International Research Journal of Human Resource and Social Sciences
ISSN(O): (2349-4085) ISSN(P): (2394-4218)
Impact Factor 6.924 Volume 9, Issue 12, December 2022
Website- www.aarf.asia, **Email** : editoraarf@gmail.com

AI'S CRUCIAL PART IN 5G NETWORK SDN

DEVENDRA KUMAR SOMWANSHI
Research Scholar, TheGlocal University, Saharanpur, Uttar Pradesh

DR. RAKESH KUMAR YADAV
Research Supervisor, TheGlocal University, Saharanpur, Uttar Pradesh

ABSTRACT

This paper proposes a security technique based on the ML algorithm, an adaptive bandwidth mechanism, and a dynamic threshold approach. Therefore, the main focus is on the DDoS attack mitigation approach considered by the ML-trained model used by the SDN controller. The recommended approach employs the most effective ML to locate security measures that boost the protection of the SDN controller and the efficacy of the network. Not only did the use of ML techniques like Extreme Gradient Boosting (XGBoost) increase the accuracy of the security solutions, but it also boosted the performance of the network as a whole. The increasing popularity of multimedia services and the need for superior service quality have prompted a sea change in the way service components like forwarding, control, and management are conceptualized and delivered to end users. Our suggested architecture is put through its paces in terms of latency, reliability, and user satisfaction using the EstiNet simulator. The software-defined unified virtual monitoring function and the Advanced Static Analysis and Transformation Protocol are among the designs simulated and compared to determine how well the proposed design functions. Compared to the alternatives, our proposed architecture has lower average delays (1800 s for 200 IoT devices), higher rates of dependability (90%), and higher levels of customer satisfaction (90%).

Keywords: - Machine learning; Distributed Denial-of-Service; SDN based 5G networks; Security solution; Extreme Gradient Boosting Algorithm (XGBoost)

INTRODUCTION

5G mobile and wireless communication networks have been ignited by the Internet of Things (IoT) and the rapid expansion of mobile video services like YouTube and Mobile TV on smart devices.Since 5G requires higher spectral efficiency than 4G systems, it faces significant challenges from the widespread adoption of bandwidth-intensive mobile applications like live video streaming and online video gaming. Cisco predicts that by 2022, IP video traffic will increase from 2017 levels to make up 82% of all consumer Internet traffic. Globally, by the year

2020, mobile video traffic is expected to account for almost 80% of all mobile data traffic. When compared to traditional media, such as televisions, tablets, smartphones, and M2M modules, VR/AR is projected to enjoy the highest growth rate (82%) between 2017 and 2022.

The projected 8 billion humans on Earth will be outnumbered by the 12.3 billion mobile-connected gadgets by 2022. The rate at which data is generated by 5G networks is expected to be 4.7 times that of 4G networks. There will be hundreds of billions of mobile devices in use before 5G networks are commercially accessible for commercial usage. This is because there are so many more things to do with mobile devices now than just talk. There will be a need for 5G networks in 2020 and beyond with up to a thousand times the capacity of current commercial 4G cellular networks. 5G is expected to have improved, ubiquitous, and increased coverage of almost 100% coverage for "anytime, anywhere" connectivity; 10-100 times higher user data rates; energy savings of above 90%; aggregate service reliability and availability of 99.999%; End-to-End (E2E) over-the-air latency of less than 1 ms; and lower electro-magnetic field levels.

The education and health care industries, as well as e-health and telemedicine, will see a significant increase in their need for a reliable wireless connection by 2020, prompting the creation of 5G. The key drivers of the 5G sector include virtual reality, rich media services like video gaming, 4K/8K/3D video, and applications in smart cities, education, and public safety, and are expected to support a global economic output of $12.3 trillion by 2035. Businesses and academic institutions alike regard 5G as the future network that will enable the specialized demands of many vertical markets. Scientists and engineers from all across the world have been debating and asking issues like,

"a) What exactly is 5G going to look like?as a result of the 5G concept. How can we get to 5G networks and what technologies will make them possible?

(a) What challenges does 5G have to overcome? In software-defined settings that make use of the cloud and other heterogeneous resources.

What kinds of service standards and Experience Level Agreement (ELA)1 can be guaranteed by automated administration of future 5G networks, and to what extent?

(d) How can the driving system-level principles (such as flexibility and programmability) be included across network isolation technologies (SDN, NFV, and MEC) to achieve the aim of 5G network/infrastructure/resource sharing/slicing?

(e) What mechanisms exist for the dynamic and flexible creation of Virtual Networks (VNs) and the underlying 5G infrastructure resource pool? How much will the introduction of new services and technology to accommodate 5G networks shake up the present network architecture? Although 5G's aims are crystal clear, many questions concerning the infrastructure, capabilities, and limitations of the technology necessary to bring them to fruition remain unresolved.

LITERATURE REVIEW

AkramHakiri (2015) To support the large volumes of data created by the new services and apps, the future 5G network will provide the underlying infrastructure allowing billions of more devices with less predictable traffic patterns to join the network. Research into 5G is still in its infancy, thus scientists are exploring many architectural paths to address their major drivers. As possible facilitators for this vision of carrier networks, software-defined networking (SDN) techniques are widely seen as having a central role in the creation of 5G wireless networks. In the future, it will be crucial to have a good handle on this new paradigm in order to tackle the various issues that will occur with SDN-enabled 5G networks. In light of this need, we provide a brief overview of the status of the area and its possible future advances before going into the particular challenges that must be faced.

HichamMagri (2018) To address the challenges of the next generation of 5G mobile networks and to reduce the expenses associated with the exponential growth of data in mobile networks and the launch of new services and applications, mobile operators should provide a range of options. It was concluded that the next generation of 5G mobile networks will benefit greatly from the architectural agility made possible by software-defined networking (SDN). Flexibility, scalability, service-oriented administration, and cost reduction via the isolation of the 5G Core network operations are what drive 5G mo.-bile networks, and these are all areas where Software Defined Networking (SDN) may make a difference. That's why it's so important to learn about the fundamentals of software-defined networking (SDN) architecture and have a look at how it may be used in 5G networks. A literature survey on software-defined networking (SDN) concepts and SDN integration in mobile networks is presented here. The benefits of integrating SDN into 5G mobile networks are outlined, and the advantages of IPv6 over SDN are explored. Finally, we suggest an SDN-based architecture for the 5G mobile network.

B. Sayadi, (2016) 5G NORMA developed a network of functions-based architecture, which is a radical departure from the conventional wisdom of network design, in order to accommodate a broad variety of services and their requirements. This change makes use of multi-tenant networks and the concepts of network slicing, as well as the advantages of new technologies like Software-Defined Networking (SDN) and Network Function Virtualization (NFV). In this paper, we take a deep dive into the concept of Software Defined for Mobile Network Control (SDM-C) networks, dissecting its definition, role in controlling the resources of intra network slices, its unique ability to be QoE aware thanks to the QoE/QoS monitoring and modeling component, and its complementary relationship with the SDM-O orchestration component. To efficiently operate several network slices on the same infrastructure, we create an entity named SDM-X to regulate the allocation of resources and network functions among the network slices. A few examples of actual application are shown and analyzed to demonstrate the energy savings that may be achieved by adopting the proposed design for the network.

Nikita Bhalani (2020) The most promising solutions in this regard are software-defined networks, which separate the network into data and control planes, and network function virtualization, which divides each network element into smaller network functions. This article

discusses the characteristics of a 5G network and provides several use cases for its potential implementation. In this post, we compare and contrast all existing options and present a detailed overview of the current state of research on SDN for 5G. Also discussed are service-oriented 5G network design, as well as software-defined networking and network function virtualization in the 5G core network.

DaifallahAlotaibi (2021) We may use one of three strategies to improve accessibility, depending on the nature of the obstacles we're trying to overcome. To begin, we prioritize the price tiers that make our services more accessible, which is unrelated to the speeds at which they load or the reliability of their connections. Second, delay levels are less important than service availability, which may be unrelated to rate and connection. Finally, the latency and rate may not be directly related to the connection levels being chosen to improve service availability. One possible solution is to use software-defined network (SDN) technology, such as SDN based multiple access, which provides flexible configurations when customers deploy new services and applications. This white paper explores novel slicing algorithms of the system based on software-defined multiple access (SoDeMa) to increase network traffic performance. By simulating this system, we can cut down on the typical response time relative to services, making more capacity for 5G slices available.

METHOD

All conceivable data flows are categorized by SDN into one of three categories, as shown in Figure 1. In order for the detecting modules to monitor traffic patterns, a default threshold has to be defined. These three parts identify DDoS attacks based on traffic volumes and dynamic bandwidth allocation. All three levels of DDoS attacks are detectable by the model. As shown in Figure 1, SDN categorizes all conceivable traffic flows into one of three categories. The threshold has been left at the default value, allowing the detection modules to identify movement patterns. These three pieces identify DDoS attacks via dynamic bandwidth allocation based on network activity. The algorithm is able to detect DDoS attacks in both high and low traffic levels.

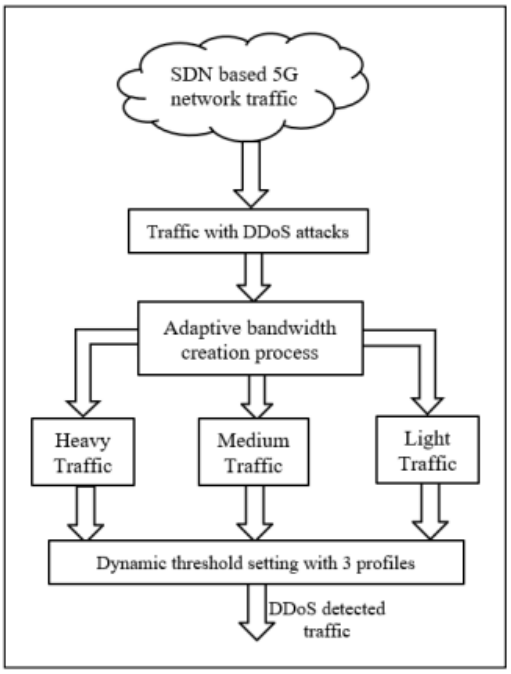

Figure 1: Process of setting the adaptive bandwidth

The proposed method employs bandwidth measurements that change with the character of traffic to identify DDoS attacks. Although bandwidth is proportional to throughput, many applications have varying requirements for available bandwidth. By using the characteristics of the attacked or abnormal traffic, dynamic threshold setting may be utilized to improve DDoS detection efficiency. The fixed threshold limits set the default three profiles, however the dynamic threshold may increase that number.

THRESHOLD SETTING

Based on the kind of traffic and the service being offered by the 5G network, the threshold may be set either manually or dynamically. SDN enables dynamic adjustment of the default threshold, which was established using facts and theory regarding traffic patterns. Parameters such as the detection threshold, machine learning techniques, the trained model, and the applied methodologies greatly affect the success of DDoS attack detection. DDoS attack mitigation might make use of similar detection methods or the workflow of the proposed system. The following three procedures are essential to the process.

- **Monitoring:**Traffic flow, SDN rules, and bandwidth all have thresholds and violation counts set up at this point.

- **Bandwidth controlling:**At this point, malicious DDoS attacks are screened out, and the frequency with which a predefined limit is broken is recorded.

- **Detection:** If the threshold breach is large enough, DDoS attacks may be spotted during the bandwidth-controlling phase.

A dataset and an ML-trained model are needed for traffic classification in order to track and prevent DDoS attacks like those observed in these three steps. The ML-trained model helps with DDoS protection quantitatively because it can more precisely predict the effects of an assault. In order to identify and counteract DDoS attacks effectively, trained SVM algorithms and models are used. In particular, SVM models are used to extract the values of the attributes of the incoming network traffic.

Proposed Theoretical Model

The theoretical model constructed in this study is shown in Figure 2. In this proposed setup, the DDoS attack mitigation method and SDN are made up of the adaptive bandwidth mechanism and the trigger-based learning model based on the Boost algorithm, respectively, and is tasked with protecting the SDN controller. A DDoS security solution for the 5G system built using ML and the XGBoost algorithm is shown in Figure 2. Here, the ML-based security solution helps subpar signal classifiers perform better.

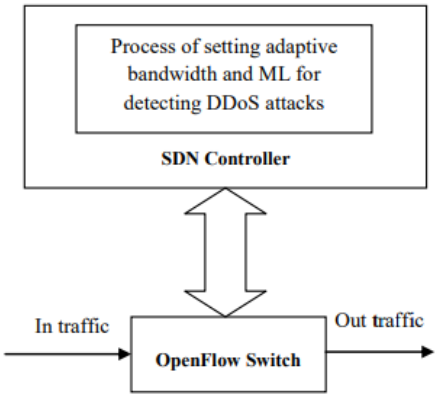

Figure 2: The proposed model with ML and SDN

Autonomous systems based on SDN and 5G networks need robust security solutions in order to progress. The proposed paradigm's capacity to protect SDN-based 5G networks from danger is only one of its many benefits. For instance, programmable traffic monitoring is a domain where SDN and ML perform very well in this system. DDoS attack patterns may be detected more accurately with the use of a programmable SDN controller and a custom-built ML algorithm. Throughout the DDoS detection phase, the ML algorithm monitors the flow's dynamic interactions. These connections symbolize the unpredictable nature of the movement between the two locations. As more and more interactions take place inside these spaces, the time it takes for the flow to occur grows considerably. Machine learning (ML) not only monitors the interactions in each flow, but also provides time estimations when it comes to identifying DDoS attacks.

When applied to SDN-based 5G networks, the proposed method may provide a reliable network security solution by detecting and mitigating DDoS assaults using the SDN controller's ML algorithms.

To begin detecting DDoS attacks and compromised 5G networks or infrastructure, SVMs algorithms are first trained on the dataset. The proposed model uses machine learning (ML) that has been taught using the selected SVM approach to differentiate between normal and abnormal traffic that is influenced by DDoS attacks. Here, the success or failure of discriminating between normal and attacked traffic depends on the accuracy of the SVM algorithm. An SDN controller is keeping an eye on the OpenFlow protocol packets gathered at the connection layer between the northern and southern nodes. SVM algorithms are fed the observed packets to make the distinction between normal network traffic and DDoS attacks. A security solution based on the XGBoost algorithm may help mitigate threats such as distributed denial of service (DDoS) and other service disruption attacks.

RESULTS

Total Time Delay: The total delay for each design is shown in Figure 3. The delay time grows in all designs as the number of devices increases. However, as our proposed SDNFV selects each device's responsibility through the edge node of the framework via NFV, it has less overall latency than the other existing solutions. For the needs of 200 IoT devices, the proposed architecture has a latency of just 1800 s, whereas ASTP and SuVMF have delays of 2500 and 3000 s, respectively.

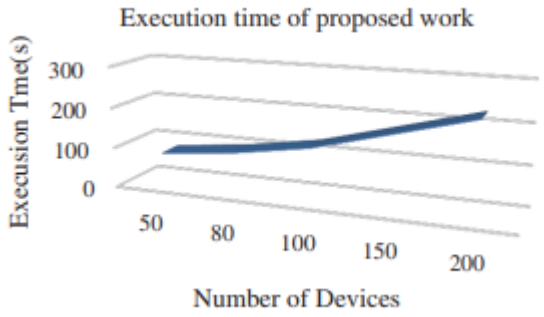

Figure 3: Execution time of the proposed architecture

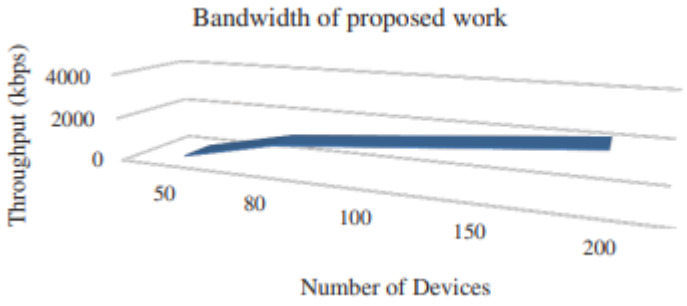

Figure 4: Throughput of the proposed architecture

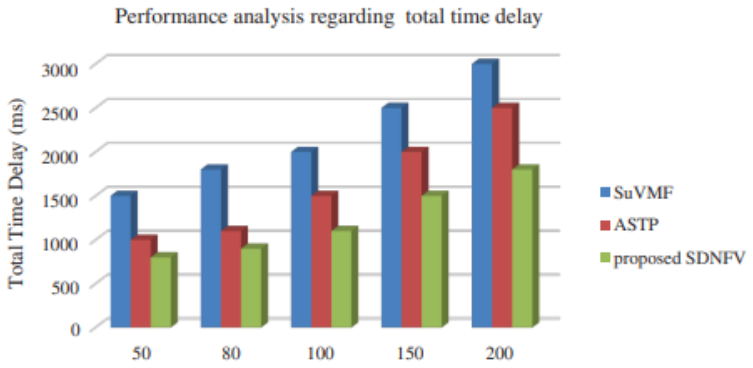

Figure 5: Performance analysis in terms of total time delay

Reliability. This statistic is essential for figuring out how productive an architecture is while doing certain work. When a small fraction of efforts to complete a task fail, the underlying architecture may be relied upon Figure 6 illustrates that as the number of nodes in a network grows, reliability decreases across the board. At the edge nodes where SDN and NFV are implemented, the orchestrator layer is in charge of verifying device requests and enforcing answers through the VNF's forwarding plane. The proposed layout is more trustworthy than its rivals. The suggested approach has a higher reliability (90%) on 200 devices than the other two designs (85%) (ASTP and SuVMF).

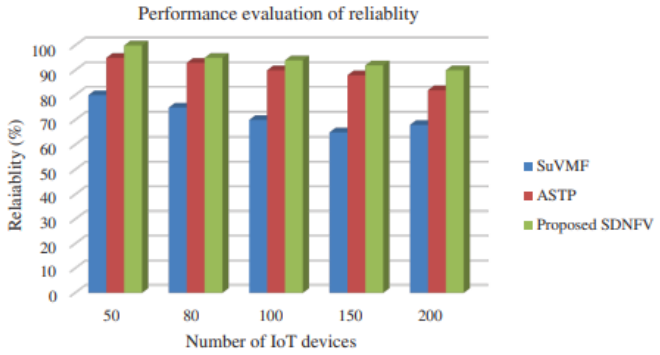

Figure 6: Performance analysis in terms of reliability

Satisfaction. Comprehensive real-time system indexing. The best design is one that responds rapidly to consumer demands and makes them satisfied in the end. As the number of requests for devices increases, it is essential that tasks be completed promptly to maintain high levels of customer satisfaction. Figure 7 depicts the results of a user-satisfaction analysis of the various topologies.

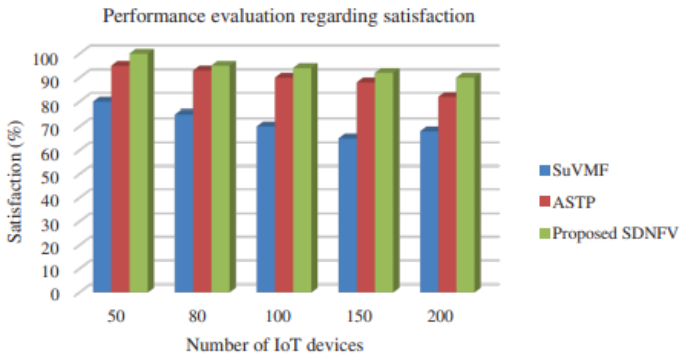

Figure 7: Performance analysis in terms of satisfaction

The proposed SDNFV on edge nodes has garnered the most positive feedback. The proposed architecture is housed in edge nodes close to the IoT devices. The response from the cloud data center to a task request is processed quickly and with minimal latency once the request has been confirmed. The end result is a solution that is both speedy and helpful for the user. We observed that 90% of people are satisfied with our proposed design, whereas ASTP and SuVMF only achieve 82% and 68%, respectively. Overall latency, reliability, and user happiness are all enhanced with our proposed SDN's usage of NFV at the edge nodes.

CONCLUSION

Both the academic and commercial sectors are quickly adopting SDN and NFV as answers to the challenge of resource management and orchestration in 5G networks. Using SDN and NFV will make future 5G networks more adaptable, programmable, and economical. In the future, we want to increase the effectiveness of SDN-based security solutions and defend against DDoS attacks using a dynamic threshold determined by machine learning (ML). In this way, the future generation of 5G+ networks may be protected by security systems that have variable dynamic thresholds. This approach increases the accuracy of security solutions by using ML to combine an adaptive bandwidth algorithm with the goal of reducing the percentage of missed packets. The SDN controller, in combination with NFV VNFs on edge nodes, is responsible for managing API-based rules. Using SDNFV in fog devices enables complicated calculations on massive amounts of data. The success of each emerging technology is threatened by the exponential growth of information. Such a design has the potential to reduce the computational complexity. Throughput, execution time, cost, reliability, and user happiness are all areas where our proposed architecture has been shown to excel in simulation.

REFERENCES

1. Hakiri, Akram&Berthou, Pascal. (2015). Leveraging SDN for the 5G Networks. 10.1002/9781118900253.ch5.
2. Hicham, Magri&Abghour, Noreddine&Ouzzif, Mohammed. (2018). 5G mobile networks based on SDN concepts. 7. 2231-2235. 10.14419/ijet.v7i4.12194.
3. Sayadi, Bessem et al. “SDN for 5G Mobile Networks: NORMA Perspective.” CrownCom (2016).

4. Nikita Bhalani (2020) “A Survey On Software Defined Network With 5g” INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 03, MARCH 2020 ISSN 2277-8616
5. DaifallahAlotaibi, VijeyThayananthan, Javad Yazdani, The 5G network slicing using SDN based technology for managing network traffic, Procedia Computer Science, Volume 194, 2021,Pages 114-121,ISSN 1877-0509,https://doi.org/10.1016/j.procs.2021.10.064.
6. C. proposal, Horizon 2020: The Framework Programme for Research and Innovation, 2012.
7. P. Ameigeiras, J. Ramos-Muñoz, L.Schumacher, J. Prados-Garzon, J.Navarro-Ortiz, J.M. López-Soler “Link-level access cloud archi-tecture design based on SDN for 5G networks” .IEEE Network 2015
8. Van-Giang Nguyen, Truong-Xuan Do, YoungHan Kim “SDN and Virtualization-Based LTE Mobile Network Architectures: A Comprehensive Survey” Volume 86, Issue 3, pp 1401-1438 DOI 10.1007/s11277-015-2997-7 Wireless PersCommun, springer 2016
9. H. Kim, N.Feamster, "Improving network management with soft-ware defined networking”, IEEE Communications Magazine, vol.51, no.2, pp. 114-119, 2013. https://doi.org/10.1109/MCOM.2013.6461195.
10. H. Kim, N.Feamster, "Improving network management with soft-ware defined networking”, IEEE Communications Magazine, vol.51, no.2, pp. 114-119, 2013. https://doi.org/10.1109/MCOM.2013.6461195
11. K.Pentikousis, Y.Wang, and W.Hu “MobileFlow: Toward Soft-ware-Defined Mobile Networks “IEEE Communications Magazine. ISSN: 0163-6804. July 2013
12. Secure and dependable software defined networks, Journal of Network and Computer Applications (2015) –doi: http: //dx.doi.org/10.1016/j.jnca.2015.11.012
13. R. Masoudi, A.Ghaffari, Software defined networks: A survey, Journal of Network and Computer Applications 67 (2016) 1 – 25
14. Van-Giang Nguyen and Younghan Kim “Proposal and evaluationof SDN-based mobile packet core networks “Nguyen and KimEURASIP Journal onWireless Communications and Networking (2015) 2015:172.
15. SBH Said, MR Sama, K Guillouard, L Suciu, G Simon, X Lagrange, J-M Bonnin, in Proceedings of second IEEE International Conference on Cloud Networking (CLOUDNET). New controlplane in 3GPP LTE/EPC architecture for on-demand connectivity service (IEEE, San Francisco, USA, 2013), pp. 205–209