engineering proceedings

MDPI

Proceeding Paper

Optimizing the Energy Efficiency in 5G Security Systems for Intrusion Detection with an Emphasis on DDOS Assaults [†]

Umar Danjuma Maiwada [1,*], Kamaluddeen Usman Danyaro [1], Aliza Bt Sarlan [1], Aminu Aminu Muazu [1] and Abubakar Rufai Garba [2]

[1] Department of Computer and Information Science, Universiti Teknologi PETRONAS, Seri Iskandar 32610, Perak, Malaysia; kamaluddeen.usman@utp.edu.my (K.U.D.); aliza_sarlan@utp.edu.my (A.B.S.); aminu.aminu@umyu.edu.ng (A.A.M.)

[2] Department of Computer Science, Faculty of Natural and Applied Science, Umaru Musa Yaradua University Katsina Nigeria, Batagarawa 820102, Nigeria; abubakar.rufai@umyu.edu.ng

[*] Correspondence: umar_21002778@utp.edu.my

[†] Presented at the 4th International Electronic Conference on Applied Sciences, 27 October–10 November 2023; Available online: https://asec2023.sciforum.net/.

Abstract: In response to the rising demand for new and existing use cases of energy efficiency, the telecoms sector is going through a dramatic shift toward 5G technology. High data speeds, extensive coverage provided by dense base station deployment, higher capacity, improved Quality of Service (QoS), and extremely low latency are required for 5G wireless networks. New deployment methods, networking architectures, processing technologies, and storage solutions must be created to satisfy the anticipated service requirements of 5G technologies. These developments further increase the need to secure the security of 5G systems and their functionality as well as energy efficiency problems. Indeed, 5G system security is the target of intense efforts by developers and academics in this industry. Significant security concerns for 5G networks have been identified with extensive research. Attackers can make use of vulnerabilities like traffic and the flow base by introducing malicious code and performing other nefarious deeds to take advantage of the system. On 5G networks, attack techniques such as model node map (MNmap), power depletion assaults, and Man-in-the-Middle (MiTM) assaults can be effectively used. However, this study analyses 5G technology's current energy efficiency problems. We recommend an unusual intrusion detection system (IDS) that makes use of Traffic Volume methods. Considering this investigation, we propose an enhancing training process by including statistical analysis on Distributed Denial-of-Service (DDoS) threats, which is how prior research recommended using OMNET and NS-3 on IDS for optimization. Additionally, the methodology for incorporating the suggested intrusion detection systems within a typical 5G architecture is presented by our research using NETSIM. The paper also offers a planned system's correction method, providing a useful implementation after completing analysis.

Keywords: 5G; security; intrusion detection systems; energy efficiency; NETSIM; DDoS; QoS

check for updates

Citation: Maiwada, U.D.; Danyaro, K.U.; Sarlan, A.B.; Muazu, A.A.; Garba, A.R. Optimizing the Energy Efficiency in 5G Security Systems for Intrusion Detection with an Emphasis on DDOS Assaults. *Eng. Proc.* **2023**, *56*, 324. https://doi.org/10.3390/ASEC2023-15258

Academic Editor: Alessandro Bruno

Published: 26 October 2023

1. Introduction

There is an increasing need to address the energy efficiency and security concerns posed by 5G systems, notably in the context of intrusion detection systems (IDSs), as telecommunications rapidly advance towards 5G technology. Because they can impair service availability and interrupt network operations, Distributed Denial-of-Service (DDoS) attacks have become one of the most serious security risks [1]. The amount of data sent via different wireless technologies, including numerous mobile phones and Internet of Things (IoT) devices, is rapidly increasing, and is impacted by a variety of variables. The telecoms industry is experiencing a change toward 5G technology in response to new and existing use cases [2]. This change is necessary for 5G wireless networks to enable high rates of data and extensive coverage with the deployment of dense base stations, higher capacity, enhanced Quality of Service (QoS), and extremely low latency. As a result, it is crucial to develop new technologies, and 5G is a result of these developments. The development of these technologies poses additional difficulties for the functionality and overall security of 5G networks [3,4]. A greater level of security is required to protect not only the facility but also the security of the community because 5G data networks will be used to connect crucial infrastructures. To provide a more advanced security technique, it is essential to analyze the security concerns related to 5G [5]. The security of 5G systems is the focus of intense efforts by developers and academics in this industry. It is essential to maximize energy economy in 5G security systems with a focus on IDSs to enable effective DDoS prevention while minimizing resource consumption [6]. Effective resource utilization reduces costs and environmental impact while also enabling efficient energy management, which supports sustainable network operations.

Considering the foregoing, the purpose of this study is to investigate methods and approaches for improving energy efficiency in 5G security systems, with a focus on intrusion detection systems (IDSs) in the context of DDoS attacks [7]. We want to create techniques that efficiently identify and mitigate DDoS assaults while optimizing the energy consumption of IDS components by utilizing technological advances and novel approaches.

An in-depth analysis of the existing research on energy-efficient security measures is performed in this study, along with an examination of their applicability to 5G systems. We will also investigate the difficulties posed by DDoS attacks in 5G networks and consider various remedies to increase the energy efficiency with IDSs in defending against such attacks. We seek to contribute to the development of sustainable and resilient network infrastructures that can successfully defend against security threats while minimizing resource utilization by addressing the energy efficiency component of 5G security systems with a focus on DDoS attacks.

The goal of this research is to examine the flaws in 5G cellular networks, which include the traffic in the network and flow base and suggest an intrusion detection system (IDS) based on energy efficiency to defend against pertinent assaults. Although existing methods advocate using OMNET for the IDS technique, this strategy needs to be improved to successfully fend off contemporary assaults. This paper addresses the critical issue of energy efficiency in 5G security systems, with a specific focus on intrusion detection for DDoS assaults. Energy optimization is not only a matter of environmental concern but also a practical necessity, as the efficient operation of security systems directly impacts the sustainability and cost-effectiveness of 5G network infrastructure. By addressing these objectives, this research aims to contribute to the ongoing efforts to secure 5G networks against DDoS assaults while ensuring the sustainability and economic viability of these networks. The findings and recommendations of this study will be invaluable for network operators, security professionals, policymakers, and researchers working to fortify the infrastructure of the 5G era against ever-evolving security threats.

The use of energy effective IDSs in 5G systems has several practical ramifications, including possible advantages for network administrators, service companies, and end users. The directions for future study and development within the area of cost-effective 5G security systems should be highlighted, considering the ongoing development of 5G equipment and new threats.

2. Review of the Related Literature

According to [8], DoS and DDoS attacks are becoming prevalent forms of attack that have a significant negative impact on the integrity of networks and the caliber of internet services. The three strategies that have been offered to prevent DoS (DDoS) assaults are as follows: using router DoS attack mitigation; increasing the trusted platform module; and increasing system defenses. This paper analyses DoS (DDoS) attack mitigation principles and provides a complete study of existing prevention techniques.

According to [9], a network architecture known as a “software-defined network” (SDN) is used to digitally construct and design hardware components. The network connection settings can be changed dynamically. Because the link is fixed in the conventional network, dynamic change is not possible. SDN is a decent strategy, but it is still susceptible to DDoS attacks. A DDoS assault poses a threat to the internet. The method of machine learning can be used to stop DDoS attacks. A Distributed Denial-of-Service (DDoS) assault is when several systems work together to simultaneously target a certain host. In SDN, the infrastructure layer's devices are controlled by software from the control layer, which sits in the middle of both the application and service layers.

According to [2], ICT will be the primary enabler in overcoming this challenge in an extensive number of ways across the complete range of businesses. Energy efficiency is an enormous chance for developed nations as well as developing nations. Power consumption and the resulting energy-related pollution are increasingly important operational and financial challenges, particularly in the telecommunications sector. Energy efficiency will become an increasingly crucial issue for wireless networks in the (near) future due to the exponential growth in traffic on networks and the increasing number of connected devices. More particular, the deployment of 5G coincides with a period in which energy efficiency is perceived as a critical issue for the network's capacity to consider and address societal and environmental challenges.

According to [10], the year 2021, which was much anticipated and is expected to live up to the expectations of fifth-century (5G) wireless technologies, has finally arrived. To address the energy difficulties in the expanding wireless systems, particularly in 5G and beyond, several solutions have been put forth. These solutions have taken into consideration, among other strategies, the development of new network architectures based on the application of cutting-edge radio access technologies known as cloud radio access networks (CRANs), the use of heterogeneous networks strategies, and the implementation of renewable energy (RE) as a substitute for conventional energy sources. Nevertheless, the method for achieving optimal energy efficiency (EE) in 5G networks and beyond is the main emphasis of their research. This approach is based on a new design concept that offers higher system-wide capacity at a low energy cost.

According to [11], the advent of 5G technology has ushered in a new era of connectivity, promising unprecedented speeds and low latency that are poised to transform industries and our daily lives. However, with the proliferation of 5G networks, security challenges have also grown exponentially. Among the most menacing threats are Distributed Denial-of-Service (DDoS) assaults, which can paralyze critical infrastructure, services, and communication networks. These attacks can cause significant financial losses and disrupt essential services, making them a top concern for network operators, service providers, and businesses. Intrusion detection systems (IDSs) play a pivotal role in safeguarding 5G networks against DDoS attacks and other security threats. These systems monitor network traffic, analyze patterns, and detect anomalies, making it possible to respond swiftly and effectively to potential breaches. However, as the complexity and scale of 5G networks continue to expand, there is an urgent need to optimize the energy efficiency of IDSs to ensure they can cope with the demands of this evolving landscape.

The authors of [12] provide a comprehensive overview of the evolving 5G security landscape, highlighting the escalating threats posed by DDoS attacks, and the growing importance of energy-efficient security systems. They explore the existing challenges in optimizing energy efficiency in 5G security systems for intrusion detection, as well as the state-of-the-art approaches and technologies used to address these challenges, and present innovative strategies and techniques that can enhance the energy efficiency of 5G IDSs while maintaining or even improving their detection capabilities. After evaluating the proposed optimization strategies using empirical studies and simulations to measure their impact on energy consumption, detection accuracy, and response time, the authors discuss the practical implications of implementing energy efficient IDSs in 5G networks, including the potential benefits for network operators, service providers, and end-users. Finally, they highlight the avenues for future research and development in the field of energy-efficient 5G security systems, considering the ongoing evolution of 5G technology and emerging threats.

According to [2], research and development efforts are concentrated on a variety of energy efficiency issues in 5G networks. These include the development of energy efficiency measures and standards, network optimization, dynamic sleep modes, eco-friendly communication strategies, energy harvesting, machine learning, and artificial intelligence. The difficulties brought on by network complexity, performance trade-offs, dynamic traffic patterns, power-constrained infrastructure, cost considerations, backward compatibility with existing systems, and standardization are the focus of these research approaches. The development of technologies, algorithms, and network designs is being sped up by continued research and collaboration among industry players, despite the restrictions and difficulties in achieving energy efficiency in 5G systems. It is critical to strike a balance between performance demands and energy efficiency, considering the unique requirements of various applications and settings. We can achieve sustainable and environmentally friendly network deployments, lower operational costs, improve network performance and reliability, and support the expansion of new applications and services made possible by 5G technology by addressing these issues and promoting energy efficiency in 5G systems.

According to [13], significant security concerns for 5G networks have been identified with extensive research. Attackers can make use of vulnerabilities that have been found by introducing malicious code and performing other nefarious deeds to take advantage of the system. On 5G networks, attack techniques such as MNmap, power loss attacks, and Man-in-the-Middle (MiTM) attacks can be efficiently used. This study analyzes 5G technology's current cybersecurity problems. We suggest a novel intrusion detection system (IDS) that makes use of machine learning methods considering this investigation. We propose enhancing the training process by including sizable datasets of Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks in the context of NSL-KDD, which is how prior research recommends using NSL-KDD for IDS training. Additionally, the methodology for incorporating the suggested intrusion detection technologies into a typical 5G architecture is presented in our research. This paper also offers the planned system's pseudo code, providing a useful implementation framework.

3. Methodology

The methodology is designed into sections as seen in Figure 1 below.

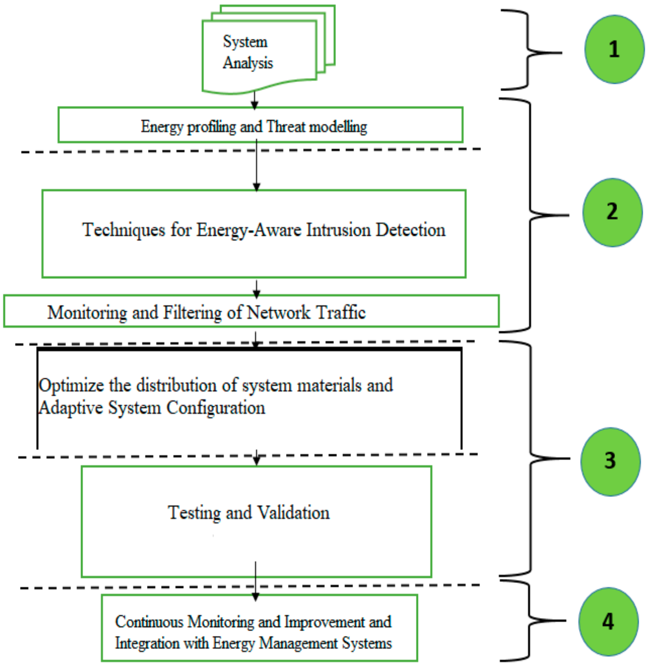
System Analysis
Energy profiling and Threat modelling
Techniques for Energy-Aware Intrusion Detection
Monitoring and Filtering of Network Traffic
Optimize the distribution of system materials and Adaptive System Configuration
Testing and Validation
Continuous Monitoring and Improvement and Integration with Energy Management Systems
1
2
3
4

Figure 1. Methodology flow.

System Analysis: To start, analyze the architecture of the current 5G security system and pinpoint the elements necessary for intrusion detection and DDoS mitigation. Understanding the security system's resource needs, such as those for CPU, memory, and network bandwidth, should be a part of this analysis.

Energy Profiling: Measure and track the specified components' energy usage both during regular operation and DDoS attacks. This profiling aids in locating procedures and components that consume a lot of energy, so they may be targeted for optimization.

Threat Modeling: Carry out a comprehensive threat modeling exercise that is centered on DDoS attacks. Find different attack methods, attack trends, and potential weaknesses in the 5G security system. This investigation will aid in the development of effective intrusion detection methods.

Techniques for Energy-Aware Intrusion Detection: Create or enact energy-efficient intrusion detection methods. To decrease the amount of computational and energy complexity related to detecting DDoS assaults, consider lightweight algorithms and clever filtering techniques. This might entail methods based on machine learning, behavior analysis, or anomaly detection.

Monitoring and Filtering Network Traffic: Put in place effective methods to track and analyze network traffic. Approaches like flow-based evaluation, rate limitation, and traffic classification can be used in this context. Energy usage can be reduced by excluding legitimate traffic and concentrating analytic efforts on potentially harmful traffic.

Next, optimize the distribution of system materials, such as CPU, memory, and bandwidth on the network, based on the risks and attack patterns that have been recognized. To reduce energy consumption, effectively assign energy during normal operation and dynamically assign resources to the most important components during DDoS attacks.

Adaptive System Configuration: Implement adaptive configuration techniques that let the security system change its operating settings in response to the danger level at any given time. This can entail modifying the accuracy of intrusion detection methods, constantly enabling, or disabling specific security modules, or optimizing system behavior based on the current network conditions.

Testing and Validation: Use simulated DDoS assaults and actual network circumstances to thoroughly test and evaluate the optimized security solution. Analyze the system's performance, efficacy, and energy efficiency considering various attacks and network conditions.

$$X = \{(x10, y10), (x50, y50), \ldots, (xn, yn)\}, \tag{1}$$

where n is the number of threats tested.

Continuous Monitoring and Improvement: Implement methods for ongoing evaluation and improvement of the security technique's efficacy and energy efficiency. Gather and evaluate input from real-world deployments and performance measurements to pinpoint areas for system improvement.

Integration with Energy Management Systems: Integrate the improved security mechanism with energy control tools or systems to enable monitoring and management of usage of energy at different points within the 5G network. This connectivity can help with coordinated energy optimization efforts and offer insights into the general use of energy.

4. Experiments

We defined the system architecture: In the simulation environment, we defined the design of the 5G security system. We also described the elements involved in DDoS mitigation and intrusion detection, such as resource management modules, firewalls, intrusion detection systems (IDSs), and traffic analyzers.

We implemented energy models: We created and set up energy models in NETSIM that precisely reflected the properties of the simulated devices and components' energy consumption. We considered the energy profiles discovered using actual measurements and made use of the energy models found in the simulator's library.

We defined DDoS attack scenarios: We identified different DDoS attack scenarios for the 5G network to mimic. We indicated the nature, magnitude, length, and targeted network resources of the attacks. Volumetric, application-layer, and protocol attacks are all possible types of DDoS attacks.

We implemented energy-aware intrusion detection techniques: Inside the simulated security system, we implemented energy-aware intrusion detection techniques. This entailed creating and setting up algorithms for techniques based on machine learning, behavior analysis, and anomaly detection. We made sure that the energy efficiency of these methods was maximized.

We collected metrics: We established metrics for assessing the security system's performance and energy efficiency. Energy use, detection precision, false positives, false negatives, detection duration, and system responsiveness are a few examples of this. We set up NETSIM to gather these metrics while the simulation is running.

We ran experiments: We set the simulation's parameters, such as network traffic, attack scenarios, system setups, and energy-saving tactics. We ran the trials several times while changing the parameters to ensure statistical significance and a full range of outcomes.

We analyzed the findings of Table 1: We examined the metrics gathered and assessed the security system's effectiveness and energy efficiency in various circumstances. We determined the best methods for energy-efficient intrusion detection in the context of DDoS attacks, and we compared the outcomes of various optimization tactics and setups.

Table 1. Different scenarios for the possible attack.

Link_Metrics										
Link ID	**Packet Congested**	**Packet Congested**	**Bytes Traced**	**Payload Traced**	**Overhead Transmitted**	**Packet Congested**	**Packet Congested**	**Bytes Traced**	**Payload Traced**	**Overhead Transmitted**
	data	control				data	control			
All	6	0	21,932,448	20,498,400	1,434,048	6	0	21,932,448	20,498,400	1,434,048
1	2	1	4,007,674	3,671,900	335,774	2	1	4,007,674	3,671,900	335,774
2	0	1	1,547,008	1,462,920	84,088	0	1	1,547,008	1,462,920	84,088
3	0	1	1,544,492	1,461,460	83,032	0	1	1,544,492	1,461,460	83,032
4	0	1	1,545,300	1,460,000	85,300	0	1	1,545,300	1,460,000	85,300
5	1	0	2,333,332	2,206,060	127,272	1	0	2,333,332	2,206,060	127,272
6	5	1	2,330,392	2,197,300	133,092	5	1	2,330,392	2,197,300	133,092
7	0	1	2,321,388	2,195,840	125,548	0	1	2,321,388	2,195,840	125,548
8	1	1	2,319,604	2,192,920	126,684	1	1	2,319,604	2,192,920	126,684
9	1	1	3,983,258	3,650,000	333,258	1	1	3,983,258	3,650,000	333,258

We refined and iterated of Table 2: As necessary, we modified the intrusion detection methods, resource allocation schemes, or system configurations based on the findings and analysis. We continued to refine the experimental procedure to confirm and improve the 5G security system's energy efficiency.

We recorded and reported: We recorded the experimental setup, technique, findings, and conclusions from the NETSIM studies. We prepared a thorough report outlining the energy efficiency effects of optimization strategies for intrusion detection in 5G security systems, with a focus on DDoS attacks in the simulator environment.

Table 2. The results of the attacks.

Attack Type	No. of Attacks	Identified Attacks
Traffic analyzers	100	97
Traffic volume	100	98
Pattern recognition	100	98
Statistical analysis	100	96
Flow based	100	82
Optimization	100	84
Prediction	100	86
Real time	100	76
Overflow	100	91
GUESS_PASSWD	100	99
Behavior	100	62
SPY	100	51
Volumetric	100	78
Protocol	100	60
Application layer	100	75
Spoofing	100	76
Behavior	100	84
Reflection	100	88
Amplification	100	88
Resource management	100	99

5. Results

The innovative IDS focused on 5G threats was welcomed. Consequently, NETSIM software (NetSim Standard13.3.x64) and the DDOS attacks dataset from Kaggle.com were used to set up the system. During the investigation, 5G assaults were discovered. The results of the studies demonstrate how successfully the proposed IDS recognizes DDOS attacks. Compared with related papers, the detection rate is slightly greater. We ran an experiment on the NETSIM simulator, including contemporary DDOS assaults; thus, the outcomes were better. Increasing the effectiveness of the suggested strategy is another goal of ours as we can see from Figure 2. The simulation was conducted using the parameters of throughput, UE, and time series to obtain the best result.

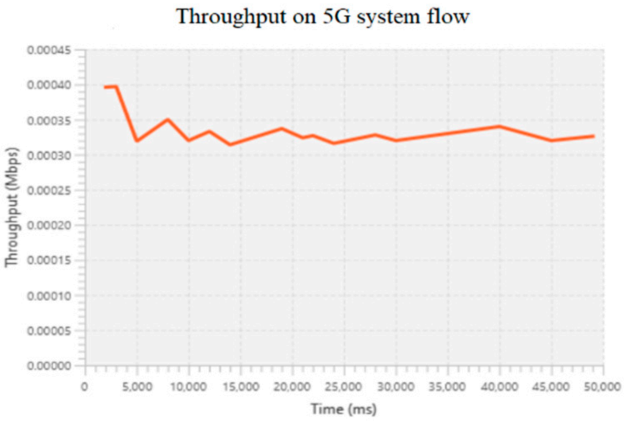

Figure 2. Throughput flow of time 10–50 ms on 5G.

The term "10–50 ms Time Range" designates a window or span of time during which the throughput flow is being gauged. In this instance, it ranges from 10 to 50 milliseconds (ms) from Figure 3. The measurement of throughput is the amount of data transferred within this time and is used to determine the throughput. Bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps) are possible units of measurement.

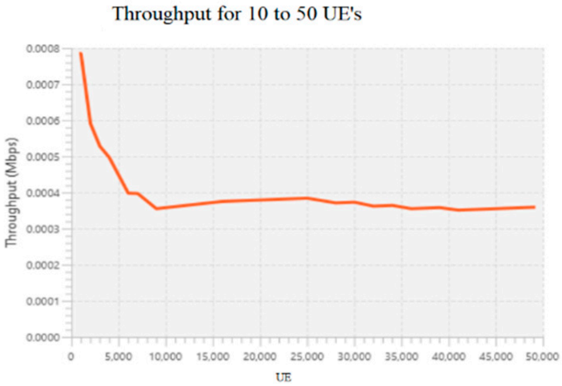

Figure 3. UE's throughputs form 10–50.

Throughput is a parameter that measures how much data the UE can send or receive in a specific length of time. Bits per second (bps), kilobits per second (Kbps), or megabits per second (Mbps) are the most common units of measurement. The time range of 10 to 50 defines a certain period for measuring the UE's throughput. It could stand for seconds (s), milliseconds (ms), or any other type of time unit as seen in Figure 4. This time, it refers to a span of time between 10 and 50 units.

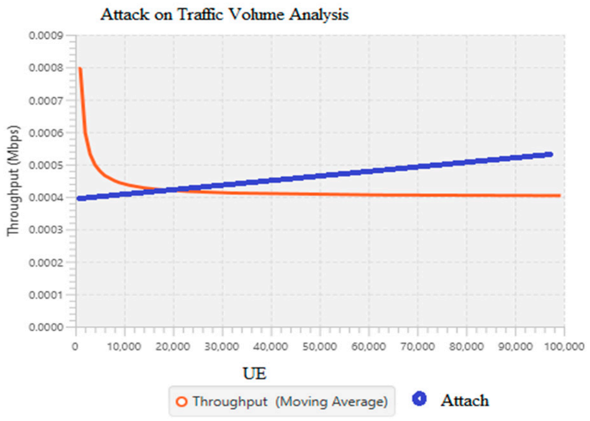

Figure 4. Attack on 5G systems for UE 10-100.

In a 5G network, several factors affect the UE's throughput. These variables include the UE's own capabilities, signal strength, distance from the base station, network congestion, available bandwidth, network load, and signal intensity. The user's experience when gaining access to services and apps is directly impacted by the UE's throughput. Faster data transfer rates due to higher throughput make it possible for seamless streaming of high-quality material as well as more fluid browsing and quicker downloads. Slower data rates might cause delays, buffering, or worse service quality because of lesser throughput. Within the predetermined time frame, the throughput that the UE experiences can change. This variance can be brought on by things like network congestion, signal quality, interference, modulation and coding techniques, and the network circumstances at a given time.

In variable throughput, the throughput flow may change over the stated time of 10 to 100 ms. It can be affected by things like the application or service being utilized, network congestion, channel conditions, modulation, and coding techniques. Regarding dynamics in 5G networks, throughput is dynamic by nature, which means it can change quickly because of many variables. To maximize throughput, the network adapts to changing circumstances and modifies the modulation, coding, and resource allocation. As a result, the network's overall performance is improved, and the radio resources that are available can be used more effectively see Figure 5.

$$\text{UE} = \text{throughput (bit/s)/time (ms)} \tag{2}$$

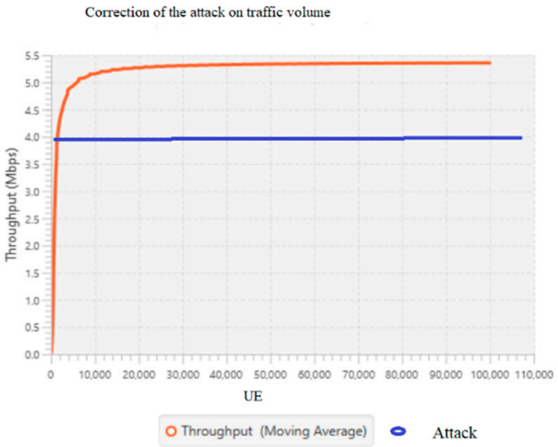

Figure 5. Using time series to correct the attack for UE.

6. Discussion

With an emphasis on DDoS attacks, you may maximize the energy efficiency of a 5G safety precaution using this technology for intrusion detection. It is crucial to remember that the precise implementation details may change depending on the system architecture, hardware, and resource availability.

We should know that depending on the capabilities of the simulator and the requirements of your experiment, the individual stages, and setups within NETSIM may differ. For thorough instructions on how to use the tool efficiently, we refer to the NETSIM instructions and resources offered by the simulator manufacturer.

Network administrators and service providers use a variety of approaches, including carrier aggregation, beamforming, improved modulation schemes, and effective resource management tactics, to optimize traffic flow in 5G networks. Throughput and user experience are eventually improved by these strategies, which help to maximize the available bandwidth, reduce disruption, and enhance overall network performance.

It is crucial to remember that the actual throughput that a UE experiences can change depending on a variety of elements, such as the network implementation, UE capabilities, network conditions, and the kinds of services being requested. For analyzing and improving network performance for improved user experiences, throughput measurements are often gathered by network testing, field trials, or simulation tools.

7. Conclusions and Future Plans

The telecommunications sector is significantly changing in favor of 5G networks, as was already mentioned. The security of the entire telecommunications sector is crucial. It is crucial to have security measures in place to defend the system against 5G network threats. The provided detection system for intrusions will assist in defending against the relevant threats.

The provided IDS provides a high level of protection, yet it still has performance issues. For the 5G network to provide secure services, significant work must be completed. The performance of mobile applications and services operating over the 5G network is directly impacted by the throughput flow. Higher throughput is advantageous for applications with high data demands, including video streaming or huge file downloads. Slower data transfer rates may cause buffering or latency problems because of reduced throughput.

The use of energy effective IDSs in 5G systems has several practical ramifications, including possible advantages for network administrators, service companies, and end users. The directions for future study and development within the area of energy-effective 5G security systems should be highlighted, considering the ongoing development of 5G equipment and new threats. Different optimization approaches are used by 5G networks to increase the UE's throughput. Beamforming, carrier aggregation, adaptive modulation and coding schemes, efficient allocation of resources, and Quality of Service (QoS) mechanisms are a few examples of sophisticated antenna technologies that may be used. In the future, more techniques should be used to improve the performance of other methods.

Author Contributions: Conceptualization, U.D.M.; methodology, U.D.M.; software, U.D.M.; validation, U.D.M., K.U.D. and A.B.S.; formal analysis, U.D.M.; investigation, U.D.M.; resources, U.D.M.; data curation, A.A.M.; writing—original draft preparation, U.D.M.; writing—review and editing, U.D.M.; visualization, A.R.G.; supervision, A.B.S.; project administration, K.U.D.; funding acquisition, K.U.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: There is no data associated with this research, datasets were obtained from Github and Kaggle.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ghali, A.A.; Ahmad, R.; Alhussian, H.S.A. Comparative analysis of DoS and DDoS attacks in Internet of Things environment. In *Artificial Intelligence and Bioinspired Computational Methods: Proceedings of the 9th Computer Science On-Line Conference 2020, Zlin, Czech Republic, 15 July 2020*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 2, pp. 183–194.
2. Chochliouros, I.P.; Kourtis, M.A.; Spiliopoulou, A.S.; Lazaridis, P.; Zaharis, Z.; Zarakovitis, C.; Kourtis, A. Energy efficiency concerns and trends in future 5G network infrastructures. *Energies* **2021**, *14*, 5392. [CrossRef]
3. Aljiznawi, R.A.; Alkhazaali, N.H.; Jabbar, S.Q.; Kadhim, D.J. Quality of service (qos) for 5g networks. *Int. J. Future Comput. Commun.* **2017**, *6*, 27. [CrossRef]
4. Jayaraman, R.; Manickam, B.; Annamalai, S.; Kumar, M.; Mishra, A.; Shrestha, R. Effective Resource Allocation Technique to Improve QoS in 5G Wireless Network. *Electronics* **2023**, *12*, 451. [CrossRef]
5. Khurpade, J.M.; Rao, D.; Sanghavi, P.D. A Survey on IOT and 5G Network. In Proceedings of the 2018 International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, 5 January 2018; IEEE: Piscataway, NJ, USA; pp. 1–3.
6. Sood, K.; Nosouhi, M.R.; Nguyen, D.D.N.; Jiang, F.; Chowdhury, M.; Doss, R. Intrusion Detection Scheme with Dimensionality Reduction in Next Generation Networks. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 965–979. [CrossRef]
7. Ahmad, I.; Shahabuddin, S.; Kumar, T.; Okwuibe, J.; Gurtov, A.; Ylianttila, M. Security for 5G and beyond. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3682–3722. [CrossRef]
8. Ali, T.E.; Chong, Y.-W.; Manickam, S. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. *Appl. Sci.* **2023**, *13*, 3183. [CrossRef]
9. Surekha, M.A.; Induvadana, K.; Krishna, R.C.; Harini, B.; Neeha, B.; Aakash, R. Detection of distributed denial of service attacks in sdn using machine learning techniques. In Proceedings of the 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 27–29 January 2021.
10. Siddiqui, M.U.A.; Qamar, F.; Tayyab, M.; Hindia, M.N.; Nguyen, Q.N.; Hassan, R. Mobility Management Issues and Solutions in 5G-and-Beyond Networks: A Comprehensive Review. *Electronics* **2022**, *11*, 1366. [CrossRef]
11. Ahuja, N.; Singal, G.; Mukhopadhyay, D.; Kumar, N. Automated DDOS attack detection in software defined networking. *J. Netw. Comput. Appl.* **2021**, *187*, 103108. [CrossRef]
12. Al-Quzweeni, A.N.; Lawey, A.Q.; Elgorashi, T.E.; Elmirghani, J.M. Optimized energy aware 5G network function virtualization. *IEEE Access* **2019**, *7*, 44939–44958. [CrossRef]
13. Eliyan, L.F.; Di Pietro, R. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Gener. Comput. Syst.* **2021**, *122*, 149–171. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.