Enhancing the Wireless Network's Energy Efficiency to Reduce Security Challenges in 5G Systems: A Review

UMAR DANJUMA MAIWADA[1], KAMALUDDEEN USMAN DANYARO[1], ALIZA BT SARLAN[1], M. S. LIEW[2], UMAR ISMAILA AUDI[1]
[1]Department of Computer and Information Science,
Universiti Teknologi Petronas,
32610 Seri Iskandar, Perak,
MALAYSIA

[2]Civil & Environmental Engineering Department,
Universiti Teknologi Petronas,
32610 Seri Iskandar, Perak,
MALAYSIA

Corresponding Author

Abstract: - The desire for faster data speeds and increased Energy Efficiency has prompted the development of femtocells, which are short-range, low-cost, customer cellular access points. However, in a situation of Distributed Denial of Service (DDoS) which is caused by inefficient energy, distributed attack sources could be employed to amplify the assault and increase the attack's impact. By flooding the network with packets and creating malicious traffic, Distributed Denial of Service (DDoS) attacks try to deplete the network's communication and processing capability. A DDoS assault must be identified and neutralized quickly before a valid user can reach the attacker's target for 5G network to have an effective Energy Efficient service. For the next Fifth Generation (5G) Wireless Network, there is a pressing need to build an effective Energy Efficient mobile network solution. Despite their evident promise in assisting the development and deployment of the complicated 5G environment. The physical product, the digital product, and the relationship between both the physical and virtual goods are said to make up Digital Twin (DT). On the other hand, DT allows real-time communication with both the physical twins. The synergy of energy efficiency and security improvements in this research contributes to a more holistic optimization of 5G networks. This approach seeks to minimize energy consumption while fortifying the network against evolving security threats. Integrating energy-efficient practices with robust security measures enhances the overall resilience and sustainability of 5G systems. This is crucial for ensuring continuous, reliable, and secure communication in the face of dynamic challenges.

Key-Words: - Digital Twin, Energy Efficiency, DDoS, 5G network, Wireless-Network, Intrusion Detection, SDLM.

Received: July 13, 2022. Revised: September 9, 2023. Accepted: November 2, 2023. Published: December 4, 2023.

1 Introduction

The exponential expansion of customers who rely on the internet and network with paradigm shift in mobile networks necessitates modifications to the security architecture due to new security issues that do not exist in previous mobile networks. In contrast, scientists are currently working to improve the Energy Efficiency of every network tier. Creating green networks or Energy-Efficient computer network architectures is one such attempt, [1].

A Distributed Denial of Service (DDoS) assault on one 5G femtocell could influence other 5Gs. For instance, overloading the host machine's network link would have an effect on the hosted 5Gs, [2]. Security takes priority when these important developments work together. Additionally, the possibility of a Distributed Denial of Service (DDoS) assault is real, and the effects it would likely have on 5G enabled IoT applications will be greater. There is need to have a defense system that is more effective than the current ones, [3].

The notion of Digital Twin (DT) arose to make physical objects and relevant data sources available to software and clients on digital channels. The terms digital counterpart, virtual twins, virtual product, research agents, and avatars are used to describe notions that are comparable or partially overlap, [4]. The physical product, the digital product, and the relationship between both the physical and virtual goods are said to make up DT. Hence, DT allows real-time communication with both the physical twins. Interested entities, such as workflows, can use a DT to read data from a physical product, evaluate it, and run simulations. With the use of a DT, actuation orders, control signals, and data may be transferred to the physical twin, [5]. Furthermore, smart phones have made it feasible to monitor numerous data sources in real time as from user without the need to elaborate the purpose-built sensor installations. This information may be utilized to enhance virtual worlds with real-world features, [6].

Global adoption of fifth generation (5G) mobile communication systems is imminent. Currently, 5G is being implemented in modest locations across practically all continents, with a greater number of networks being made available in Europe and the USA, [7]. In future, 5G is predicted to account for at least 15% of the total mobile communications market by 2025, [8]. As a result, there is a high need to look at the impact of 5G on major areas of data management and processing research, such as databases, distributed systems, block-chain, machine learning, and cryptography.

The 5G Digital Twin is a novel approach to testing and assurance that provides a software duplicate of the 5G physical network which enables continuous prototyping, testing, assurance, and self-optimization of the living network. Therefore, a virtual solution that can construct a digital model and correctly replicate the 5G ecosystem is also required. This will assist in overcoming all the above challenges to meet the 5G needs. The DT can evaluate performance, predict the influence of environmental change, and optimize 5G network processes and decision-making for that matter. The Digital 5G model will coexist with the physical 5G network in the 5G DT to conduct operational forecasts and enforce optimum decisions into the living network and associated systems. A dependable, high performance, incredibly fast internet connection using cutting-edge networking technology is a crucial necessity for the integration and deployment of all the technologies in the digitization process. One of the primary pillars of the modernization process is the Digital Twin technology. It enables the creation of digital representations of physical systems, which has a number of advantages like security, real-time monitoring, greater productivity, and efficiency, [9].

2 Research Problem

In wireless networks, Energy Efficiency is a major challenge, especially with the introduction of 5G technology. To power and sustain the network infrastructure, 5G systems' increasing data speeds, higher network density, and proliferation of connected devices require a considerable quantity of energy. But in addition to adding prices, this increased energy use has negative effects on the environment, [3]. In parallel, 5G security issues are getting more complicated and varied. There are various potential vulnerabilities for attackers to take advantage of due to the large number of connected devices and the massive network infrastructure. Unauthorized access, data breaches, identity theft, and other malicious actions are examples of potential threats that could jeopardize the availability, confidentiality, and integrity of network resources and services.

An attempt to interfere with an online service is made by a Distributed Denial-of-Service

(DDoS) attack. Such an attack might have disastrous effects, especially in the chaotic economy of today, when many companies now offer services online and many workers work from home. For instance, if any video conferencing services, such as Microsoft Teams, Zoom or Google Meet, are disrupted, it would not only have a negative effect on the service provider but also have disastrous effects on other companies that depend on these internet platforms to conduct business, [10], [11], [12].

5G is quickly becoming a central topic of discussions about connectivity and digital transformation in general. Low latency, high bandwidth, high capacity, excellent reliability, enhanced mobility, and extended battery life are among the features that potentially alter industry use cases for WSN, [13]. In complicated systems, however, such precise prediction is generally difficult to attain. Since connected devices are frequently used to conduct Distributed Denial-of-Service (DDoS) assaults, mobile operators must keep an eye on their network security infrastructure, traffic patterns, and capacity demands to avoid potential damage from incoming and outgoing attacks. DDoS assaults pose a danger to 5G's capacity to supply high-bandwidth, low-latency services, which are required for the efficiency of energy, [6], [8]. As a result, the research problem seeks to identify novel approaches that can improve wireless networks' Energy Efficiency in the 5G era while successfully addressing security issues. It entails looking into ways to reduce power consumption in different network elements such as base stations, user devices, and network protocols without compromising network performance or security precautions. The objective is to create plans that strike a balance between security and Energy Efficiency, allowing 5G systems to operate sustainably and securely. There is no research and development of user-centric security solutions that empower end-users to actively participate in securing their devices and data. There is need for extended research which includes future generations of wireless networks (5G and beyond) and their energy efficiency and security requirements.

2 Review of Some Related Literatures

According to, [6], they concentrated on resource allocation, power management, sleep mode operation, and energy harvesting technologies in 5G networks. They find out more on the security issues that are unique to 5G networks, such as mobile verification, privacy-preserving protocols, secure key management, secure network slicing, and defense against new threats like jamming, spoofing, and network slicing assaults.

According to, [2], to balance energy consumption and security requirements in 5G networks, the research looks at some suggested energy-aware security techniques. It investigates efficient Intrusion Detection and prevention systems (IDPS) designed for resource-constrained devices in 5G networks, as well as Energy Efficient encryption techniques, lightweight authentication protocols, and IDPS. They examined how NFV and SDN can improve the security and Energy Efficiency of 5G networks. Their research touches network slicing, dynamic resource allocation, and virtualized security services in the context of safe and Energy Efficient network operations.

According to, [14], the pillars of the digital transformation process are numerous, and they included all parts of research units, from IT operations to automation and intelligence, as well as training employees for such a change. In a survey of research that has successfully digitally changed.

According to, [15], 5G DT is viewed as a catalyst for new emergent services, including a city management technologies that could aid poor countries in managing crucial difficulties like a traffic control, water and sanitation management, and urban security. Considering the current global pandemic crisis, a 5G DT might genuinely aid in the understanding of COVID-19's spread and depending on 5G DT's AI which could predict the approximate position of epidemic hotspots. Developing a DT using a 3D model of the metropolitan area and overlapping the 5G system with additional data, including a transportation system, street lines, structures, IoT data, individual movements and operations, and epidemic data from recent and past pandemic trends, may be used to achieve this.

According to, [16], [17], the DT may assess the overall performance of a 5G connected vehicle and enable customized services to be delivered. AI is used to forecast a vehicle's performance under a variety of dynamic scenarios, diagnose issues, and implement improvements, making the user's driving experience safer. Before deploying the technology on public roadways, it must be thoroughly tested using emulations. The Spirent 5G DT uses a 3xD drive-in simulator to simulate a 5G network for evaluating the behavior and performance of connected vehicles in a controlled realistic environment.

According to, [18], In relation to the density of femtocell deployment, the UE simultaneously achieves enhanced QoS and significantly reduced energy consumption per bit. More complex HO decision algorithms with the inclusion of LTE femtocells are necessary, alongside an Energy Efficient HO decision procedure for the macrocell - femtocell LTE system that seeks to lower power transferred at the mobile terminals, thus allowing to optimally utilize the native femtocell authority in terms of improved QoS and lower consumption of energy.

According to, [19], different service levels in terms of throughput, latency (delay), jitter (delay fluctuation), and packet errors or loss are provided for different types or streams of data to offer QoS. The goal of their work is to present a basic QoS principle for the 5G LTE service.

According to, [20], they uses WLAN models from network simulators to create Energy Efficiency and secure wireless networks. The main contributions of this study include the effect of proposed Energy Efficient WTLS security protocol modifications on the energy used by the IPsec protocol, principles to enhance the precision and effectiveness of WLAN energy models to effectively simulate massive and intricate wireless networks, and design and verification of energy models for WLAN situations using real-world measurements.

According to, [21], Modeling and Simulation (M&S) has been used for a long time as a method of decision-making for a range of complex problem solutions, including the application in Digital Twins. In contrast to the overall multi-dimensional nature of real-world complex systems, standard single type M&S techniques, such as Discrete Event Simulation (DES), System Dynamics (SD), and Agent-Based Simulation (ABS), might encounter significant challenges in accurately representing such systems at various abstraction, temporal, or spatial levels. To address these difficulties, a variety of hybrid and multi-model M&S techniques for simulation and modeling of various aspects of complex systems have been developed.

According to, [22], Attacks via Distributed Denial of Service (DDoS) damage the Internet's digital accessibility. The user's expectation of receiving prompt and efficient services could be severely harmed by DDoS attackers. There are numerous stories of DDoS attack incidents that have had catastrophic repercussions on Internet users and web services. Users are multiplying daily in the current digital environment, which is dominated by wireless, mobile, and IoT gadgets. Because most users are inexperienced, DDoS assaults frequently target their devices, or they unintentionally join the DDoS attack Force.

According to, [23], Threats from the radio interface can be deadly due to 5G's increasing access speeds and the rapidly expanding IoT technology. To address the three stages of a DDoS attack, the breach or infection of terminals, the weaponization of the terminal, and the DDoS attack itself, DDoS detect, and mitigation will be required. Even when under attack, critical network services and customer experience must be maintained. For 5G enterprise customers, security reporting and analysis will be crucial. These will comprise attack mitigation records, event analysis, host infection predictive analysis, and pattern reports.

According to, [24], The current research has covered a range of 5G concerns as well as the security risks posed by IoT. The repercussions of the most serious cyberattack, known as a Distributed Denial of Service Attack (DDoS), call for loT's attention, making finding solutions essential. As a result, it offers an overview of the development of 5G, 5G-enabled IoT applications, and the size of DDoS attacks in such applications. Their study offers guidance on creating secure 5G enabled IoT apps by outlining several DDoS attack defense strategies.

Table 1. Table of related works

NAME OF AUTHOR	PROBLEM	METHOD	RESULT
[28]	Complex difficulties in the real world Consider the power grid.	Online investigation of the power system using a large-scale network model.	With only a sub-second latency, it tracks or mirrors the operating condition of a large-scale Power grid in real-time.
[29]	Examine DT advancement in product design and learn about DT trends in prominent research fields.	Conceptual design, detailed design, design verification, and redesign are the four categories for methodology adoption.	It has been discovered that using data from existing product DT, DT may successfully aid in concept creation and redesign.
[30]	The radio resource allocation problem	Game theoretical framework	The simulation results show that the proposed method can significantly decrease the traffic load on the core network and thereby, enhance the total coverage and data rate performance.
[31]	Current tools may not be able to be integrated and utilized concurrently for a certain goal due to differences in formats, protocols, and standards.	The research looked at and summarized technology and techniques that make DT possible.	The document gives broad guidelines for enabling technologies, as well as some examples of tools and how to choose them.
[32]	Too much energy is used, and resource allocation and job offloading strategies are not optimized.	To train the DL algorithm, like a Digital Twin of the real network is used.	Improve the EE of users in a MEC system, while keeping in mind the URLLC services' latency and reliability limits, as well as the stability requirements of delay tolerant services.
[33]	Several real-world issues with sophisticated telecommunications networks.	Design, building, and operation of equipment, as well as the creation of modernization concepts.	Monitoring traffic, including its normal behavior, helps prevent erroneous actions in emergency circumstances and to become a useful instrument for undertaking multidisciplinary research.

From the research of, [25], IoT devices will be able to communicate and share data with 5G networks more quickly than ever before, but this development is likely going to make existing systems more vulnerable to security risks, like those caused by malicious nodes. Studies have proposed novel 5G network-compatible remedies for several of the issues related to security, such as an efficient control system for access that addresses the challenge of one functionality bottleneck which avoids unwanted procedure within the network. Thus, however, it is not what the model is intended to do; rather, it is focused on a vehicular situation.

This study, [26], documents network vulnerabilities from a wide angle and tracks the status of traffic monitoring. By integrating and combining many security service modules, it effectively uses traffic flow detection to find intrusions. Once the network flows were classified using a combination of the kmean++ and the adaboost model algorithms, a selection of common traffic features was selected using Random Forest, an automated learning technique. Since there are not many suitable, sizable 5G traffic datasets, a method for gathering data has been proposed. This method examines beam-selection techniques on automotive-to-infrastructure via millimeter waves by generating 5G propagation channel data using a ray-tracing simulator coupled with a vehicle traffic simulator. Regression, classification, and learning by reinforcement have all benefited from the evaluation and analysis of deep learning. Furthermore, it anticipates the best beam combinations for mmWave to mobile networks using machine learning, but it does not calculate the necessary bit size to characterize the properties of the entire network, [27].

Table 1 below shows the related works based on the author's name, problem talked about, method used to solve the problem and lastly the result they obtained at the end of their analysis. In that case we formulated our research problem and focused on the challenges of energy efficiency. Upgrading existing infrastructure and implementing energy efficient technologies may require significant investment. Optimizing energy efficiency while maintaining network performance and security requires sophisticated management mechanisms. Ensuring compatibility and interoperability between different vendors' equipment and protocols can be challenging. The constantly evolving nature of security threats requires continuous monitoring, updates, and adaptation of security measures.

3 Methodology

3.1 Modelling Approaches of Digital Twin

In most research endeavors, several modelling methodologies are expected. Digital Twins can employ a variety of modelling techniques, including geometric and geographical modelling, as well as computational/mathematical/numerical modelling. The model of the supply chain scenario utilized an actor language, in which each actor has a state machine-like behavior. The researchers aren't constrained by any one simulation paradigm, approach, or programme, [34].

3.2 Tool for Modelling of Digital Twin

Digital Twins are discussed in numerous domains of technology, economics, and medical in the scientific literature. However, most of the scholarly literature on the usage of Digital Twins pays little attention to the creation of modeling for Digital Twins. Frequently, the notion of a Digital Twin is discussed, rather than the model used to imitate an actual system. The scope of simulation within the idea of Digital Twin defines and justifies the demands for modeling in Digital Twin. Models for Digital Twins are typically necessary to correctly imitate the original system. One of the prerequisites for Digital Twin modelling is the integration of models throughout the Digital Twin's lifespan, as well as a user-friendly interface for managing and affecting the model in a manner similar to the original system, [35].

3.3 System Development Life Cycle Model (SDLCM)

A comprehensive framework for managing the development of systems is provided. The methods of start determine the type and reach of the study. It is doubtful that the approach will be adequate for satisfying the needs of the research if this phase is not carried out well. The research is properly organized in depth after the initiation stage. In addition to integrating and carrying out the research's activities in line with the project management strategy, it also involves organizing people and resources. To identify possible issues early and take corrective action when necessary to regulate the model's execution, monitoring and controlling methods are used to keep track of how works are being carried out. Continue to maintain and improve the system. Closing of model- that is the end of the research, work has finished, [36].

3.4 Waterfall Model

Following the completion of each phase of the life cycle in order, the results go on to the following phase. Once a phase is finished (like a waterfall), it is impossible to go back or very difficult to do so as seen in Figure 1 below. The primary outputs for each step are usually created on paper. (Hundreds of pages in length). Each phase's decisions are final, which means they cannot be modified. The criteria are expressed precisely and concisely, and they hold true throughout the entirety of the work's development. A new developer can easily obtain all the essential information through documentation of each phase of development. This provides resilience for alterations in human resources. Problematic issues are less when the project management organization is carefully planned. It is simple to gauge progress because each phase has a defined beginning and ending point, [37].

Figure 1 below shows the waterfall model with the requirement analysis, system design, implementation, testing and finally deployment.

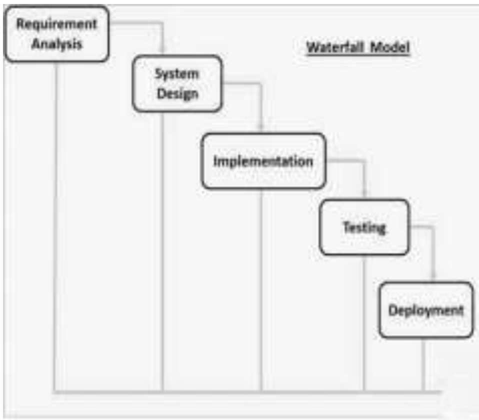


Fig. 1: Waterfall Model

4 Result of Findings

Designing a framework for applying Digital Twin to solve difficulties of Energy Efficiency which is posed by DDoS attack. The DT model can be used to detect attacks, and the solution may be helpful to prevent DDoS attacks. In-depth study / analysis of connected issues, as well as the 5G itself, which would be used on EE. Finally, we discussed a DT network model and tested some models of 5G in Energy Efficiency. It is expected that DT network will be used for the deployment of 5G network to improve the Energy Efficiency of wireless network to have security mitigation against DDoS attack in 5G Systems.

Figure 2 below shows the energy efficiency of network between time series and throughput to ensure seamless connection of the network.

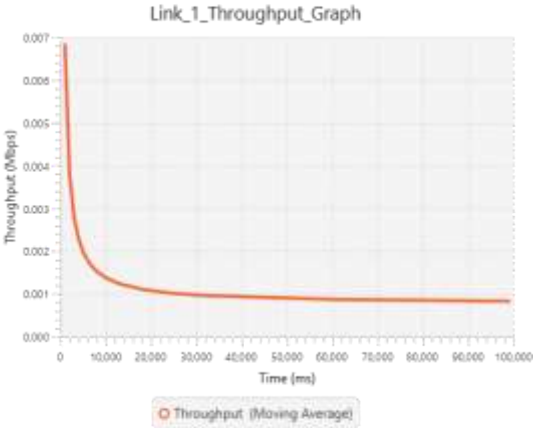
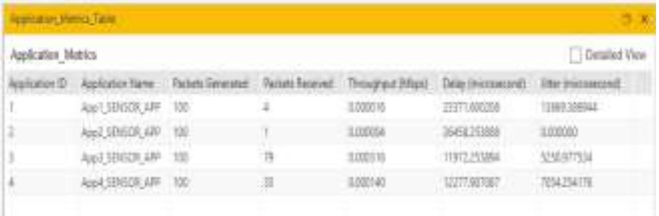


Fig. 2: Throughput vs Time

The compatibility levels mentioned in the matrix represent the current state of compatibility between the application and the listed systems, packets, throughput, delay, and jitter from Table 2 below.

Table 2. Application Metrics table



Application_Metrics_Table

Application_Metrics

□ Detailed View

Application ID	Application Name	Packets Generated	Packets Received	Throughput (Mbps)	Delay (microsecond)	Jitter (microsecond)
1	App1_SENSOR_APP	100	4	0.000016	23371.600208	13869.386944
2	App2_SENSOR_APP	100	1	0.000004	26458.253888	0.000000
3	App3_SENSOR_APP	100	79	0.000316	11972.253864	5256.977534
4	App4_SENSOR_APP	100	33	0.000140	12277.907087	7054.254178

The movement of UE inside the network is shown in Figure 3 below where there is a graph of network moving with UE.

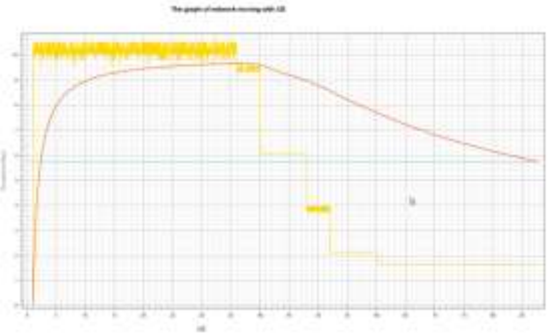
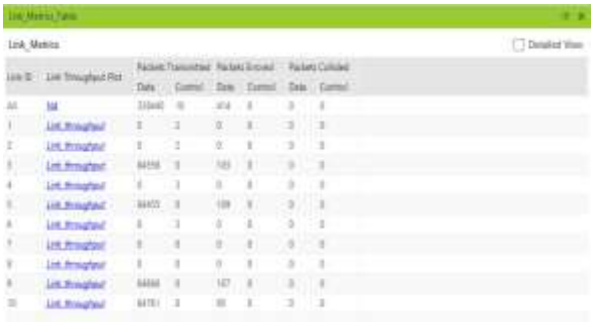


Fig. 3:Throughput Vs User Equipment

From Table 3 below, it is seen that the internal links connect related packets, improving the UE and facilitating navigation. For external links, focus on linking to reputable and authoritative packets that add value to the content.

Table 3. Table of Link Metrics



Link_Metrics_Table

Link_Metrics □ Detailed View

Link ID	Link Throughput Plot	Packets Transmitted		Packets Errored		Packets Collided	
		Data	Control	Data	Control	Data	Control
All	All	333440	0	414	0	0	0
1	Link_throughput	0	0	0	0	0	0
2	Link_throughput	0	0	0	0	0	0
3	Link_throughput	64456	0	103	0	0	0
4	Link_throughput	0	0	0	0	0	0
5	Link_throughput	64405	0	109	0	0	0
6	Link_throughput	0	0	0	0	0	0
7	Link_throughput	0	0	0	0	0	0
9	Link_throughput	0	0	0	0	0	0
8	Link_throughput	64466	0	107	0	0	0
10	Link_throughput	64781	0	93	0	0	0

Figure 4 shows UE in A3 state that UE is relaxed for the period with no work done to avoid unnecessary handover.

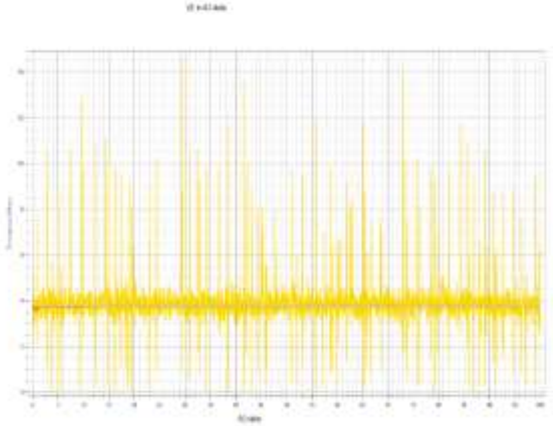


Fig. 4:UE in A3 State

A3_event=∣RSRP target−RSRP source ∣<Hysteresis (1)

Here:
RSRP target is the Reference Signal Received Power (RSRP) of the target cell.
RSRP source is the RSRP of the source cell.
Hysteresis is the hysteresis value, which is a parameter set to avoid unnecessary handovers due to small, rapid changes in the radio environment.
Energy Efficiency Metric (EEM) = Accuracy of Mobility State Detection / Energy Consumption (2)

Before a site visit, a virtual 5G rollout was tested using the DT as seen in Figure 5.

Fig. 5: Digital Twin in 5G network protected against DDoS attack.

The research has reduced the deployment of random femtocells which makes mobility difficult. Overall handover suffers because of cell type and cell size, the research has helped in providing solution to the handover in terms of DDoS attack. Slice isolation is anticipated to be able to lessen the effects of attacks by DDoS on a basic network service. The 5G DT design has reduced human participation in physical network design and validation, which has two benefits: cheaper labor costs and fewer human mistakes (Figure 6).

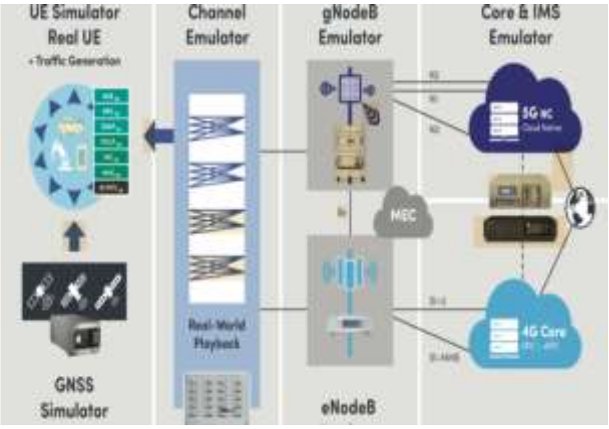


Fig. 6:Digital twin and 5G Systems

5G network testing involves network traffic, data services, and signaling messages to ensure that the network's functionalities and performance meet the expected standards in improving energy efficiency (Figure 7) below.

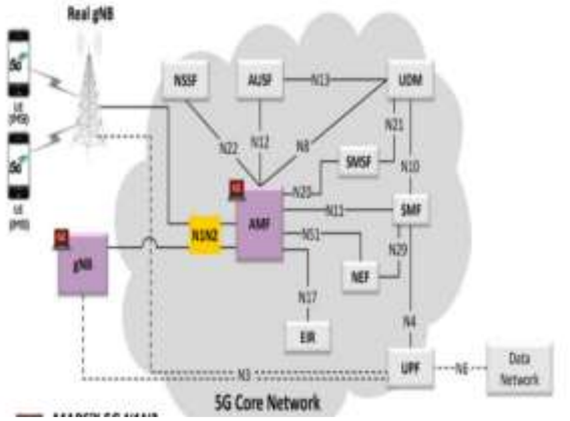


Fig. 7:Energy Efficient 5G System

In the End-to-End 5G network architecture, the network comprises various components, including the 5G Access Network (gNB), Access and Mobility Management Function (AMF), Authentication Server Function (AUSF), Network Slice Selection Function (NSSF), Unified Data Management (UDM), Session Management Function (SMF), Short Message Service Function (SMSF), Equipment Identity Register (EIR), and User Plane Function (UPF) connected to Data Server or Application Functions, and to EPC/IMS core for interoperability from Figure 8 below.

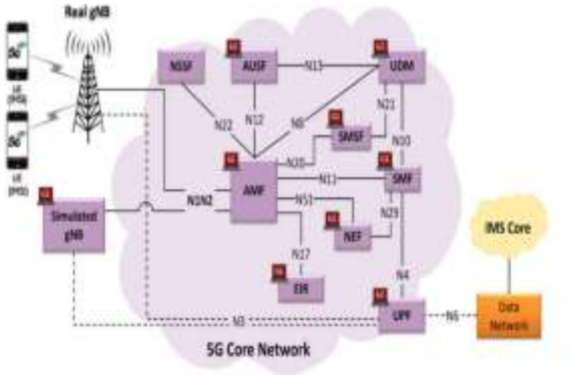


Fig. 8:Energy Efficient 5G System with IMS core

5 Discussion

The introduction of 5G technology represents a huge step forward in the evolution of wireless communication systems, providing unparalleled data rates, reduced latency, and connection in an increasingly interconnected world. However, as 5G system deployment advances, two important concerns emerge: the urgent need for improved energy economy and the requirement to combat rising security vulnerabilities. This paper investigates the complex link between these difficulties, looking at how advances in Energy Efficient network design can potentially mitigate security risks in 5G networks from Figure 7. Energy usage efficiency is a primary concern in the design and operation of wireless networks, particularly in the context of 5G systems. The expansion of high-capacity base stations, complex network design, and the significant energy demand of data centers necessitate novel techniques to energy consumption reduction as seen in Figure 8. As energy-saving solutions, concepts such as dynamic spectrum sharing, network virtualization, and improved power management techniques have emerged. These solutions not only decrease operational expenses but also contribute to a lower carbon footprint, which is in line with the global environmental agenda. The transition to 5G opens new opportunities, but it also presents a larger attack surface and a slew of new security challenges. The integration of Internet of Things (IoT) devices, as well as the convergence of physical and digital infrastructure, expands the potential vectors for cyberattacks. Vulnerabilities in 5G networks demand a holistic security paradigm, from man-in-the-middle assaults to authentication breaches. It is critical to protect sensitive user data, preserve network integrity, and assure continuous service availability. The symbiotic relationship between Energy Efficiency and security provides a thought-provoking aspect. While energy-saving measures help to optimize resource allocation and expedite network operations, they can have an unintended influence on security. Mechanisms like sleep modes and reduced computing overhead, for example, may impede real-time threat detection. Security measures, on the other hand, such as encryption and frequent authentication processes, can put a pressure on energy resources. Striking a precise balance between these interconnected considerations is critical to creating a strong and comprehensive network design. Recent research efforts have highlighted the possibility for novel technologies that address both Energy Efficiency and security simultaneously. Novel algorithms, machine learning-driven anomaly detection techniques, and blockchain-based authentication frameworks have resulted from collaborative efforts. These developments have the potential to reconcile the opposing objectives of energy conservation and security reinforcement. Researchers are pioneering ways that maximize performance, reduce energy expenditure, and strengthen protection mechanisms by exploiting real-time data analytics and the capabilities of edge computing. The goal of Energy Efficiency and security in 5G networks is not without difficulties. Striking the right balance between tight security requirements and efficient energy use necessitates meticulous calibration. Furthermore, the growing technological landscape, including the possible integration of 6G and beyond, provides dynamism, necessitating flexible and responsive solutions. For example, the fledgling possibility of quantum computing adds an exciting dimension to the security-energy equation. In an era of exponential development and unprecedented connectivity, the convergence of Energy Efficiency and security is critical for the long-term evolution of 5G systems. As demonstrated by the research presented, new solutions at the intersection of these difficulties give a look into a future in which seamless, secure, and Energy Efficient networks benefit societies and enterprises alike. Collaborative efforts among researchers, industry stakeholders, and regulators are critical to realizing this goal and ensuring that the promise of 5G is fully realized while protecting against new security threats.

6 Conclusion

In conclusion, a critical area of research and development with significant consequences for the future of telecommunications is the endeavor to improve the energy efficiency of the wireless network to concurrently reduce security concerns in 5G systems as seen in Figure 2, Figure 3 and Figure 4. This dual-focused strategy recognizes the complex interrelationship between security and energy efficiency and the ways in which accomplishments in one area can strengthen and support those in the other. To put it simply, the process of improving 5G systems' energy efficiency and reducing security risks is dynamic and continuous. The results of this study could completely reshape the possibilities of 5G technology, offering not only quicker and more effective communication but also a safe and long-lasting basis for digitalization, (Figure 6). This dual optimization strategy will be crucial in determining how 5G develops and shapes the upcoming wave of wireless networks. A cost-efficient solution in virtualized networks requires appropriate resource management. Networks that have been virtualized have a variety of benefits and drawbacks. Virtual networks have certain security flaws; however, security is a necessity that is always being enhanced. Attacks on networks, however, are also increasing in frequency and sophistication. DDoS attacks are simpler to launch and more difficult to counter. Therefore, it is necessary to continuously develop fresh defenses against DDoS attacks. The safety of virtual networks was our main concern. We focus on the co-residency problem in 5G networks as well as the effects of DDoS assaults on availability of services in 5G mobile networks and EE. We ran tests in EE to see how DDoS attacks affect service availability as in Figure 1.

The use of DT for 5G technology has lately attracted a lot of attention, notably from major telecoms. DT could evaluate performance, forecast the impact of environmental change, and enhance 5G network operations and decision-making as a result. The digital 5G framework in Figure 5 has operated in tandem with physical 5G technology to provide operational forecasts and implement optimum decisions in the live network and its related services. Deploying an experimental 5G network would be prohibitively expensive, especially in underdeveloped nations where the 4G deployment is still underway. If the influence of 5G cell deployment can be reliably forecast in advance, this could tremendously assist decision-makers in developing appropriate policies for their respective nations, prevent costly and irrevocable investment blunders.

The 5G DT design has reduced human participation in physical network design and validation from Figure 5, which has two benefits: cheaper labor costs and fewer human mistakes. Before a site visit, a virtual 5G rollout must be tested using the DT. The model will be tested in a genuine 5G DT environment developed, utilizing 5G environment model to evaluate the mechanism's efficacy. The testing finding has confirmed that the suggested approach is capable of efficiently improving Energy Efficiency and mitigate DDoS attack in 5G systems. In general, improving the

Energy Efficiency of wireless networks to lessen security issues in 5G systems could boost network performance, cut costs, strengthen security, and contribute to a sustainable and dependable 5G infrastructure.

Subsequent investigations into augmenting the energy efficiency of wireless networks to mitigate security obstacles in 5G systems ought to concentrate on multiple crucial avenues to tackle nascent concerns and enhance the durability and safety of 5G networks. Examine how edge and fog computing might improve 5G network security. Examine how putting security features closer to the network edge can minimize energy consumption and cut down on the latency of security checks. By advancing research in these areas, 5G networks will continue to develop and become more robust, secure, and long-lasting in the face of new obstacles and a variety of application scenarios. The advancement of 5G technology depends on the interdisciplinary nature of this study, which brings together knowledge in networking, security, and energy efficiency. Future developments in technology, new threats, and the changing telecom environment will probably influence how to improve the energy efficiency of the wireless network to lessen security issues in 5G systems. These future paths demonstrate the necessity of a thorough and flexible strategy for dealing with the changing difficulties in 5G networks. The relationship between security and energy efficiency will remain crucial as networks develop and new technologies appear. Researchers and industry players will be key players in determining how wireless communication develops in the future by creating creative solutions that balance security and energy efficiency.

7 Practical Application

Improving the energy efficiency of the wireless network to lessen security issues in 5G systems has a few useful applications that solve important issues with network resilience, operating costs, and sustainability. Here are a few real-world examples:

1. Green networking in smart cities: Putting energy-saving techniques into 5G networks for applications related to smart cities. Lowering the carbon footprint of smart city infrastructure, maximizing energy efficiency in crowded regions, and encouraging environmentally friendly urban growth.
2. Deploying 5G networks with improved energy efficiency for industrial Internet of things applications is the second use of energy efficient industrial IoT (IIoT) deployments. Reducing environmental impact and costs by providing energy-efficient connectivity for a wide range of IoT devices in industrial environments.
3. Remote Healthcare Services: Putting secure, energy-efficient 5G networks into place to facilitate remote healthcare services. Optimizing energy consumption and enhancing the security and dependability of healthcare communications to enable effective telemedicine and remote patient monitoring.
4. Energy-Efficient Edge Computing: Including edge computing features in energy-efficient 5G networks. Optimizing energy usage for edge nodes, lowering latency for edge applications, and enhancing edge computing performance overall.
5. Sustainable and Safe Rural access: Expanding 5G networks that use less energy to offer safe access in remote locations. Providing dependable and secure communication and bridging the digital divide in rural areas while optimizing energy use for infrastructure.
6. Catastrophe Response and Public Safety: Using secure, energy-efficient 5G networks for public safety and catastrophe response. Reducing the amount of energy required by adaptable base stations and communications equipment in disaster-affected areas, as well as guaranteeing reliable and secure connection during catastrophes.
7. Efficient Data Centers and Cloud Services: Connecting 5G networks that are energy-efficient with data centers and cloud services. Improving network and cloud resource connectivity will lower data center energy usage and help create a more economical and environmentally friendly cloud infrastructure.
8. Lowering Operational Expenses for Telecom Operators: Energy-efficient technologies can be integrated into 5G networks to lower operating expenses. By enabling telecom operators to reduce their energy costs, 5G installations will be more economically sustainable overall.

9. Safe and Energy-Saving Mobile Banking: Installing 5G networks that are both safe and energy-saving to enable mobile banking services. Improving financial transaction security while maximizing mobile device and network infrastructure energy utilization.

10. Energy-Efficient Smart Grids: 5G networks that are energy-efficient are used in smart grid systems to facilitate communication. Optimizing energy consumption in communication infrastructure for power grid monitoring and management, as well as enhancing the effectiveness and dependability of smart grids.

These real-world uses demonstrate the range of ways that improving 5G networks' energy efficiency can address security issues and offer dependable, long-term connectivity for a range of businesses and services. The telecommunications ecosystem is made more resilient, economical, and ecologically friendly by the integration of security and energy saving technologies.

8 Contribution

The research can help create energy-saving approaches, algorithms, and protocols for 5G systems by concentrating on Energy Efficiency. As a result, the network operations may use less energy and produce less carbon dioxide, improving their environmental sustainability. For network operators, increased Energy Efficiency can save a lot of money. The research can assist in lowering operational costs related to energy usage and infrastructure maintenance by optimizing energy consumption in various network components, such as base stations and user equipment. In 5G networks, user devices like smartphones and IoT devices may have longer battery lives with Energy Efficient network architecture and protocols. Hence, the user experience may be improved, disruptions may be minimized, and frequent battery charge may be less necessary. By maximizing resource allocation and lowering network congestion, Energy Efficient approaches can increase network uptime and reliability. As such, the network architecture may become more stable and reliable, ensuring consumers receive uninterrupted service and minimizing downtime brought on by energy-related problems. The research has suggested strategies to improve the safety measures of 5G networks by tackling security problems. This can involve creating effective Intrusion Detection systems, encryption methods, and techniques for authentication that are customized for energy-constrained devices. The dangers of data breaches, unauthorized access, and other hostile activities can be reduced with stronger security measures. The study has helped discover and address new security risks that are particular to 5G systems, like network slicing attacks or flaws brought on by virtualized network services. The research has improved the overall security adaptability of 5G networks by comprehending these threats and creating suitable responses. It has applied secure and Energy Efficient practices in 5G systems, the research has offered network operators, service providers, and regulators useful guidance and recommendations. This can aid in the adoption of best practices, efforts at standardization, and the establishment of policies to build a secure and sustainable ecosystem.

DDoS attacks are increasing in frequency and power as computing resources become more affordable. A very few bots can overwhelm a server during DDoS assaults, rendering the service inaccessible to authorized users. We have discussed the DT model in Figure 5, which provides mitigation over DDoS attacks targeted at a particular service by utilizing the technically virtual design of Software-Defined Networks. The way DT operates is by copying the network. The outcomes of our experiments have demonstrated that DT reduces DDoS attacks by increasing the accessibility of a particular network resource through a virtual environment.

The research has established a new model for achieving Energy Efficiency using Digital Twin, specifically in telecommunication sector by providing a new way of treating DDoS in the network. The research suggested the use of Digital Twin's network for handling DDoS and improving EE. The research provides the reasoning model for achieving Efficient Energy in networks and mitigating the risk of DDoS. The contribution will enhance the strength of virtual environment over the real-world knowledge, not only in Malaysia but the world in general.

Acknowledgement:
I wish to acknowledge the contribution of Universiti Teknologi PETRONAS for giving me the tools and materials while conducting the entire preparation of this manuscript.

References:

[1] Series, M., IMT Vision–Framework and overall objectives of the future development of IMT for 2020 and beyond. *Recommendation ITU*, 2015. 2083: p. 21.

[2] Vishwakarma, R. and A.K. Jain, A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication systems*, 2020. 73(1): p. 3-25.

[3] Deivanai Gurusamy, Deva Priya M, Barmura Yibgeta, Assabu Bekalu, DDoS risk in 5G enabled IoT and solutions. International *Journal of Engineering and Advanced Technology*, 2019. 8(5): p. 1574-1578.

[4] Datta, S.P.A., Emergence of digital twins. arXiv preprint arXiv:1610.06467, 2016.

[5] Glaessgen, E. and D. Stargel. The digital twin paradigm for future NASA and US Air Force vehicles. in *53rd AIAA/ASME/ASCE/AHS/ASC structures, structural dynamics and materials conference 20th AIAA/ASME/AHS adaptive structures conference 14th AIAA*. 2012.

[6] Yiming Miao, Yingying Jiang, Limei Peng, M. Shamim Hossain, Ghulam Muhammad, Telesurgery robot based on 5G tactile internet. *Mobile Networks and Applications*, 2018. 23(6): p.1645-1654.

[7] Gillispie, C., South Korea’s 5G Ambitions. Academic Paper Series. *Korea Economic Institute of America*, 2020.

[8] Tobin, M., New Zealand Bans Huawei from 5G, *China Has Message for New Zealand*. This Week in Asia, 2019.

[9] Aidan Fuller, Zhong Fan, Charles Day, Digital twin: Enabling technologies, challenges and open research. *IEEE access*, 2020. 8: p. 108952-108971.

[10] Goodyear, M., The dark side of videoconferencing: The privacy tribulations of Zoom and the fragmented state of US data privacy law. HLRe: Off Rec., 2019. 10: p. 76.

[11] Ilag, B.N., Introduction: microsoft teams, in Introducing Microsoft Teams. 2018, Springer. p. 1-42.

[12] Basilaia, G. and D. Kvavadze, Transition to online education in schools during a SARS-CoV-2 coronavirus (COVID-19) pandemic in Georgia. *Pedagogical Research*, 2020. 5(4).

[13] Maiwada, U.D., A.A. Muazu, and N. Noor, The Security Paradigm That Strikes a Balance Between a Holistic Security Mechanism and The WSN's Resource Constraints. *East Asian Journal of Multidisciplinary Research*, 2022. 1(3): p. 343-352.

[14] Mashaly, M., Connecting the Twins: A Review on Digital Twin Technology & its Networking Requirements. *Procedia Computer Science*, 2021. 184: p. 299-305.

[15] Anssi Savisalo, Jukka Hemilä, Juha Salmelin, Kari Tuukkanen, Nokia Oyj, Sitowise Oy, Digital Twin as City Management Tool. in *19th Annual Conference on Land and Poverty: Land Governance in an Interconnected World*. 2018.

[16] Huan X Nguyen, Ramona Trestian, Duc To, Mallik Tatipamula, Digital twin for 5G and beyond. *IEEE Communications Magazine*, 2021. 59(2): p. 10-15.

[17] Stavropoulos, P. and D. Mourtzis, Digital twins in industry 4.0, in Design and operation of production networks for mass personalization in the era of cloud technology. 2022, *Elsevier*. p. 277-316.

[18] Xenakis, D., N. Passas, and C. Verikoukis. A novel handover decision policy for reducing power transmissions in the two-tier LTE network. in 2012 *IEEE International Conference on Communications (ICC)*. 2012. IEEE.

[19] Malisuwan, S., D. Milindavanij, and W. Kaewphanuekrungsi, Quality of service (QoS) and quality of experience (QoE) of the 4G LTE perspective. *International Journal of Future Computer and Communication*, 2016. 5(3): p. 158.

[20] Alviola, T., Energy efficiency in wireless networks. 2013.

[21] Somayeh Malakuti, Pieter Van Schalkwyk, Birgit Boss, Shyam Varan Nath, Digital twins for industrial applications. Definition, Business Values, Design Aspects, Standards and Use Cases. Version, 2020. 1: p. 1-19.

[22] Chaganti, R., B. Bhushan, and V. Ravi, The role of Blockchain in DDoS attacks mitigation: techniques, open challenges and future directions. arXiv preprint arXiv:2202.03617, 2022.

[23] Kautish, S., A. Reyana, and A. Vidyarthi, SDMTA: Attack Detection and Mitigation Mechanism for DDoS Vulnerabilities in Hybrid Cloud Environment. *IEEE Transactions on Industrial Informatics*, 2022.

[24] Akshat Gaurav, Brij B Gupta, Brij B GuptaFrancisco José García-Peñalvo, Kostas E. Psannis, Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks, in Security and Privacy Preserving for IoT and 5G Networks. 2022, *Springer*. p. 263-278.

[25] Afshan Ahmed, Sohail Jabbar, Muhammad Munwar Iqbal, Dr-Muhammad Ibrar, Aiman Erbad, Houbing Herbert Song, An Efficient Hierarchical Mobile IPv6 Group-Based BU Scheme for Mobile Nodes in IoT Network. *IEEE Internet of Things Journal*, 2022. 10(10): p. 8684-8695.

[26] Mohammed Al-Garadi, Amr Mohamed, Abdulla K. Al-Ali, Xiaojiang Du, Mohsen Guizani, A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, 2020. 22(3): p. 1646-1685.

[27] Tang, F., Y. Zhou, and N. Kato, Deep reinforcement learning for dynamic uplink/downlink resource allocation in high mobility 5G HetNet. *IEEE Journal on selected areas in communications*, 2020. 38(12): p. 2773-2782.

[28] Amani, A.M. and M. Jalili, Power grids as complex networks: Resilience and reliability analysis. *IEEE Access*, 2021. 9: p. 119010-119031.

[29] Fei Tao, He Zhang, Ang Liu, Andrew Y C Nee, Digital twin in industry: State-of-the-art. *IEEE Transactions on industrial informatics*, 2018. 15(4): p. 2405-2415.

[30] Ahmed, K.I., H. Tabassum, and E. Hossain, Deep learning for radio resource allocation in multi-cell networks. *IEEE Network*, 2019. 33(6): p. 188-195.

[31] Qinglin Qi, Fei Tao, Tianliang Hu, Nabil Anwer, Ang Liu, Yongli Wei, Lihui Wang, A.Y.C. Nee, Enabling technologies and tools for digital twin. *Journal of Manufacturing Systems*, 2021. 58: p. 3-21.

[32] Huilin Li, Haitao Xu, Chengcheng Zhou,Xing Lü, Zhu Han, Joint optimization strategy of computation offloading and resource allocation in multi-access edge computing environment. *IEEE Transactions on Vehicular Technology*, 2020. 69(9): p. 10214-10226.

[33] Dong Chen, Xu Guiqiong, Meng Lei, Yang Pingle, CPR-TOPSIS: A novel algorithm for finding influential nodes in complex networks based on communication probability and relative entropy. Physica A: *Statistical Mechanics and its Applications*, 2022. 603: p. 127797.

[34] Souvik Barat, Vinay Kulkarni, Tony Clark, Balbir Barn, An actor based simulation driven digital twin for analyzing complex business systems. in 2019 winter simulation conference (WSC). 2019. *IEEE*.

[35] Grieves, M.W., Virtually intelligent product systems: digital and physical twins. 2019.

[36] Koraish, Z. and O. Lustig Lindström, Understanding the software engineering challenges in blockchain technology: *A systematic literature review*. 2022.

[37] Carlos Baquero Barneto, Matias Turunen, Sahan Damith Liyanaarachchi, Lauri Anttila, Alberto Brihuega, Taneli Riihonen, Mikko Valkama, High-accuracy radio sensing in 5G new radio networks: Prospects and self-interference challenge. in 2019 *53rd Asilomar Conference on Signals, Systems, and Computers*. 2019. IEEE.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed to the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)