Evaluating Security Techniques in 5G MIMO-Based IoT Networks

Chrysostomos-Athanasios Katsigiannis
Computer Engineering and Informatics Department
University of Patras
Patras, Greece
Email: up1072490@upnet.gr

Konstantinos Tsachrelias
Computer Engineering and Informatics Department
University of Patras
Patras, Greece
Email: up1096511@upatras.gr

Vasileios Kokkinos
Computer Engineering and Informatics Department
University of Patras
Patras, Greece
Email: kokkinos@cti.gr

Apostolos Gkamas
Department of Chemistry
University of Ioannina
Ioannina, Greece
Email: gkamas@uoi.gr

Christos Bouras
Computer Engineering and Informatics Department
University of Patras
Patras, Greece
Email: bouras@upatras.gr

Philippos Pouyioutas
Computer Science Department
University of Nicosia
Nicosia, Cyprus
Email: pouyioutas.p@unic.ac.cy

2025 Sixteenth International Conference on Ubiquitous and Future Networks (ICUFN) | 979-8-3315-2487-6/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICUFN65838.2025.11170089

***Abstract*— The rapid expansion of Internet of Things (IoT) devices in various sectors, from healthcare to industrial automation, has heightened the need for secure and efficient communication networks. Multiple Input Multiple Output (MIMO) systems, integral to 5G networks, offer high throughput and low latency essential for real-time IoT applications. However, the integration of robust security mechanisms into MIMO systems often leads to increased latency, potentially undermining the performance of time-sensitive IoT applications. This paper proposes a framework for enhancing the security of MIMO networks specifically designed for IoT environments while maintaining ultra-low latency. The study explores lightweight encryption techniques, physical layer security methods, and optimized beamforming strategies that collectively safeguard data integrity and confidentiality without compromising network performance. Through theoretical analysis and extensive simulations, this research demonstrates that it is possible to achieve a secure MIMO-based IoT network that balances both latency and security requirements.**

Keywords*— *Beamforming, 5G Networks, Multiple Input Multiple Output (MIMO), Security, Internet of Things (IoT)

I. Introduction

The rapid proliferation of the Internet of Things (IoT) has led to a new era of connectivity, integrating billions of devices that communicate seamlessly across sectors such as healthcare, manufacturing, and smart cities. These devices rely on real-time data transmission, placing unprecedented demands on network performance. As a response, the deployment of 5G networks with Multiple Input Multiple Output (MIMO) technology has become a critical enabler. MIMO significantly enhances data throughput and reduces latency, making it particularly suitable for the strict requirements of IoT applications that demand high-speed and low-latency communication.

However, the growing number of interconnected devices introduces complex security challenges. IoT networks often handle highly sensitive data ranging from personal health records to critical infrastructure controls making them a prime target for malicious attacks. Ensuring robust security in such networks is vital to protect against threats like eavesdropping, data breaches, and jamming. Traditional security mechanisms, though effective, tend to introduce additional latency, which could hinder the performance of time-sensitive applications [1]. This necessitates the development of novel security frameworks that can achieve a balance between data protection and network efficiency. This study addresses this issue by proposing a security framework tailored for MIMO-based IoT networks in 5G environments, with a focus on maintaining the low-latency requirements crucial for real-time applications.

Several studies have explored the integration of 5G and IoT to address the demands of modern applications. For instance, paper [2] investigates the security of a 5G-IoT ecosystem, emphasizing the diverse applications such as smart homes, healthcare, and transportation, which are vulnerable due to the large number of interconnected devices. The study highlights the potential consequences of security breaches, particularly in critical sectors like healthcare, where breaches could endanger human life. To address these challenges, the authors propose a hybrid security algorithm incorporating a deep Q-learning-based Intrusion Detection System (IDS) and lightweight computation, which is suitable for resource-constrained IoT devices. The algorithm also integrates network slicing technology and Security-Aware Workflows (SAWS) to ensure business continuity by isolating attacks and reallocating IoT tasks. This approach aims to enhance availability and mitigate the impact of potential security incidents, aligning with key principles of Confidentiality, Integrity, and Availability (CIA).

Paper [3] addresses the security challenges in 5G-based IoT networks using Virtual Multiple-Input Multiple-Output (V-MIMO) techniques. The authors present a secure and energy-efficient V-MIMO enabled Simultaneous Wireless Information and Power Transfer (SWIPT) framework, which leverages beamforming and cooperative jamming signals to maximize the secrecy rate of IoT systems. The framework formulates an optimization problem that jointly optimizes beamforming vectors, power splitting, and time switching ratios. To solve this nonconvex problem, the study introduces an iterative algorithm employing the penalty function method. Simulation results demonstrate that the proposed solution outperforms existing methods in terms of secrecy rate and energy efficiency, making it a promising approach for securing 5G-centric IoT networks.

Furthermore, the research work in paper [4] explores the transformative impact of 5G technology on IoT, highlighting how features like network slicing, edge computing, and MIMO enhance the performance and scalability of IoT systems across various sectors, including smart cities, healthcare, and autonomous vehicles. The paper also discusses the potential challenges of this integration, such as security concerns, spectrum management, and the need for new regulatory frameworks. The authors argue that further research is needed to optimize 5G for IoT applications, enhance security, and explore novel use cases to build smarter and more connected ecosystems that drive global advancements.

The proposed framework distinguishes itself by integrating lightweight encryption techniques and physical layer security measures that are optimized for resource-constrained IoT devices. Unlike previous research, which often concentrates on theoretical approaches or lacks performance validation, this paper presents a comprehensive solution that can be practically implemented without compromising network performance. Through a combination of theoretical analysis and simulation results, this study explores how these security measures can be seamlessly integrated into MIMO systems to provide robust protection while preserving the efficiency of IoT communications [5], [6], [7], [8], [9].

The rest of the paper is organized as follows: In Section II, the mathematical model utilized in the simulation environment is introduced. Moving to Section III, the algorithm analysis that forms the basis for constructing the experiment scenarios is delved into. Section IV outlines the simulation setup and methodology employed to assess the performance of MIMO 5G Heterogeneous Networks. Following that, in Section V, the simulation results are presented, and a comprehensive analysis of the findings is conducted. Finally, Section VI concludes the paper and offers insights into potential avenues for future research.

II. Mathematical Model

This section presents the mathematical models used to evaluate the latency, throughput, and security performance in MIMO-based IoT networks. The models incorporate the effects of various encryption techniques on network efficiency, taking into account key parameters such as energy consumption, Signal-to-Noise Ratio (SNR), and Bit Error Rate (BER).

The total latency experienced by an IoT device can be described as a sum of the inherent transmission delay and the additional latency introduced by the encryption process. L_{total} represents the total latency, L_{trans} denotes the baseline transmission latency for a device, and L_{enc} indicates the encryption-induced latency. The total latency L_{total} for each device i and encryption method j is given by:

$$L_{total,i,j}=L_{trans,i}+L_{enc,j} \quad (1)$$

The encryption latency, L_{enc}, varies depending on the computational complexity and security strength of the chosen method. For example, Advanced Encryption Standard (AES) introduces a higher latency due to its computational overhead compared to lightweight methods such as Speck or Simon. These latency values are derived from empirical measurements and represent the delay each encryption algorithm adds to the overall data transmission time.

Throughput (T) is a critical metric in communication systems, defined as the rate at which data is successfully transmitted over a communication channel. For an IoT device, the throughput is influenced by several factors, including the application of encryption mechanisms. Encryption methods can cause a reduction in throughput due to the additional processing overhead required to secure the data. Let Tbaseline represent the baseline throughput of a device, which is the throughput without any encryption. When an encryption method j is applied, the throughput T_{enc} after encryption can be modeled as:

$$T_{enc,i,j}=T_{baseline,i}\left(1-\Delta T_{i,j}/100\right) \quad (2)$$

In this equation, $T_{baseline,i}$ is the baseline throughput of device i in the absence of encryption. $\Delta T_{i,j}$ represents the percentage reduction in throughput for device i when encryption method j is applied. This reduction is determined by the computational overhead introduced by the encryption algorithm and its impact on the data flow. More complex encryption methods generally introduce higher throughput reductions due to greater computational demands. Finally, T enc,$_{i,j}$ is the resulting throughput for device i after applying encryption method j. For the physical layer security analysis, the impact of encryption on the BER is also evaluated. The BER, which represents the rate of bit errors in a transmission, is a function of the SNR. The SNR represents the ratio of the received signal power to the noise power in the system. It is crucial for assessing the quality of the communication link. The SNR is influenced by various factors, including the path loss, which reduces the received signal power over distance. The effect of path loss is directly on the received power. Specifically, as the distance between the transmitter and receiver increases, the path loss increases, which leads to a decrease in the received signal power. This reduction in received power is one of the primary factors affecting SNR. The SNR is then calculated as the ratio of the received signal power (after accounting for path loss) to the noise power, typically represented as::

$$SNR=P_{noise}/P_{recv} \quad (3)$$

The received power P_{recv} is dependent on the transmission power P_{trans}, and the Path Loss $PL(d)$ at a distance d, defined as:

$$P_{recv}=P_{trans}-PL(d) \quad (4)$$

Also, in order for the equation to be valid, the logarithmic values of the parameters in equation (4) are being used, with the units being in dB. For MIMO-based systems, where multiple antennas are used to enhance data transmission and reduce interference, the SNR can be improved through techniques such as beamforming. The *BER* is then derived from the SNR using the complementary error function Q-function, which provides the probability of bit errors in a given modulation scheme. For a modulation scheme like 16-QAM, the *BER* can be expressed as:

$$\mathrm{BER}=\mathrm{Q}\left(\sqrt{2\,\mathrm{SNR}}\right) \tag{5}$$

where the *Q*-function represents the tail probability of the Gaussian distribution. The *BER* is further analyzed under different scenarios, including the presence of jamming attacks or artificial noise injection, to assess the robustness of the encryption techniques. The energy consumption model considers the power required for encryption operations in resource-constrained IoT devices. The total energy consumed, E_{total}, for a device transmitting data with encryption is a sum of the baseline transmission energy E_{trans} and the energy required for encryption E_{enc}:

$$\mathrm{E}_{\mathrm{total}} = \mathrm{E}_{\mathrm{trans}} + \mathrm{E}_{\mathrm{enc}} \tag{6}$$

The encryption energy E_{enc} varies significantly between methods, with heavier algorithms such as AES [10] consuming more energy compared to lightweight counterparts such as Speck [11] or Simon [11]. This difference is critical in determining the overall energy efficiency of the network, especially for battery-operated IoT devices. In addition, Throughput is modeled based on the Shannon capacity formula [12]:

$$\mathrm{C=Blog2(1+SNR)} \tag{7}$$

By employing these mathematical models, the study provides a comprehensive framework to analyze the impact of encryption on key performance metrics such as latency, throughput, *BER*, and energy consumption. The results from these models form the basis for evaluating the effectiveness of various security mechanisms in maintaining a balanced trade-off between data protection and network performance [13], [14].

III. Algorithm Analysis

This section outlines the theoretical algorithm derived from the simulation code provided, describing the key steps in evaluating the performance of different encryption methods in a MIMO-based 5G IoT network. Algorithm 1 incorporates parameters such as energy consumption, latency, throughput reduction, and security strength, and analyzes the performance impact of various encryption techniques on different IoT device types.

Algorithm 1 Security and Performance Optimization Algorithm for MIMO IoT Networks

```
Step 1: Initialization of Encryption Parameters:
Define the encryption methods to be evaluated (AES, ECC, Speck, Simon) along with their respective parameters, including energy consumption, latency, throughput reduction, and security strength.
Step 2: Network Configuration:
Configure the MIMO-based IoT network with parameters like the number of MIMO antennas, carrier frequency, bandwidth, transmission power, noise power, and modulation and coding schemes.
Initialize the positions and types of IoT devices in the network, such as smartphones, smart TVs, and microsensors.
Step 3: Performance Evaluation:
For each encryption method, calculate the additional latency, according to (1), and throughput reduction, according to (2), for each IoT device type. Adjust the latency and throughput based on the encryption overhead.
Compute the path loss for each device type using a standard path loss model and determine the received power and SNR at each device according to (3).
Step 4: Security Assessment:
Calculate the BER, according to (5), for each device based on the computed SNR values. Analyze the impact of different security scenarios (e.g., baseline, artificial noise, beamforming) on the BER.
Visualize the BER vs. SNR for different encryption techniques, illustrating the trade-off between security and communication performance.
Step 5: Energy Efficiency Analysis:
Determine the energy consumption, according to (6), for each encryption method based on the throughput and energy requirements of the IoT devices.
Evaluate the energy efficiency of the security protocols, defined as the ratio of throughput to energy consumption, to identify the most efficient encryption schemes.
Step 6: Simulation of Security Mechanisms:
Implement different security mechanisms, such as artificial noise and beamforming, to enhance physical layer security.
Measure the impact of these mechanisms on network performance metrics like latency, throughput, and BER.
Step 7: Authentication and Access Control:
Analyze the effect of increasing the number of IoT devices on latency and throughput for each encryption method.
Calculate the latency and throughput, according to (1) and (2) respectively, for varying numbers of IoT devices using a lightweight authentication protocol.
Step 8: Traffic Management and Prioritization:
Evaluate different traffic management algorithms (e.g., Round-Robin, Priority Scheduling, Weighted Fair Queueing) to analyze their impact on network latency under different traffic loads.
Visualize and compare the performance of these algorithms based on latency metrics.
Step 9: Impact of Jamming Attacks:
Simulate the effect of jamming attacks on network throughput and latency and assess the robustness of the encryption methods under jamming conditions.
Measure the impact of different jamming power levels on communication performance.
Step 10:Result Visualization:
Generate comprehensive plots for latency, throughput, energy efficiency, BER, and the effect of security mechanisms to visualize and compare the results of the experiments.
```

The proposed algorithm provides a structured and detailed framework for evaluating encryption techniques within MIMO-based 5G IoT networks. By incorporating essential parameters such as energy consumption, latency, throughput reduction, and security strength, the algorithm enables a comprehensive analysis of how different encryption methods impact both security and network performance. Its versatility makes it applicable to a wide range of real-world IoT environments, such as smart cities, healthcare, and industrial automation, where different types of devices with varying constraints are involved.

A key strength of the algorithm lies in its ability to adapt to diverse IoT devices and encryption schemes. This flexibility allows for tailored security strategies depending on specific application requirements, whether the focus is on high data throughput or low-latency communication. Furthermore, the inclusion of advanced security mechanisms, such as artificial noise injection and beamforming, bolsters the security at the physical layer. These features help mitigate risks like eavesdropping and interference, making the system more resilient in the face of common threats in MIMO-based networks. The algorithm also tackles practical challenges like balancing energy consumption with network performance. By simulating different traffic loads and interference conditions, including jamming attacks, the algorithm provides valuable insights into how encryption impacts throughput and energy usage. This is especially relevant for resource-constrained IoT devices that need to maintain high performance without consuming excessive energy. In this way, the algorithm offers an effective means of optimizing security for low-power devices, while ensuring the network maintains robust performance. Additionally, the algorithm supports traffic management and prioritization mechanisms, allowing it to handle dynamic network conditions. By simulating different scheduling algorithms, it ensures that high-priority data can be transmitted with minimal latency even when encryption is applied, which is crucial for time-sensitive IoT applications. Overall, the algorithm provides a practical and flexible solution for optimizing security in IoT networks while balancing the trade-offs between encryption strength, energy efficiency, and network performance.

IV. Simulation Environment

In this simulation, a 5G-enabled MIMO-based IoT network environment that encompasses a variety of IoT devices such as smartphones, smart TVs, and microsensors is created. These devices are distributed randomly across a predefined network area to reflect a real-world scenario where such IoT devices operate in diverse environments like smart homes, cities, or industrial settings. The network operates at a carrier frequency of 3.5 GHz, which is typical of sub-6 GHz 5G networks, with a bandwidth of 20 MHz to ensure sufficient data throughput. The macro Base Station (BS), positioned centrally, uses four MIMO antennas to enhance data transmission and improve overall network efficiency, as you can see in Fig.1.

The devices used in the network differ not only in type but also in their specific performance parameters. Smartphones, for instance, are modeled with a transmission power of 15 dBm and a baseline throughput of 500 Mbps. Smart TVs and microsensors are also included, with each device category assigned realistic latency, energy consumption, and throughput values. For example, smart TVs operate at 10 dBm transmission power with a 400 Mbps throughput, while microsensors, due to their smaller size and power constraints, operate at 5 dBm transmission power and achieve a throughput of 50 Mbps. A summary of the simulation parameters is provided in Table I.

In addition to the variety of IoT devices, the simulation includes jammers positioned within the network to assess the impact of interference on the performance of these devices. The network is tested under various encryption schemes, including AES, ECC [15], Speck, and Simon, each with distinct energy consumption, latency, and throughput reduction characteristics. AES, for instance, is a strong but energy-intensive encryption method, while Simon is a lightweight option that provides lower security but higher energy efficiency. This setup allows for a thorough analysis of the trade-offs between security and network performance.

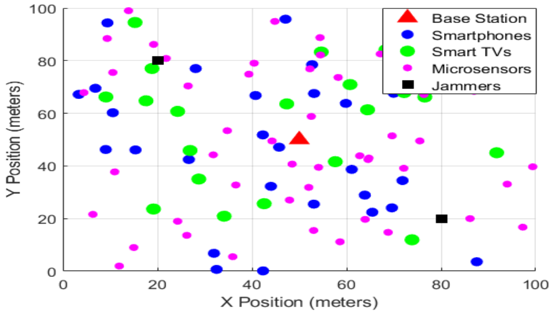

Fig. 1. Network Topology

TABLE I. Simulation Parameters

Parameter	Value
Carrier Frequency	3.5 GHz
Bandwidth	20 MHz
Number of MIMO Antennas	4
Transmission Power	30 dBm
Noise Power/jamming Power	-90 dBm/-80 dBm
Encryption Methods	AES, ECC,Spek, Simon
Number of Smartphones/ Smart TVs/Microsensors	30/20/50

To further assess the network's robustness, physical layer security mechanisms such as artificial noise and beamforming are incorporated to simulate real-world vulnerabilities and mitigation strategies. These mechanisms help secure the communication channels by improving the SNR and reducing the BER, making the network more resistant to eavesdropping and jamming attacks.

V. Performance Evaluation

The simulation results of the experiments performed are detailed as follows, providing insights into the impact of encryption methods on IoT networks. Each figure is analyzed based on the data presented in the plots, offering numerical examples to support the findings.

The experiment in Fig. 2 illustrates the latency comparison of encryption methods for different IoT devices. The results show that AES has the highest latency across all device types, with smartphones experiencing a latency of approximately 45ms, smart TVs at 40ms, and microsensors at 25ms. ECC shows a slight reduction in latency, with smartphones at 43ms, smart TVs at 37.5ms, and microsensors at 23ms. Speck, being a lightweight encryption algorithm, significantly reduces latency, with values as low as 38ms for smartphones, 33ms for smart TVs, and 18ms for microsensors. Similarly, Simon achieves the lowest latency among the tested methods, with smartphones at 35ms, smart TVs at 31ms, and microsensors at 15ms. This experiment highlights the analogy between security and performance, as higher latency is associated with stronger encryption methods such as AES, which provides more robust security compared to Speck and Simon.

Fig. 3 examines the performance of an authentication protocol in terms of latency and throughput when different encryption methods are applied. The results show distinct differences among the encryption methods, particularly between AES and Simon. Latency, which measures the time taken for data to be transmitted or processed, as expected, increases for all encryption methods as the number of IoT devices rises. However, AES and ECC show significantly higher latency compared to Speck and Simon. For instance, with 100 IoT devices, AES reaches a latency of about 60ms, while Simon exhibits a much lower latency of 51ms. Speck and ECC lie in between these values, with Speck at 53ms and ECC at 57ms, highlighting the efficiency of lighter encryption methods like Simon in handling larger networks.

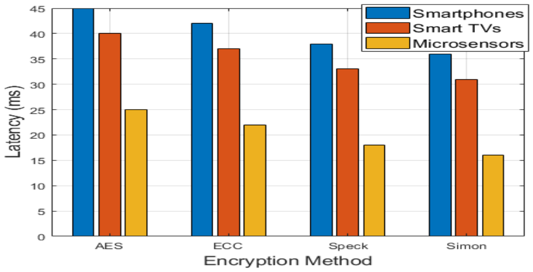

Fig. 2. Latency Comparison of Encryption Methods across IoT Devices.

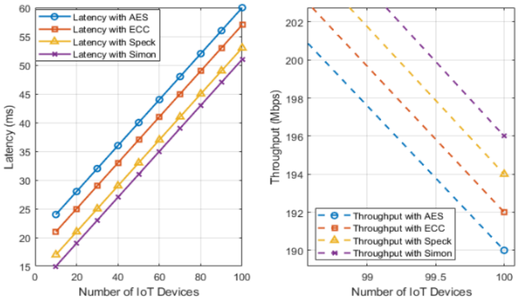

Fig. 3. Latency and Throughput for Authentication Protocol using Different Encryption Methods.

The Throughput decreases as more IoT devices are added to the network. AES and ECC exhibit a sharp decline in throughput compared to Speck and Simon. For example, with 100 devices, AES reduces throughput to around 190 Mbps, while Simon maintains a higher throughput close to 196 Mbps. ECC and Speck fall between these extremes, with ECC at 192 Mbps and Speck at 194 Mbps. These results suggest that while AES and ECC offer stronger security, they do so at the cost of increased latency and reduced throughput. In contrast, Simon and Speck provide faster processing and higher data rates, making them more suitable for dense IoT environments where efficiency is prioritized.

The third experiment in Fig. 4 compares the latency of different traffic management algorithms, specifically Round-Robin Scheduling, Priority Scheduling, and Weighted Fair Queueing. Round-Robin Scheduling shows a stable latency distribution, with a mean latency of approximately 30ms. Priority Scheduling demonstrates a wider range of latency values, with a mean around 30ms and noticeable outliers caused by delayed traffic for low-priority tasks. Weighted Fair Queueing (WFQ) balances the latency distribution between different traffic classes, achieving a mean latency of 28ms. These results suggest that Weighted Fair Queueing offers a better compromise for managing traffic while maintaining acceptable latency for most devices.

The fourth experiment in Fig. 5 evaluates the impact of jamming attacks on the IoT network's throughput and latency. In this context, the jamming power is measured in dBm, where negative values such as -100 dBm and -60 dBm indicate very low power levels. This change in power influences the network's performance by increasing interference.

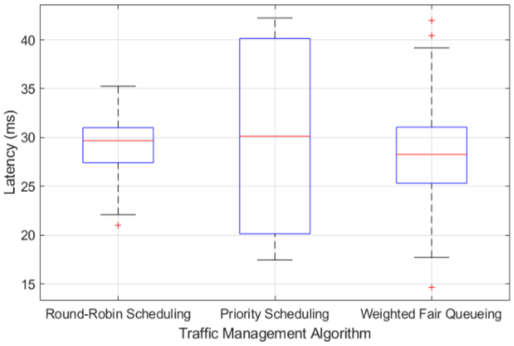

Fig. 4. Latency Comparison of Traffic Management Algorithms in IoT Devices.

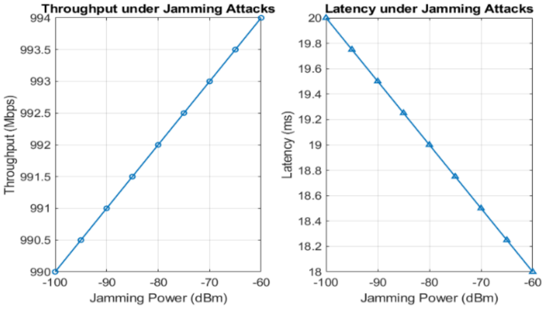

Fig. 5. Impact of Jamming Attacks on Throughput and Latency.

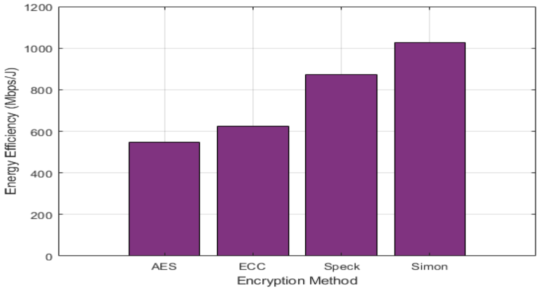

Fig. 6. Energy Efficiency of Security Protocols for IoT Devices

As the jamming power increases, the throughput slightly decreases from 994 Mbps to 990 Mbps, while latency increases from 18ms to 20ms. Despite this increase in jamming power, the impact on throughput and latency remains moderate. This indicates the IoT network's ability to maintain a high level of performance, even in the presence of a stronger jamming signal. The network's resilience under these conditions suggests that its design, featuring robust security mechanisms and interference mitigation strategies, effectively counteracts the negative effects of jamming. This demonstrates the effectiveness of the network's overall architecture in maintaining stability during potential jamming attacks.

The fifth and final experiment Fig. 6 examines energy efficiency across different encryption methods. Simon, the most lightweight encryption algorithm, achieves the highest energy efficiency, with a value exceeding 1000 Mbps/J. AES, being the most resource-intensive algorithm, results in an energy efficiency of approximately 546 Mbps/J. ECC and Speck fall in between these two extremes, with Speck offering higher energy efficiency than ECC. These results emphasize the importance of choosing encryption methods that not only provide adequate security but also optimize energy consumption, particularly for battery-constrained IoT devices.

In conclusion, the simulation results demonstrate the trade-offs between security, performance, and energy efficiency in IoT networks. Strong encryption methods like AES and ECC provide robust security but at the cost of increased latency and reduced energy efficiency. In contrast, lightweight encryption methods like Simon and Speck offer lower latency and higher energy efficiency, making them more suitable for resource-constrained environments. The experiments further highlight the role of security enhancements, such as artificial noise and beamforming, in improving physical layer security without significantly compromising network performance. These findings provide valuable insights for optimizing the security and efficiency of IoT networks in various real-world applications.

VI. Conclusion and Future Work

This research thoroughly examined the performance of various encryption techniques within MIMO-based 5G IoT networks, focusing on key metrics such as latency, throughput, energy efficiency, and security strength. The study provides valuable insights for network designers and researchers into how different encryption methods impact performance, particularly in environments constrained by power and resources. The results highlight the trade-offs between strong encryption algorithms, like AES, which offer high security at the expense of increased latency and energy consumption, and lightweight algorithms, such as Speck and Simon, which provide lower latency and improved energy efficiency but with reduced security strength. These findings reinforce the need for careful selection of encryption techniques based on the specific requirements of IoT applications, where balancing security and efficiency is critical.

Moreover, this study stands out by taking a holistic approach in evaluating encryption performance alongside traffic management techniques and the impact of physical layer security mechanisms under jamming attacks. By integrating these factors, the research offers a broader understanding of how encryption methods perform under real-world conditions. The insights gained from the experiments demonstrate the network's resilience against jamming, as well as the importance of choosing the right traffic management strategy to optimize performance. This comprehensive analysis serves as a foundation for designing secure and efficient IoT networks that are adaptable to various operational environments and challenges.

While this research provides a detailed evaluation of encryption techniques and traffic management in IoT networks, several areas offer potential for future investigation. One promising direction is the exploration of hybrid encryption schemes that blend the strengths of multiple algorithms to achieve a more optimal balance between security and performance. Additionally, future studies could investigate the impact of dynamic network conditions, such as varying traffic loads, mobility patterns, and changing interference levels, to develop adaptive security frameworks that can respond in real time to evolving threats and network demands.

As 5G networks continue to evolve and with the forthcoming transition to 6G, incorporating advanced technologies such as machine learning and artificial intelligence for security and traffic management optimization could offer new opportunities. These technologies could enable more intelligent decision-making in real time, enhancing both the security and efficiency of large-scale IoT deployments. Furthermore, exploring the integration of quantum-resistant encryption methods, particularly in the context of critical infrastructure and highly sensitive IoT applications, would be a valuable area for future research, ensuring that IoT networks remain secure as the threat landscape evolves.

Acknowledgment

The research project was supported by the Hellenic Foundation for Research and Innovation (H.F.R.I.) under the "2nd Call for H.F.R.I. Research Projects to support Faculty Members & Researchers" (Project Number: 02440).

References

[1] R. A. Peña, M. Pascual, A. Astarloa, D. Uribe and J. Inchausti, "Impact of MACsec security on TSN traffic", *2022 37th Conference on Design of Circuits and Integrated Circuits (DCIS)*, Pamplona, Spain, pp. 01-06,2022.

[2] Z. G. Nkosi and T. E. Mathonsi, "A Hybrid Security Algorithm for 5G-Internet of Things", 2024 International Conference on Electrical, Computer and Energy Technologies (ICECET, Sydney, Australia, 2024, pp. 1-6.

[3] A. Jaiswal, et al, "Secrecy Rate Maximization in Virtual-MIMO Enabled SWIPT for 5G Centric IoT Applications", in IEEE Systems Journal, vol. 15, no. 2, pp. 2810-2821, June 2021.

[4] Y. S. Chowdhary and G. Singh, "The Convergence of IoT and 5G: Transforming Connectivity in Smart City Applications", 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, pp. 311-318, 2024.

[5] A. Jaiswal, S. Kumar, O. Kaiwartya, N. Kumar, H. Song and J. Lloret, "Secrecy Rate Maximization in Virtual-MIMO Enabled SWIPT for 5G Centric IoT Applications", in IEEE Systems Journal, vol. 15, no. 2, pp. 2810-2821, June 2021

[6] X. Lu, et al., "Reinforcement Learning-Based Physical Cross-Layer Security and Privacy in 6G", in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 425-466, Firstquarter 2023

[7] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi and M. Mustaqim, "Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios", in IEEE Access, vol. 8, pp. 23022-23040, 2020

[8] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan and X. Chen, "Convergence of Edge Computing and Deep Learning: A Comprehensive Survey", in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 869-904, 2020

[9] Z. Ding et al., "Application of Non-Orthogonal Multiple Access in LTE and 5G Networks", in *IEEE Communications Magazine*, vol. 55, no. 2, pp. 185-191, 2017

[10] Joan, Daemen, and Rijmen Vincent.,"The design of Rijndael: AES-the advanced encryption standard", Information Security and Cryptography 196 (2002).

[11] R.Beaulieu,et al, "The SIMON and SPECK lightweight block ciphers", Proceedings of the 52nd annual design automation conference. 2015

[12] "Shannon–Hartley theorem," Wikipedia, 29-Mar-2023. [Online]. Available:"https://en.wikipedia.org/wiki/Shannon%E2%80%93Hartley_theorem". [Accessed: 28-Apr-2023]

[13] C. Silva, V. A. Cunha, J. P. Barraca, and R. L. Aguiar, "Analysis of the Cryptographic Algorithms in IoT Communications", Information Systems Frontiers, vol. 26, no. 4, pp. 1243-1260, Aug. 2024.

[14] S. Gallenmüller, J. Naab, I. Adam and G. Carle, "5G QoS: Impact of Security Functions on Latency", NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, pp. 1-9, 2020.

[15] V. S. Miller, "Use of Elliptic Curves in Cryptography", in Advances in Cryptology - CRYPTO '85 Proceedings, H. C. Williams, Ed. Berlin, Heidelberg: Springer, pp. 417-426, 1986.