JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ROLE OF ML ALGORITHM IN SDN IN 5G NETWORK

Vinod Kumar Shamrao Jadhav[1], Dr, Vijay Prakash Singh[2]

[1]Research Scholar, Department of Electronics and Communication Engineering, Sri Satya Sai University of Technology and Medical Sciences, Sehore, M.P.

[2]Research Supervisor, Department of Electronics and Communication Engineering, Sri Satya Sai University of Technology and Medical Sciences, Sehore, M.P.

ABSTRACT

In this article, the ML algorithm, an adaptive bandwidth mechanism, and a dynamic threshold approach are proposed as part of a security strategy. Thus, the primary emphasis is placed on the DDoS attack mitigation technique taken into account by the SDN controller's ML-trained model. The best ML is used in the suggested technique to identify security solutions that improve both the safety of the SDN controller and the efficiency of the network. The Extreme Gradient Boosting (XGBoost) and other ML algorithms utilized in this approach not only improved the precision of the security solutions, but also the efficiency of the whole network. A radical shift in the abstraction, separation, and mapping of forwarding, control, and management components of services has been spurred by the rising consumption of multimedia services and the need for high-quality services from clients. With the EstiNet simulator, we test our proposed architecture in terms of latency, reliability, and user satisfaction. To evaluate how well the suggested design performs, it is simulated and then compared to the performance of other architectures, including the software-defined unified virtual monitoring function and the Advanced Static Analysis and Transformation Protocol. Analysis shows that our suggested architecture outperforms the alternatives in terms of overall time delay (1800 s for 200 IoT devices), reliability (90%), and satisfaction (90%).

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

INTRODUCTION

The Internet of Things (IoT) and the meteoric rise of mobile video services like YouTube and Mobile TV on smart devices have sparked international efforts to create 5G mobile and wireless communication networks .The proliferation of bandwidth-intensive mobile applications like live video streaming and online video gaming, as well as the proliferation of smart devices like tablets and smartphones, pose substantial hurdles for 5G since they need better spectral efficiency than that of 4G systems. IP video traffic is expected to account for 82% of all consumers Internet traffic by 2019, up from 75% in 2017, according to the Cisco Visual Networking Index (VNI) Forecast. By 2019, mobile video traffic will dominate, making up about 80% of all mobile data traffic worldwide. From 2017 to 2019, VR/AR traffic is expected to rise at a CAGR of 82%, while TVs, tablets, smartphones, and M2M modules will see growth of 21%, 29%, 49%, and 49%, respectively.

The number of mobile-connected devices is forecast to reach 12.3 billion in 2019, much exceeding the estimated 8 billion people in the planet. It is predicted that 5G networks would produce data at a pace 4.7

times higher than 4G networks. Until 5G networks are widely available for commercial use, the number of mobile devices will likely exceed hundreds of billions. This is due to the proliferation of new uses for mobile devices beyond simple communication. There will be a demand for up to a thousand times the capacity of today's commercial 4G cellular networks in the 5G networks of 2019 and beyond. Compared to LTE, 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 millisecond; and reduced electro-magnetic field levels.

A surge in demand from essential infrastructure systems like e-health and telemedicine, as well as the education sector, to reap the full advantages of wireless connection by 2019 has prompted the development of 5G. Virtual reality, rich media services like video gaming, 4K/8K/3D video, and applications in smart cities, education, and public safety are some of the primary drivers of the 5G industry, which is estimated to facilitate a worldwide economic output of $12.3 trillion by 2035. Vertical sectors have varying needs for network performance and services, and both businesses and universities see 5G as the future network that will allow these niches. Researchers and engineers all across the globe have been discussing, debating, and asking questions such,

"a) What will 5G be?" because of the 5G "theme." What are some of the necessary components of 5G networks and the technologies that might make them possible?

(b) What difficulties does 5G face? In cloud/heterogeneous-native enabled software-defined environments.

(c) how and to what degree can future 5G network management be automated to guarantee that various service criteria and Experience Level Agreement (ELA)1 are met?

(d) How can the goal of 5G network/infrastructure/resource sharing/slicing be realized by incorporating the driving system-level concepts (such as flexibility and programmability) across network ostracization technologies (SDN, NFV, and MEC)?

(e) How can Virtual Networks (VNs) and the underlying 5G infrastructure resource pool be created and managed in a dynamic and flexible manner? To what extent may the current network architecture be disrupted by the introduction of novel services and technologies that can meet the needs of 5G networks? While 5G's goals and objectives are very obvious, many concerns remain unanswered about the technology required to make them a reality, the networks that will support them, and the kind of applications that will be possible.

LITERATURE REVIEW

Akram Hakiri (2015) The future 5G network will offer the underlying infrastructure enabling billions of additional devices with less predictable traffic patterns to join the network, in order to accommodate the massive amounts of data generated by the new services and applications. Since 5G is still in its infancy, researchers are actively investigating various architectural avenues to solve their primary motivators. Software-defined networking (SDN) approaches are expected to play a pivotal role in the development of 5G wireless networks since they are viewed as potential enablers for this vision of carrier networks. In order to solve the many problems that will arise with SDN-enabled 5G networks in the future, it will be vital to have a firm grasp on this new paradigm. With this need in mind, we first review the current state of the field and its potential future developments before delving into the specific difficulties that have to be overcome.

Magri Hicham (2018) Mobile operators should provide a variety of solutions to meet the difficulties of the next generation of 5G mobile networks and to save costs associated with the exponential expansion of data in mobile networks and the introduction of new services and apps. Because of this, software-defined networking (SDN) was recommended as a major technical development that would help the next generation of 5G mobile networks achieve the necessary architectural agility. The major drivers of 5G mo.-bile networks are flexibility, scalability, service-oriented administration, and cost reduction via the ostracization of the 5G Core net-works functions, all of which Software Defined Networking (SDN) stands to improve upon. Therefore, it is crucial to investigate the underpinnings of software-defined networking (SDN) architecture and examine the integration and application possibilities of this technology in the next generation of mobile networks, 5G. This study provides a review of the literature on software-defined networking (SDN) ideas and SDN integration in mobile networks. The advantages of IPv6 over SDN in 5G are discussed, and the benefits of SDN integration in 5G mobile networks are provided. We conclude with a proposal for an SDN-based design for the 5G mobile network.

B. Sayadi, (2016) To create a network that can handle a wide range of services and their needs, 5G NORMA created a network of functions-based architecture, which departs significantly from the established norms of network design. This shift takes use of network slicing and multi-tenancy principles, as well as benefits provided by emerging technologies like as Software-Defined Networking (SDN) and Network Function Virtualization (NFV). In this paper, we examine the Software Defined for Mobile Network Control (SDM-C) network concept in detail, including its definition, its role in controlling the intra network slices' resources, its specificity to be QoE aware thanks to the QoE/QoS monitoring and modeling component, and its complementarity with the orchestration component called SDM-O. An entity called SDM-X is developed to effectively run numerous network slices on the same infrastructure by regulating the distribution of resources and network functions among the network slices that have been formed. Some use cases are shown and examined to illustrate how the suggested architecture improves the network's energy efficiency.

METHOD

Figure 1 demonstrates how SDN classifies all possible data flows into one of three broad groups. The detecting modules are able to observe traffic patterns thanks to the preset default threshold. These three components detect DDoS assaults based on traffic rates with adaptive bandwidth. The model can identify DDoS assaults in all three traffic intensities. In Figure 1, we can see how SDN classifies all possible traffic flows into one of three broad groups. The threshold is at its factory setting, enabling the detection modules to pick up on traffic patterns. These three components detect DDoS assaults with adaptive bandwidth based on the traffic rate. The model can identify DDoS assaults in all traffic conditions, including high, moderate, and low volumes.

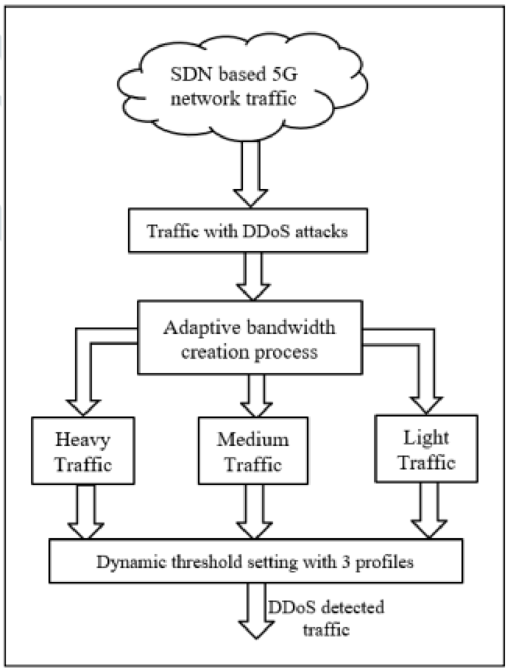
SDN based 5G network traffic
Traffic with DDoS attacks
Adaptive bandwidth creation process
Heavy Traffic
Medium Traffic
Light Traffic
Dynamic threshold setting with 3 profiles
DDoS detected traffic

Figure 1: Process of setting the adaptive bandwidth

To detect DDoS assaults, the suggested approach uses bandwidth measurements that vary with the nature of the traffic. In spite of the fact that bandwidth directly correlates to throughput, different types of traffic need different levels of bandwidth. Dynamic threshold setting may be used to increase DDoS detection efficiencies by differentiating between different types of DDoS assaults based on the characteristics of the attacked or anomalous traffic. The dynamic threshold increases the number of profiles beyond the default three, which are determined by the fixed threshold limits.

THRESHOLD SETTING

The threshold may be adjusted manually or dynamically, depending on the kind of traffic and the service provided by the 5G network. The default threshold was determined using data and theory about traffic flows, however SDN makes it possible to dynamically adjust this value. The effectiveness of DDoS attack detection is very sensitive to the parameters used for the detection threshold, machine learning methods, the trained model, and the applied approaches. Similar detection algorithms, or the workflow of the suggested system, may also be used for DDoS attack mitigation. The next three steps are crucial to the workflow.

- **Monitoring:** At this stage, bandwidth, SDN rules, and traffic flow all have thresholds and violation counters in place.
- **Bandwidth controlling:** In this stage, DDoS assaults are filtered out and the number of times a threshold is exceeded is tallied.
- **Detection:** DDoS assaults may be detected in the bandwidth-controlling phase if the threshold violation exceeds the predetermined threshold limit.

To trace and stop DDoS assaults like the ones discovered in these three stages, a dataset and an ML-trained model are required for traffic categorization. Quantitatively, the ML trained model aids in DDoS mitigation because to its capacity to provide a more accurate estimate of the impact of an attack. Successful DDoS detection and mitigation is aided by trained SVM algorithms and models. Specifically, the values of the properties of the incoming network traffic are extracted using SVM models.

Proposed Theoretical Model

Figure 2 depicts the theoretical model developed in this work. The adaptive bandwidth mechanism and trigger-based learning model based on the Boost algorithm make up the DDoS attack mitigation scheme and SDN in this suggested system, which is responsible for safeguarding the SDN controller. Figure 2 depicts a DDoS security solution for the 5G system that is constructed using ML with the XGBoost algorithm. In this case, the ML-based security solution improves the performance of low-quality signal classifiers.

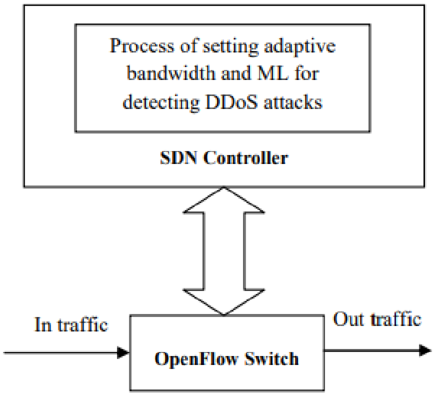
Process of setting adaptive bandwidth and ML for detecting DDoS attacks
SDN Controller
In traffic
OpenFlow Switch
Out traffic

Figure 2: The proposed model with ML and SDN

Successful security solutions are crucial to the development of autonomous systems using SDN and 5G networks. The suggested paradigm has numerous advantages, one of which is its ability to safeguard SDN-based 5G networks from potential threats. SDN and ML perform well in this framework, for example, in the context of programmable traffic monitoring. The combination of a customizable SDN controller and a tailored ML algorithm improves the effectiveness of spotting DDoS assault patterns. The ML algorithm keeps an eye on the dynamic interactions of the flow throughout the DDoS detection process. These couplings stand for the erratic behavior of flow between the two sites. The time it takes for the flow to occur inside these locations increases dramatically as more exchanges take place. When it comes to detecting DDoS assaults, ML not only keeps tabs on the interactions in each flow, but also estimates how long it will take.

The suggested approach is able to offer a dependable network security solution in SDN-based 5G networks by detecting and mitigating DDoS attacks using the SDN controller, which incorporates the ML algorithms.

First, SVMs algorithms are trained on the dataset to identify DDoS assaults and compromised 5G networks or infrastructure. The suggested model relies on machine learning (ML) taught using the chosen SVM technique to distinguish between typical and anomalous traffic that is impacted by DDoS assaults. Here, the efficacy of the SVM algorithm determines the success or failure of differentiating between regular and attacked traffic. The OpenFlow protocol packets collected at the connection layer between the north and south ends are also being monitored by an SDN controller. For the purpose of distinguishing between regular network traffic and DDoS assaults, the observed packets are transmitted to SVM algorithms. Protecting against distributed denial of service (DDoS) and other service interruption threats is made easier by a security solution built on the XGBoost algorithm.

RESULTS

Total Time Delay: Figure 3 shows the overall lag time for each architecture. All architectures have an increase in delay time proportional to the number of devices. Our suggested SDNFV, on the other hand, has less overall latency than the other current designs since it chooses each device's duty via the edge node of the framework through NFV. The suggested architecture has a latency of just 1800 s for the demands of 200 IoT devices, whereas ASTP and SuVMF both have delays of 2500 and 3000 s, respectively.

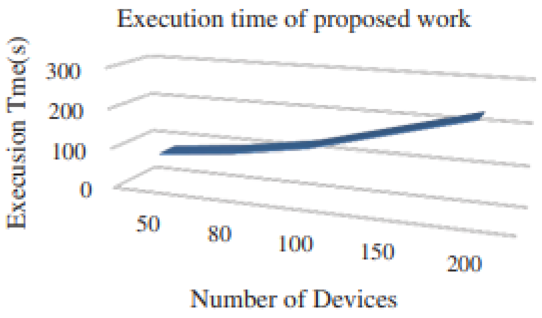

Figure 3: Execution time of the proposed architecture

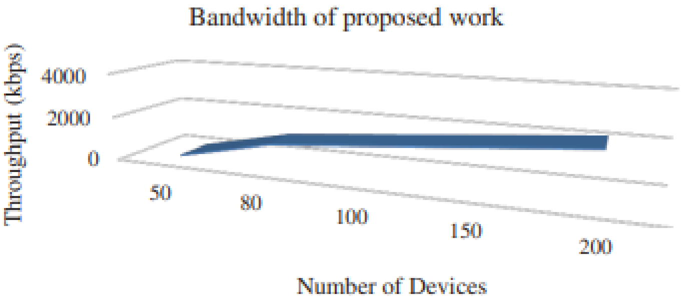

Figure 4: Throughput of the proposed architecture

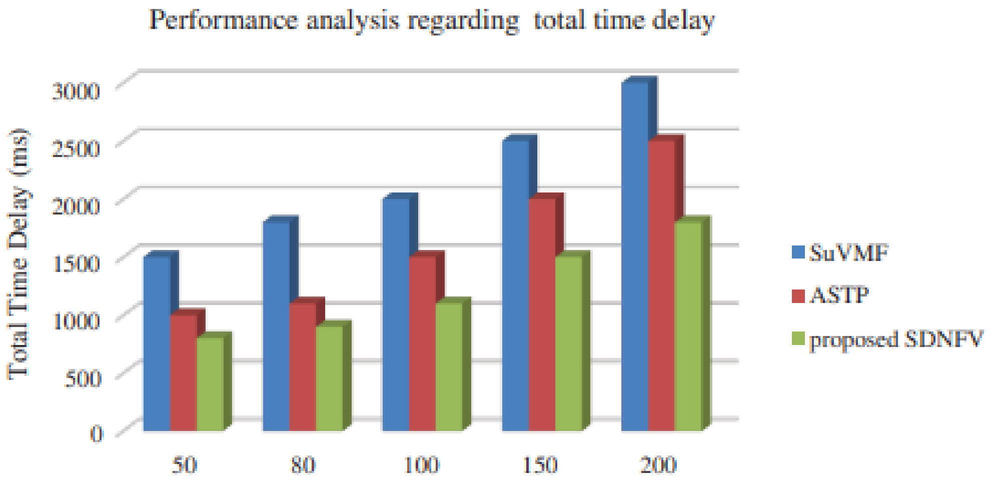

Figure 5: Performance analysis in terms of total time delay

Reliability. This metric is crucial for determining the efficiency of a certain architecture while performing a given activity. When the percentage of attempts to perform a job that fail is low, the dependability of the underlying architecture is high. As can be shown in Fig. 6, the dependability of all topologies falls as the number of devices increases. When implementing SDN with NFV on edge nodes, the orchestrator layer is responsible for validating device requests and implementing responses through the VNF's forwarding plane. The suggested design has more dependability than the alternatives. Reliability on 200 devices is 90% with the proposed design, which is better than the other two architectures (85% with ASTP and 70% with SuVMF).

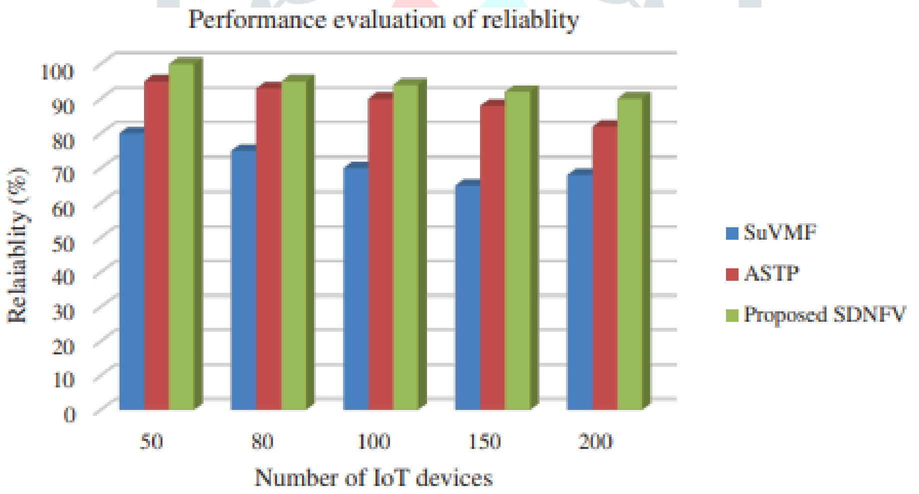

Figure 6: Performance analysis in terms of reliability

Satisfaction. A real-time system index that covers everything. The optimal design is one that is quick to act on requests and leaves the end-user happy. Tasks need to be handled quickly as the number of requests for devices rises; else, user satisfaction will suffer. The user-satisfaction study of the architectures is shown in Fig. 7.

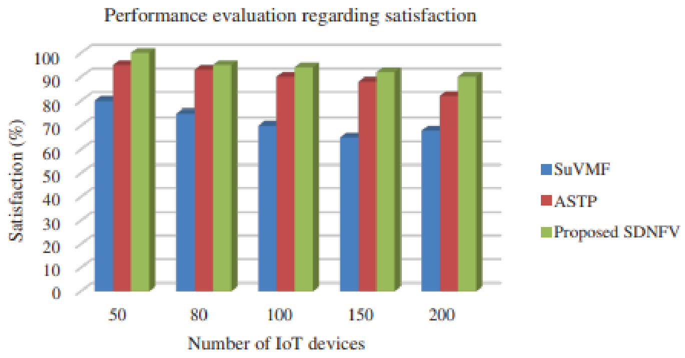

Figure 7: Performance analysis in terms of satisfaction

The suggested SDNFV on edge nodes is the most well-received design. Edge nodes next to IoT devices host the suggested architecture. High execution speed and low latency are achieved when processing the cloud center's answer to a task request, and the request is verified before being handled. As a result, the user will obtain a satisfactory answer as quickly as feasible. We found that our suggested design leads to 90% satisfaction, whereas ASTP and SuVMF only manage 82% and 68%, respectively. In conclusion, our suggested SDN boasts improved performance across the board, from overall time delay to dependability to user satisfaction when using NFV on edge nodes.

CONCLUSION

SDN and NFV are being rapidly adopted by both the academic community and the business sector as solutions to the problem of resource management and orchestration in 5G networks. Future 5G networks will be more flexible, programmable, and cost-effective if SDN and NFV are used. Future efforts will focus on enhancing the efficiency of SDN-based security solutions and protecting against distributed denial-of-service (DDoS) assaults with the help of a dynamic threshold established by machine learning (ML). With this method, security solutions with varied dynamic thresholds will be better equipped to protect the next 5G+ networks. By combining an adaptive bandwidth algorithm with ML, this method improves security solution precision while simultaneously decreasing the proportion of dropped packets. Rules are managed through API, and this is the responsibility of the SDN controller in conjunction with NFV VNFs on edge nodes. Through the use of SDNFV in fog devices, significant data may be calculated with little complexity. The exponential expansion of information has the potential to undermine the success of any developing technology. The computational complexity may be decreased with the aid of such a design. Simulation findings show that our suggested design outperforms the state-of-the-art in terms of throughput, execution time, cost, reliability, and user satisfaction.

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. 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

5. 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 Pers Commun, springer 2016

6. 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.

7. 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

8. K.Pentikousis, Y.Wang, and W.Hu "MobileFlow: Toward Soft-ware-Defined Mobile Networks "IEEE Communications Magazine. ISSN: 0163-6804. July 2013

9. 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

10. R. Masoudi, A. Ghaffari, Software defined networks: A survey, Journal of Network and Computer Applications 67 (2016) 1 – 25

11. Van-Giang Nguyen and Younghan Kim "Proposal and evaluation of SDN-based mobile packet core networks "Nguyen and Kim EURASIP Journal on Wireless Communications and Networking (2015) 2015:172.

12. 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 control plane in 3GPP LTE/EPC architecture for on-demand connectivity service (IEEE, San Francisco, USA, 2013), pp. 205–209