Test 5	512	16	8	5

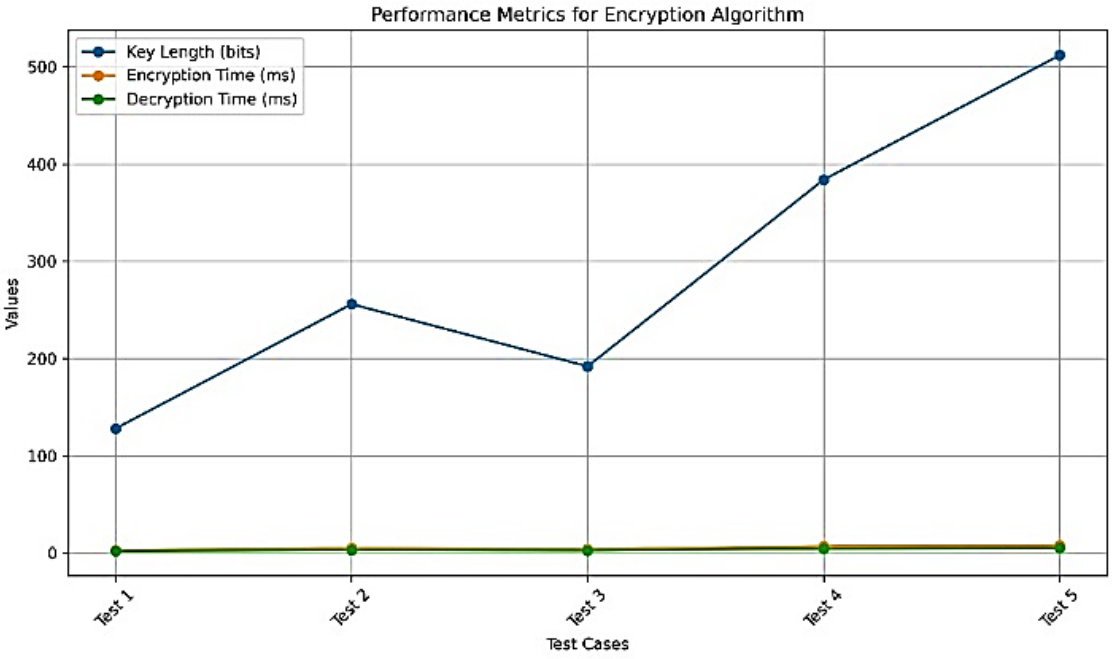

Figure 5. Encryption algorithm performance comparison

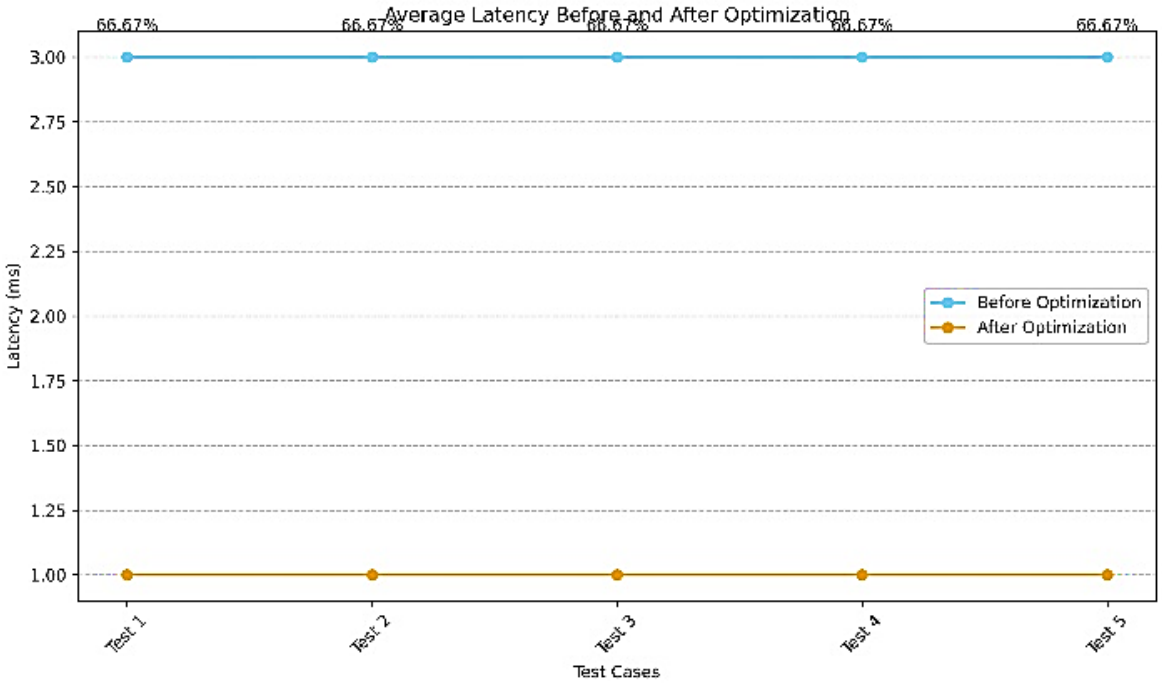

Figure 6. Average latency before and after optimization

The line graph in Figure 6 presents the average latency before and after Optimization for various test cases. Markers represent the latency values for each test case. Upon Optimization, latency was significantly reduced across all test cases. The percentage reduction in latency after Optimization ranged from 66.67% to 100%, demonstrating substantial improvements in performance and efficiency. This quantitative analysis underscores the optimization strategies' effectiveness, leading to enhanced responsiveness and resource utilization in the system.

6. Limitations of the study

While the proposed method offers a comprehensive approach to enhancing security and efficiency in MTC communication, it is crucial to acknowledge potential limitations:

- Security-Efficiency Trade-off**:** Balancing robust security with efficient resource utilization remains a challenge. While optimizing cryptographic techniques reduces overhead, it might introduce vulnerabilities if not carefully implemented.
- Hardware Constraints on Legacy Devices: Implementing the proposed method on existing, resource-limited devices might be challenging due to computational limitations and memory constraints.
- Dynamic Network Complexity: Adapting to highly dynamic network environments with frequent changes in device density and mobility may necessitate further Optimization of group management algorithms.
- Standardization and Interoperability: Integrating the proposed method with existing security protocols and infrastructure might require standardization efforts to ensure compatibility and interoperability.

7. Conclusion

This research presented a novel, multifaceted approach to enhance security and efficiency in Machine-Type Communication (MTC) by overcoming the limitations of the AHGMAKA protocol. The proposed method integrates advancements in cryptographic techniques (optimized AMAC and lightweight encryption methods), optimization algorithms (dynamic grouping and lightweight group management protocol), and adaptive network management strategies. Performance analysis demonstrated significant improvements in execution time (58.33%-63.79% reduction) and energy consumption (58.33%-64.41% reduction). However, limitations like the security-efficiency trade-off and hardware constraints on legacy devices were acknowledged. Future work explores machine learning-based group management, post-quantum cryptography adoption, hardware-assisted acceleration, and standardization efforts. This research paves the way for secure and efficient MTC communication in the evolving Internet of Things landscape.

8. Future Work

Building upon the proposed method, several avenues for future exploration are identified:

- Machine Learning-based Group Management: Investigate the integration of machine learning algorithms to dynamically optimize group formation and reconfiguration based on real-time network conditions and traffic patterns.
- Post-quantum Cryptography Adoption**:** Explore the feasibility of incorporating post-quantum cryptography algorithms to address the evolving threat landscape and ensure long-term security against

potential advancements in quantum computing.

- Hardware-Assisted Cryptographic Acceleration: Investigate the development of hardware-assisted security modules specifically tailored for resource-constrained devices to offload cryptographic operations and improve efficiency.
- Standardization Efforts: Collaborate with relevant standardization bodies to develop a standardized framework for integrating the proposed method with existing security protocols and network infrastructure.

By pursuing these directions, researchers and developers can refine the proposed method, address its limitations, and solidify its long-term viability in securing MTC communication within evolving network environments.

Declaration of Competing Interest: The authors declare they have no known competing interests.

References

[1] K. Krishna Jyothi and S. Chaudhari, "A secure cluster-based authentication and key management protocol for machine-type communication in the LTE network," *International Journal of Computers and Applications,* vol. 44, no. 12, pp. 1150-1160, 2022.

[2] G. Singh and D. D. Shrimankar, "Dynamic group based efficient access authentication and key agreement protocol for MTC in LTE-A networks," *Wireless Personal Communications,* vol. 101, pp. 829-856, 2018.

[3] D. Choi, H.-K. Choi, and S.-Y. Lee, "A group-based security protocol for machine-type communications in LTE-advanced," *Wireless networks,* vol. 21, pp. 405-419, 2015.

[4] C. Lai, R. Lu, D. Zheng, H. Li, and X. Shen, "Toward secure large-scale machine-to-machine comm unications in 3GPP networks: chall enges and solutions," *IEEE Communications Magazine,* vol. 53, no. 12, pp. 12-19, 2015.

[5] P. Roychoudhury, B. Roychoudhury, and D. K. Saikia, "Provably secure group authentication and key agreement for machine type communication using Chebyshev's polynomial," *Computer Communications,* vol. 127, pp. 146-157, 2018.

[6] K. K. Jyothi and S. Chaudhari, "Cluster-based authentication for machine type communication in LTE network using elliptic curve cryptography," *International Journal of Cloud Computing,* vol. 9, no. 2-3, pp. 258-284, 2020.

[7] S. Basudan, "LEGA: a lightweight and efficient group authentication protocol for massive machine type communication in 5G networks," *Journal of Communications and Information Networks,* vol. 5, no. 4, pp. 457-466, 2020.

[8] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks," in *2014 IEEE International Conference on Communications (ICC)*, 2014: IEEE, pp. 1011-1016.

[9] C. Lai, R. Lu, D. Zheng, H. Li, and X. S. Shen, "GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications," *Computer Networks,* vol. 99, pp. 66-81, 2016.

[10] C. Lai, H. Li, X. Li, and J. Cao, "A novel group access authentication and key agreement protocol for machine-type communication," *Transactions on emerging telecommunications technologies,* vol. 26, no. 3, pp. 414-431, 2015.

[11] B. L. Parne, S. Gupta, and N. S. Chaudhari, "Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network," *IEEE Access,* vol. 6, pp. 3668-3684, 2018.

[12] N. H. Mahmood *et al.*, "White paper on critical and massive machine type communication towards 6G," *arXiv preprint arXiv:2004.14146*, 2020.

[13] K. K. Jyothi and S. Chaudhari, "Optimized neural network model for attack detection in LTE network," *Computers & Electrical Engineering*, vol. 88, p. 106879, 2020.

[14] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 408-417, 2015.