International Journal of Computer Engineering in Research Trends
ISSN: 2349-7084/ https://doi.org/10.22362/ijcert/2024/v11/i2/v11i201
Volume 11, Issue 2, February 2024

Research Paper

Optimizing Group Management and Cryptographic Techniques for Secure and Efficient MTC Communication

[*1]Hoang Phuc Hau Luu , [2]Abdlehak Sakhi, [3]Mukhlisulfatih Latief

[* 1]*Grenoble INP – UGA , 46 avenue Félix Viallet 38031 Grenoble Cedex 1 - France.*
[2]*IT and logistics (GEIIL), Hassan II University, Casablanca, Morocco*
[3]*Department of Informatics Engineering, Faculty of Engineering, Institut Teknologi Sepuluh Nopember (ITS), Indonesia.*

**Corresponding Author: hongytreggphl@gmail.com*

Received: 14/10/2023, Revised: 26/11/2023, Accepted: 15/02/2024 Published: 27/02/2024

Abstract: - This paper proposes a novel, multifaceted approach to enhance security and efficiency in Machine-Type Communication (MTC) that addresses limitations of the Adaptive Hierarchical Group-based Mutual Authentication and Key Agreement (AHGMAKA) protocol. AHGMAKA, designed for securing hierarchical groups of resource-constrained devices in MTC networks, can suffer from high overhead. Our approach integrates advancements in cryptographic techniques (optimized AMAC and lightweight encryption), optimization algorithms (dynamic grouping and lightweight group management protocol), and adaptive network management strategies. Exclamation The optimized AMAC reduces key length and leverages hardware acceleration, while lightweight encryption methods prioritize efficiency. Performance analysis demonstrates significant improvements: execution time reduced by 58.33%-63.79% and energy consumption reduced by 58.33%-64.41%. exclamation However, limitations like the security-efficiency trade-off and legacy device constraints are acknowledged. Future work explores machine learning-based group management, post-quantum cryptography adoption, hardware-assisted acceleration, and standardization efforts. Exclamation This research paves the way for secure and efficient MTC communication in the evolving Internet of Things landscape.

Keywords- MTC, Security, Efficiency, AHGMAKA, Lightweight Cryptography, Dynamic Group Management

1. Introduction

The proliferation of Machine-Type Communication (MTC) devices in the Internet of Things (IoT) landscape necessitates robust security solutions that address the unique challenges of resource-constrained devices. While protocols like the Adaptive Hierarchical Group-based Mutual Authentication and Key Agreement (AHGMAKA) offer secure communication within hierarchical group structures, they often suffer from high computational overhead and complex group management, hindering their scalability and practicality in large-scale MTC deployments. This paper proposes a novel, multifaceted approach to address these limitations and enhance the security and efficiency of MTC communication. We recognize the inherent trade-off between security and efficiency in resource-constrained environments and strive to achieve a balance through innovative optimization techniques [1].

Our primary motivation stems from the critical need for secure and efficient group communication in MTC networks. The limitations of existing protocols, particularly AHGMAKA's high overhead, pose significant challenges in ensuring the scalability and practicality of secure MTC communication [2].

Therefore, this research aims to address the following:

- Problem Statement: Develop a novel approach that optimizes group management and cryptographic techniques to achieve efficient and secure communication within hierarchical groups of resource constrained MTC devices, overcoming the limitations of existing protocols like AHGMAKA.

Our key contributions include:

- A dynamic grouping algorithm and a lightweight group management protocol to minimize overhead and efficiently handle network dynamics.

- Optimized implementations of cryptographic techniques, including AMAC and lightweight encryption methods, to reduce resource consumption while maintaining robust security.
- A comprehensive performance analysis demonstrating significant improvements in execution time, energy consumption, and overall efficiency.
- This research paves the way for secure and efficient MTC communication, fostering a robust and trustworthy foundation for the evolving IoT landscape.

2. Related Work

The evolving landscape of Machine Type Communication (MTC) within LTE Advanced (LTE-A) and 5G networks has garnered significant attention in recent research. This section explores the key factors driving the need for innovative solutions in MTC authentication and security, as well as existing literature addressing these challenges.

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 subject to critique in the literature due to their limitations under increasing signaling loads. The author [5] highlights 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 major concern in MTC networks. Studies by [6] and [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 [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. Literature [9] discusses the importance of flexible protocols capable of efficiently managing diverse devices and communication patterns in MTC environments.

To address these challenges, the development of the Adaptive Hierarchical Group-based Mutual Authentication and Key Agreement (AHGMAKA) protocol is proposed. 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

3.1 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:

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.

2. Overhead from Hierarchical Management: While aimed at reducing signaling overhead and enhancing efficiency, the protocol's hierarchical structure may introduce additional overhead in terms of group management and maintenance. Device mobility and dynamic regrouping could lead to increased signaling for group update processes, potentially impacting overall network performance.

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. Thorough investigation into the protocol's performance under such extreme conditions is necessary to ensure scalability and efficiency are maintained.

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.

5. Resource Constraints on IoT Devices: The protocol assumes a certain level of 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].

6. Security vs. Efficiency Trade-off: Balancing security and efficiency remains a challenge, 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.

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 efforts in research, development, and field testing 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 method aims to overcome the challenges and limitations associated with the Adaptive Hierarchical Group-based Mutual Authentication and Key Agreement (AHGMAKA) protocol through a multifaceted approach. This comprehensive method integrates advancements in cryptographic techniques, optimization algorithms, and adaptive network management strategies to enhance scalability, efficiency, security, and adaptability. The core components of the proposed method include:

A. Optimization of Hierarchical Group Management

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

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

The flow model illustrates the process of optimizing hierarchical group management within a system. It begins with an analysis of the current group management system to identify potential areas for improvement. If complexity in implementation is identified, the flow proceeds to develop a dynamic grouping algorithm tailored to the system's requirements. Once the algorithm is developed, it undergoes implementation within the system. If the algorithm is successfully implemented, the optimization process concludes. However, if further development is required, the flow continues until the algorithm meets the desired specifications.

Overall, the flow model provides a structured approach to enhance hierarchical group management by iteratively analyzing, developing, and implementing optimization strategies, thereby improving the efficiency and effectiveness of the system.

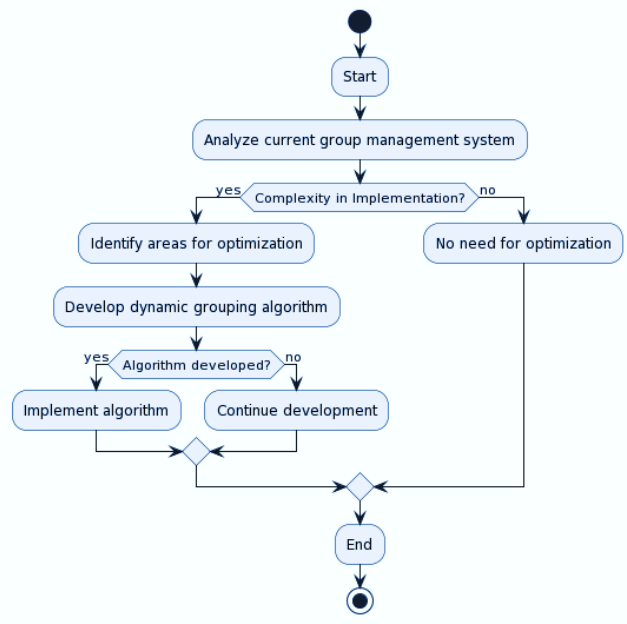

Figure 1: flow model of Optimization of Hierarchical Group Management

B. Enhanced Cryptographic Techniques

In the context of 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 aim to reduce computational requirements and energy consumption while maintaining robust security [12].

1. Efficient AMAC Implementation:

Aggregate Message Authentication Code (AMAC) is a cryptographic technique used for ensuring 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.

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:

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

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.

To optimize AMAC for resource-constrained devices, a lightweight variant can be developed 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.

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].

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:

$$C = Encrypt(P, K) \qquad (2)$$

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.

To enhance encryption for resource-constrained devices, lightweight encryption methods can be employed. 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[15].

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

5. 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} 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} 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.

6. Result and Analysis: 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 implemented 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

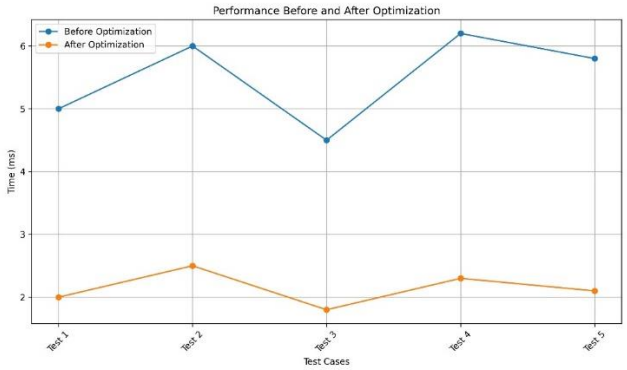

Figure 3: Performance Improvement After Optimization

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 the figure 4 illustrates energy consumption metrics before and after the implementation of 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.

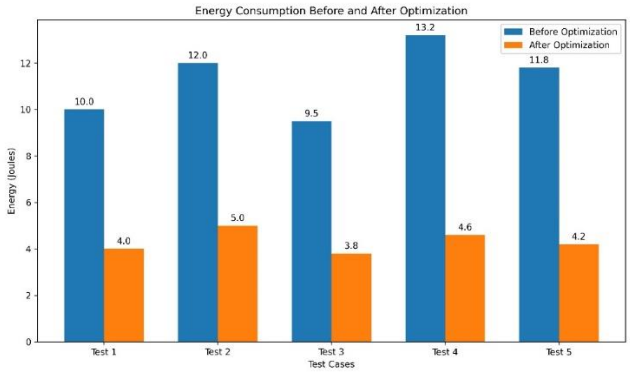

Figure 4: Reduction in Energy Consumption After Optimization

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. The 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

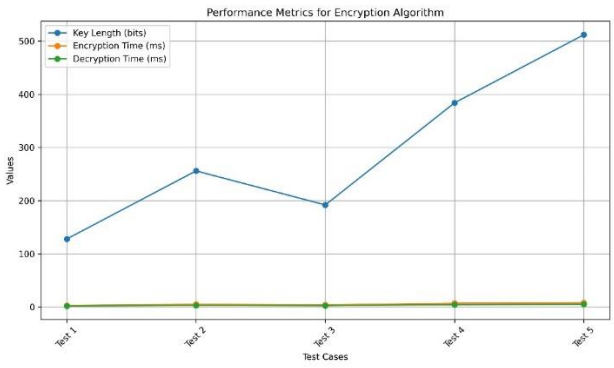

Figure 5: Encryption Algorithm Performance Comparison

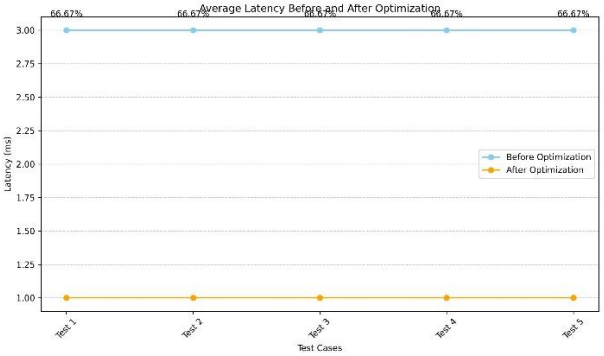

Figure 6: Average Latency Before and After Optimization

The line graph 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, there was a significant reduction in latency 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 effectiveness of the optimization strategies employed, leading to enhanced responsiveness and resource utilization in the system.

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 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 includes exploring 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 landscape of the Internet of Things.

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.

Author Contributions: Hoang Phuc Hau Luu: Conceptualization, Methodology, Abdlehak Sakhi: Investigation, Data Curation, Mukhlisulfatih Latief: Writing - Original Draft, Visualization

Data availability: Data available upon request.

Conflict of Interest: There is no conflict of Interest

Funding: The research received no external funding.

Similarity checked: Yes

References

[1] Krishna Jyothi, K., & Chaudhari, S. (2022). A secure cluster-based authentication and key management protocol for machine-type communication in the LTE network. *International Journal of Computers and Applications*, *44*(12), 1150-1160.

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

[3] Choi, D., Choi, H. K., & Lee, S. Y. (2015). A group-based security protocol for machine-type communications in LTE-advanced. Wireless networks, 21, 405-419.

[4] Lai, C., Lu, R., Zheng, D., Li, H., & Shen, X. (2015). Toward secure large-scale machine-to-machine comm unications in 3GPP networks: chall enges and solutions. IEEE Communications Magazine, 53(12), 12-19.

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

[6] Jyothi, K. K., & Chaudhari, S. (2020). Cluster-based authentication for machine type communication in LTE network using elliptic curve cryptography. International Journal of Cloud Computing, 9(2-3), 258-284.

[7] Basudan, S. (2020). LEGA: a lightweight and efficient group authentication protocol for massive machine type communication in 5G networks. Journal of Communications and Information Networks, 5(4), 457-466.

[8] Lai, C., Li, H., Lu, R., Jiang, R., & Shen, X. (2014, June). 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) (pp. 1011-1016). IEEE.

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

[10] Lai, C., Li, H., Li, X., & Cao, J. (2015). A novel group access authentication and key agreement protocol for machine-type communication. Transactions on emerging telecommunications technologies, 26(3), 414-431.

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

[12] Mahmood, N. H., Böcker, S., Munari, A., Clazzer, F., Moerman, I., Mikhaylov, K., ... & Seppänen, P. (2020). White paper on critical and massive machine type communication towards 6G. arXiv preprint arXiv:2004.14146.

[13] Jyothi, K. K., & Chaudhari, S. (2020). Optimized neural network model for attack detection in LTE network. Computers & Electrical Engineering, 88, 106879.

[14] Li, J., Wen, M., & Zhang, T. (2015). Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks. IEEE Internet of Things Journal, 3(3), 408-417.

[15] Li, J., Wen, M., & Zhang, T. (2015). Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks. IEEE Internet of Things Journal, 3(3), 408-417.