Secure and Reliable 5G Network Slicing in 5G Network using Deep Learning

HM Adnan Zami, Kazi Rafshan Hasin, Jebun Nahar Moni
Department of Electrical and Computer Engineering,
North South University,
Dhaka, Bangladesh.
{hm.zami, kazi.hasin, nahar.moni}@northsouth.edu

Abstract — **Secure and reliable 5G network slicing is becoming an essential concern as the 5G network is being rolled out in the telecommunication industry. The availability of 5G can be used to provide a network as a service (NaaS) for different use cases. Network slicing allows network operators to build multiple virtual networks on a shared infrastructure. However, 5G has strict requirements that need to be addressed, and greater performance power means higher security risk. Mobile operators are on the lookout for solutions that will allow multiple users to be on the same physical infrastructure and reliable end-to-end network resource allocation with Network Slicing. This paper will assess the reliability of a machine learning model for network slicing known as DeepSlice. This model will implement a neural network to manage network load efficiency and network availability and predict the resource demand for a class of users. Another machine learning model, namely Secure 5G, will be assembled with DeepSlice to detect and remove threats based on undesired connection requests detected from data. We analyzed the model performance and evaluated the trends in data that led to the model's decision in slicing the network and maintaining safety. The Secure 5G model has shown noticeable results in removing threats and ensuring end-to-end security from devices to the core network. This model can serve network operators to sell network slicing as a service with high reliability and security.**

Keywords: DeepSlice, 5G Cellular Networks, Network Slicing, DDOS Attack, Deep Learning Neural Networks, Secure Network Slicing, Secure 5G.

I. INTRODUCTION

The world's population has approximately two-thirds of mobile network-connected devices, and the architecture of mobile-connected networks has security vulnerabilities that may significantly affect device users. The next wave of wireless revolution is at the doorstep in the form of the fifth-generation (5G) wireless network [10]. It is expected to handle sizeable mobile data traffic and allow extreme wireless connectivity. It achieves exceptional cost and energy efficiency, which are significant concerns for cellular network operators. The quality of service (QoS) in communication delay, reliability, and security will also leap forward. It is expected that 5G will be a huge technical achievement and inaugurate a new way of thinking in terms of mobile communication style.

A. 5G REQUIREMENTS

The standardization of the 5G wireless system is currently under development. The detailed technical specifications will be made available soon. On the other hand, the industry and academia identified the following technical requirements as essential [10].

Data Rate: The 5G network must uphold the lowest bound for the user-experience data rate at 1 Gb/s (considering anytime and anywhere case) [13].

High-mobility user end channels require more resources for channel state information (CSI) acquisition, resulting in a reduced effective data rate. In essence, the network will have to ensure a certain level of quality of service (QoS) for terminals with mobility even at very high speeds (e.g.500 km/h).

Latency : The latency is the time required to deliver the data demanded to the destination. The end-to-end latency requirement for the 5G network will be 1–5 ms [11], much smaller than that of the current LTE system.

Connected Devices: The 5G network will be required to handle an excessive number of connected devices, almost 100 times more than the current networks. Examples of some new devices will include wearable computing, machine-type communications, wireless sensors, and the Internet of Things [12]. Essential features of these devices, such as data rate and delay, may vary quite dramatically.

Multiple Radio Access Terminals (RATs): The 5G network is not envisioned to replace the existing wireless networks as a whole. Instead, the existing wireless technologies, including GSM, 3G, LTE and LTE-advanced, and Wi-Fi technologies, will continue to evolve and be integrated into a unified system [12].

Energy and Cost Efficiency: 5G wireless technologies must be designed to achieve significantly better cost efficiency (measured in US$/b) and energy efficiency (measured in b/J)[10].

New sources of revenue can be created by reducing operation costs incurred using one core network for different services. Multiple automation features such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Network Slicing in 5G. Moreover, this process increases efficiency and elasticity for scaling new business demands from IoT, Public Safety, Automotive and Healthcare applications. For example, Massive Internet of Things (IoT) devices require high

reliability with limited data rates and low latency for connectivity of smart electric meters and smart city sensors.

Similarly, augmented and virtual reality (AR-VR) programs need high throughput and low latency. Other mission-critical situations like autonomous driving require ultra-reliable low latency and high bandwidth. Because of the network function virtualization, Implementing SDN based architecture can make the system more vulnerable to malicious attacks than the monolithic core architecture. This results in the need for designing a secure system that provides a robust and reliable 5G network. This case is quite sensitive as attacks on the 5G network can have more significant damage due to its high bandwidth and throughput, requiring flexible security architecture for isolated networks optimized for applications with varying needs from a security and privacy perspective.

The main objective of this paper is to implement machine learning algorithms to perform reliable network slicing for 5G networks. One model that succeeded in performing this is DeepSlice. We will observe its performance and evaluate its reliability by inappropriately selecting a network slice for a device, correctly predicting the slice and allocating enough resources to that slice based on the traffic prediction. Moreover, to evaluate the system's security, we will simulate the flow of traffic in networks and implement another machine learning model named Secure5G. This model will analyze patterns in traffic and predict any unusual or malicious flow of traffic. Based on previous data, this model will then terminate the flow of traffic as malicious or safe, which will help identify attackers to try to perform DDoS attacks on the network system. We ensemble these two machine learning models to achieve a reliable and secure network splicing method for 5G networks. Deep learning neural networks are essential tools for accomplishing these goals. To help make the most efficient and optimized selection of network slices for devices and services, this paper makes use of ML and Deep Learning Neural Networks (DLNN).

II. LITERATURE REVIEW

A network configuration that lets numerous networks, independent or virtualized, be created in shared physical infrastructure is network slicing. It is a crucial component of the overall 5G architectural landscape. Every part, or slice, of the network is generally allocated depending on the customer's needs, application or use case.

A. Network Slicing for 5G Networks

For latency, services like smart-parking meters value high reliability and security are acceptable; others (like driverless cars) may need ultra-low latency (URLLC) and high data speeds. The efficient reassignment of resources from one virtual network slice to another, network slicing in 5G, supports these various services and facilitates.

- **Extreme Mobile Broadband (eMBB)** - This mobile network generates high bandwidth and traffic because they are video-centric.
- **Massive Machine-Type Communications** (mMTC). IoT devices fall in this category, with billions of connected devices to the network. Generally, these devices will create less traffic than eMBB applications, but the number of devices will play a prominent role in network traffic.
- **Ultra-reliable Low-Latency Communications** (urLLC) - This classification of network use is standard for things like remote surgery or vehicle-to-X (v2x) communications and requires MNOs to have mobile edge computing capacity in place.

B. Network Slicing using Deep Learning

The nature of 5G makes it crucial for performing fine network slicing and management to ensure efficient network usage. Various techniques for network slicing were introduced that performed well in handling networks. In their paper, S. O. Oladejo and O. E. Falowo discuss the multi-tenancy nature of the 5G network slicing by showing how to transmit power. The number of users affects the capacity of an MVNO. [1] Moreover, SDN and NFV-based 5G core network architecture is defined by L. Ma, X. Wen, L. Wang, Z. Lu and R. Knopp. [2] Furthermore, an application-specific mobile network using an architecture based on deep learning was introduced by Ping and Akihiro to apply application-specific radio spectrum scheduling in the RAN [3]. Another paper introduced a framework that prioritizes network traffic for intelligent cities using a priority management SDN approach. Similarly, Taewhan Kim started work early on network slicing and discussed standardization of network slicing, network slice selection, identifying slice-independent functions and then proposed architecture for slicing and the RRC frame [5]. Furthermore, several network surveys and industry white papers have predicted the growth of mobile devices and 5G network connections and the overall data usage in the coming years.

To perform reliable network slicing using Deep Learning, Thantharate, Anurag and Paropkari, Rahul and Walunj, Vijay & Beard, Cory developed a ‘DeepSlice’ model by implementing Deep Learning (DL). Neural Network manages network load efficiency and availability, utilizing in-network deep learning and prediction.[10] They used specific Key Performance Indicators (KPIs) available to train their model by analyzing incoming traffic and predicting the network slice for an unknown device type. The purpose of this model was to intelligently allocate resources to use the available resources on existing network slices efficiently and offer load balancing. This model has been quite successful at making intelligent decisions and selecting appropriate network slices regardless of network failure. [10]

C. Security Concerns of 5G Network Slicing

Generally, security threats and challenges on the 4G/LTE network today are similar to the threats in the 5G ecosystem. Moreover, 5G networks have strict throughput, latency, and security requirements to meet the service level agreements for diverse applications and services. This is especially true for its diverse ecosystem that may contain millions of IoT devices. In 2019, the F-secure threat report [4] showed that 99.9% of the attack traffic comes from bots or some automation tool. Almost 78% of IoT bot activity represented malware network activity (detection events) across carrier networks. This number has increased to more than triple the rate of 2016 since the introduction of the Mirai botnet, the most significant DDoS attack in history. Mirai was a brute force password guessing attack on open telnet and SSH ports by scanning the internet for open Telnet ports, then attempting to log in default passwords.

Typically in DDoS attacks, the system is flooded by hackers who send vast amounts of opposing traffic, fake ping and connection requests to the targeted network. This makes bandwidth and resources unavailable or busy for regular traffic. For example, a UDP attack makes the host server unresponsive and busy by flooding random ports on a remote host. Moreover, ICMP packets clog the system by continuously attacking ping packets without waiting for replies. Another SYN flood method exploits the

3-way handshake mechanism and does not close the connection after receiving acknowledgement from the server, causing a server bottleneck. Similarly, Ping of Death is another form of attack that sends malicious pings with IP packets more than 65,535 bytes in length. This saturates and overwhelms the site making its resource unavailable for regular traffic.

Here is a list of common 5G threats on networks and devices:

UE/Device	Malware, Virus, Botnets, Firmware Hacks
	IoT Sensors, Rogue Devices, User Information, Device Tamperi
RAN	Rogue Access Points, Denial services for Users
	X2 and S1 Link Compromis
Mobile Edge	DDoS, Sniffing
	Cloud Security, Server Vulnerability
Core Network	Virtual Network Functions
	Control and User plane Malware
Air Interface	Man in the Middle Attack
	Roaming PLMN, Jamming

Table I. Threat Vectors of 5G that are common across Networks and Devices.

III. METHODOLOGY

The utilization of neural networks will develop because the ever-developing gadgets on 5G networks generate big data, and nowadays, neural networks are broadly used withinside the industry. Correct evaluation and choice-making may be overwhelming and require quicker processing times for any individual. To determine which community slice to apply for given entered information. First, we create an ML version and later construct a DLNN. For any new unknown tool kind connecting to the community, the developed `DeepSlice` is then used to manipulate community load, slice failure situations and come across the maximum suitable slice. The DeepSlice uses a convolutional neural community (CNN) classifier, and a statistical ML version is primarily based on the Random Forest (RF) algorithm. RF and CNN are each broadly used fashions in their respective domain names. We use the specific equal dataset for each of our ML and DLNN fashions, together with over 65,000 particular enter combinations.

A. 'Secure 5G' and 'DeepSlice' Deep Learning Neural Network Model Overview

'DeepSlice' model is a machine learning model developed to manage network load, slice failure conditions, and detect the most appropriate slice for any new unknown device type connecting to the network. This ML model was developed using a Random Forest (RF) algorithm. Moreover, this model also uses a convolutional neural network (CNN) classifier. Both RF and CNN are widely used models in their respective domains.

The dataset used for this project includes the most relevant KPIs from both the network and the devices. This data consists of the type of device used to connect (Smartphone, IoT device, URLLC device), User Equipment (UE) category, QoS Class Identifier (QCI), packet delay budget, maximum packet loss, time and day of the week. All KPIs mentioned can be used from the control packets between the UE and network. There are several types of input devices requesting access to this system. Table II shows the types of devices used as the input type. This list includes smartphones, IoT devices, AR-VR devices, Industry 4.0 traffic, e911 or public safety communication, healthcare, smart city or intelligent homes traffic, or even an unknown device requesting access to one or multiple devices services. These include UE category values, and the network also allocates a pre-defined QCI value to each service request.
Moreover, the packet loss rate and packet delay budget are crucial parts of the 5QI (5G QoS Identifier) included in the model. Similarly, Secure5G uses the same input connections, except that it focuses more on identifying the traffic pattern to sniff out attackers. The model also observes time and day of the week to provide a well-informed decision in network slicing.

Input Type	Duration (sec)	Packet Loss Rate	Packet Delay Budget (ms)	Predicted Slice
Smartphone	300	$10^{-2}/10^{-3}/10^{-6}$	60/75/100/150/300	eMBB
IoT Devices	60	10^{-2}	50/300	mMTC
Smart Transportation	60	10^{-6}	10	URLLC
Industry 4.0	180	$10^{-3}/10^{-6}$	10/50	mMTC/URLLC
AR / VR / Gaming	600	10^{-3}	10/50	eMBB
Healthcare	180	10^{-6}	10	URLLC
Public Safety/E911	300	10^{-6}	10	URLLC
Smart City / Home	120	10^{-2}	50/300	mMTC
Unknown Device Type	60/120/180/300	$10^{-2}/10^{-3}/10^{-6}$	10/50/60/75/100/150/300	eMBB/mMTC/URLLC

Table II. Feature highlights of 'Secure 5G' and 'DeepSlice' simulation model

B. Ensemble Learning with Random Forest Algorithm and DLNN

Data that is well-structured and has multiple attributes generally perform well when Random Forest (RF) and DLNN are used. Random Forest is a supervised learning model that is generally used to create predictive models for classification and regression problems. RF is mainly chosen for this problem over other machine learning algorithms because of the dataset's nature and amount of data. There are around 65K unique inputs, among which all the data are well structured. Hence, RF reduces the risk of overfitting by using multiple sub-trees. However, RF is quite effective at swiftly classifying input data into any predefined category for this experiment. For large databases, RF runs efficiently and gives accurate predictions. It can estimate missing data and maintain accuracy regardless of missing input data.

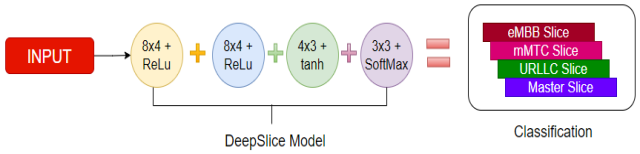


Figure 1: Overview of 'DeepSlice' DLNN Model

Figure 1 shows an overview of the DeepSlice DLNN model. Here, we can see the input goes through 4 layers of the neural network before it is classified into its respective network group. The master slice is the main class that allocates any other 3 group that requires extra bandwidth. The RF model was implemented on top of this as an ensemble method. Generally, ML modelling uses decision trees to predict output with majority voting. According to input data, eight different input strings will combine to provide the model's decision. During the training phase, the RF created several decision trees depending on the inputs, and each branch of the tree represented a possible occurrence or response. The dataset was divided into 70-30. 70% of the input dataset was used to train the model, and the remaining 30% was used to predict the classifier accuracy.

The Deep Learning Neural Network performs well with unstructured data. The same dataset was used to perform training for several neurons of the DLNN. Based on the input from UE, it predicted the correct network slice. This DLNN can accurately give predictions for network slicing, which was used to select the correct slice for unknown device types. This model also assists in redirecting traffic to the Master slice when load balancing is required in the network slices.
Moreover, for network slice failures, it could handle traffic flow well. The given DeepSlice model predicted the network load depending on the incoming connection. Moreover, network slices were tracked to identify the utilization of each network slice. Incoming devices were then allocated to slices by efficiently distributing between the eMBB, URLLC, mMTC or the master slice based on load and output predicted by the DeepSlice DLNN model.

IV. RESULTS AND DISCUSSION

It was observed and concluded that eventually, DeepSlice would be capable of learning and understanding the type of a device and defining the slice to which it belongs. Over time, this system will evolve to handle traffic and devices better by improving its predictions. It will be able to predict future connections requiring a specific service or a network slice. This will be useful in preparing a network for any new connections by efficiently allocating resources in advance. Our results have shown that this system can reliably and securely provide network slicing services that can be applied to 5G networks. This will save any delays later too. RF algorithms can also be improved to add more features to improve the model predicting network slices at given times during the day or night.

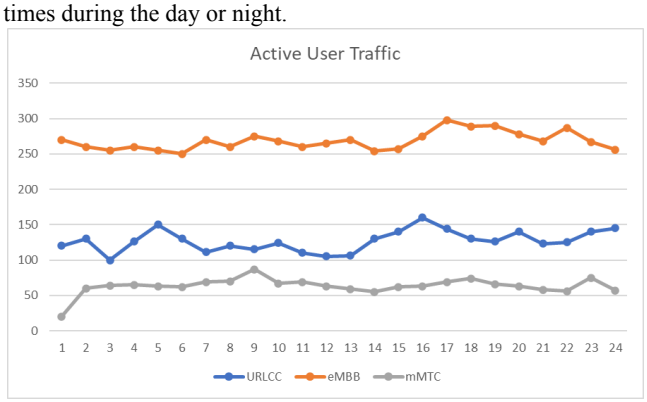


Figure 2: Active users traffic from sample data

A. Evaluating Reliability of 5G Network Slicing

To ensure reliability, the DeepSlice model was verified, and its performance was evaluated to see how it can be used to provide slice prediction, load balancing and network availability:
We checked the validity of the approach by demonstrating how slices are accurately selected for any unknown device types requesting connections to the system.
Load balancing was evaluated to see how efficiently the system utilizes each available network slice. When an individual slice utilization goes beyond the specific threshold of its total available resources, this model directs any new connections to the master slice. This master slice is responsible for carrying devices when a slice utilization exceeds a predefined threshold.
In case of slice failures, the system was observed to provide effective network utilization.
In case of slice failure, all traffic was routed to the master slice instead. This prevented any loss of service during the failure of the slice. DeepSlice was capable of capturing the time of any connection failure and some attributes around the failure. This data can be used in the future to try and isolate the issues and prepare for such situations in advance.

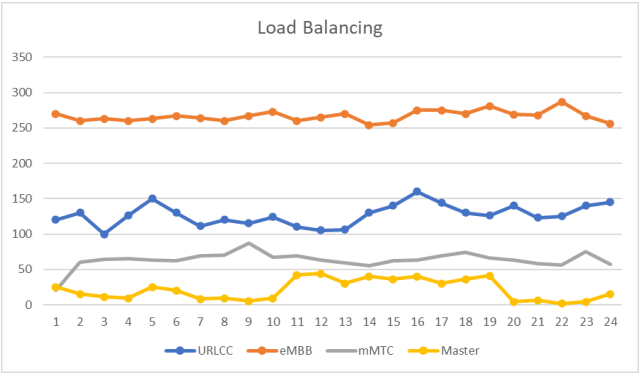


Figure 3: Load Balancing with DeepSlice

B. Protection against DDOS Attacks

To evaluate the security, two scenarios were considered: Volume Based Attack (Flooding) and Masking Botnets. Secure5G has the ability to analyze in-depth various device request patterns and assign optimal slices. This model also showed evolving promises, allowing it to predict future traffic patterns. This can be used for capacity forecasts. A plus side of this is that it can provide insights on unusual network usage related to DDoS attacks. Moreover, it prepares the network for assigning slices to new applications or service requests that the network may not know. Furthermore, it provides a secure system from DDoS attacks or Slice failures.

One of the widespread forms of attack is volume-based attack. In this attack, hackers tend to disrupt normal service flow by flooding the target with a high volume of packets or connection requests. Once this overwhelms the network, servers or bandwidth resources, users tend to get stuck and fail to receive services from the network. After evaluating the Secure 5G model by performing a simulation of this attack, we recorded the results. The attack simulated were making multiple connection requests to the network simultaneously. Secure5G model succeeded in detecting this malicious traffic and blocked it before reaching the cote network.

Moreover, the Secure5G model continued to analyze and identify incoming connections or traffic patterns. This knowledge helps it identify an attacker's device and monitor its behaviour. Once it detects suspicious behaviour that tends to flood the network, it will ultimately deny any more service by the network. After being detected, all of the attacker's traffic will be moved to the black hole route, and this device will be marked as a possible threat to

the database. However, any device that initially attaches can request to make an immediate connection request to a different slice. Despite security issues, it is not adequate to deny any genuine user or an original connection request to be flagged as a suspicious user because they make multiple requests divided by a short time interval.
For this reason, a specific expiry timer has been assigned to each incoming request to avoid false flagging. Secure5G model will only flag this as a threat if the device makes multiple requests to different slices after the timer has expired. There is a customization option for the timer expiry set to 5 seconds in this simulation. However, network operators can choose to define their threshold based on slice requirements.

The robustness of Secure5G was evaluated by simulating a spoofing attack scenario by hackers. This works because a device or client masking is an impersonation of a user where the attacker disguises the source of an attack. It then allows the infected traffic to appear legitimate. Generally, hackers spoof DNS servers and IP addresses for spreading the virus. Botnets are malware that infects devices that an attacker uses to generate massive traffic to consume the server capacity, multiple network connection requests to flood the system resulting in server downtime, and in most scenarios, even without their owners' knowledge.

V. CONCLUSION

This paper assessed the effectiveness of the DeepSlice and Secure 5G algorithm to perform reliable and secure network slicing for 5G networks. Both of these models were presented previously and showed promising results. In this paper, an ensemble technique was used to observe the performance of both models. The framework introduced in this paper accounted for security concerns in the 5G network to produce a deep learning neural network model that was robust at performing a Network Slicing framework to combat DDoS attacks. This was done by filtering malicious UE connections to the 5G network.
Moreover, spoofing attacks and volume-based flooding were studied to evaluate the overall performance. Detection accuracy for this model reached more than 98% with this limited dataset. Results from this experiment process that Secure5G implementation with DeepSlice will ensure the end-to-end security of the 5G network.

References

[1] S. O. Oladejo and O. E. Falowo, "5G network slicing: A multi-tenancy scenario," 2017 Global Wireless Summit (GWS), Cape Town, 2017, pp.88-92.

[2] L. Ma, X. Wen, L. Wang, Z. Lu and R. Knopp, "An SDN/NFV based framework for management and deployment of service based 5G core network," in Oct 2018 China Communications, vol. 15, no. 10, pp. 86-98.

[3] P. Du and A. Nakao, "Deep Learning-based Application Specific RAN Slicing for Mobile Networks," 2018 IEEE 7th International Conference on Cloud Networking (CloudNet), Tokyo, 2018, pp. 1-3.

[4] R. Abhishek, S. Zhao and D. Medhi, "SPArTaCuS: Service priority adaptiveness for emergency traffic in smart cities using software-defined networking," 2016 IEEE International Smart Cities Conference (ISC2), Trento, 2016, pp. 1-4.

[5] T. Yoo, "Network slicing architecture for 5G network," 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2016, pp. 1010-1014.

[6] R. A. Paropkari, A. A. Gebremichail and C. Beard, "Fractional Packet Duplication and Fade Duration Outage Probability Analysis for Handover Enhancement in 5G Cellular Networks," 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 2019, pp. 298-302.

[7] F. Kurtz, C. Bektas, N. Dorsch and C. Wietfeld, "Network Slicing for Critical Communications in Shared 5G Infrastructures - An Empirical Evaluation," 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), Montreal, QC, 2018, pp. 393-399.

[8] R. A. Paropkari, C. Beard, A. V. De Liefvoort, "Handover performance prioritization for public safety and emergency networks," 2017 IEEE 38th Sarnoff Symposium, Newark, NJ, USA, 2017, pp. 1-6.

[9] Thantharate, Anurag & Paropkari, Rahul & Walunj, Vijay & Beard, Cory & Kankariya, Poonam. (2020). Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond. 0852-0857. 10.1109/CCWC47524.2020.9031158. 5G: A Technology Vision, Dec. 2013. [Online]. Available: http://www.huawei.com/5gwhitepaper/

[10] Thantharate, Anurag & Paropkari, Rahul & Walunj, Vijay & Beard, Cory. (2019). DeepSlice: A Deep Learning Approach towards an Efficient and Reliable Network Slicing in 5G Networks. 10.1109/UEMCON47517.2019.8993066.

[11] E. Hossain, M. Rasti, H. Tabassum, and A. Abdelnasser, "Evolution towards 5G multi-tier cellular wireless networks: An interference management perspective". IEEE Wireless Commun. Mag., vol. 21, no. 3,pp. 118–127, June 2014