SliceSecure: Impact and Detection of DoS/DDoS Attacks on 5G Network Slices

Md Sajid Khan*, Behnam Farzaneh*, Nashid Shahriar*, Niloy Saha†, Raouf Boutaba†
*Department of Computer Science, †David R. Cheriton School of Computer Science
*University of Regina, Canada, †University of Waterloo, Canada
{mkc829, behnamfarzaneh, nashid.shahriar}@uregina.ca, {niloy.saha, rboutaba}@uwaterloo.ca

***Abstract*—5G Network slicing is one of the key enabling technologies that offer dedicated logical resources to different applications on the same physical network. However, a Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack can severely damage the performance and functionality of network slices. Furthermore, recent DoS/DDoS attack detection techniques are based on the available data sets which are collected from simulated 5G networks rather than from 5G network slices. In this paper, we first show how DoS/DDoS attacks on network slices can impact slice users' performance metrics such as bandwidth and latency. Then, we present a novel DoS/DDoS attack dataset collected from a simulated 5G network slicing test bed. Finally, we showed a deep-learning-based bidirectional LSTM (Long Short Term Memory) model, namely, SliceSecure can detect DoS/DDoS attacks with an accuracy of 99.99% on the newly created data sets for 5G network slices.**

***Index Terms*—DoS, DDoS, 5G Network Slicing, Deep Learning, Bidirectional LSTM.**

I. Introduction

Network slicing, now an important part of 3GPP Release 16, is a core component of the 5G mobile network architecture. One of the motivating factors behind the introduction of slicing is the ability to support wide-variety of applications with heterogeneous Quality of Service (QoS) requirements using the same physical infrastructure.

Network slicing security threats are common concerns that can be divided into life-cycle security, intra-slice security, and inter-slice security [1]. The 5G communication system elements including User Equipment (UEs), access networks, and core networks are all vulnerable to security attacks. In a 5G network slicing environment, many access and core network functions (e.g., User Plane Function (UPF)) are expected to be virtualized on the same physical resources, thus increasing the attack surface. For example, a UE compromised with malware can send a large amount of DoS traffic targeting a virtualized UPF function. In worst cases, multiple compromised UEs can form a botnet to execute DDoS attacks against a UPF by manipulating a group of linked UEs [2]. Such attacks can impact the performance of uncompromised UEs using the same or different slice that share the attacked UPF. However, to the best of our knowledge, there is no study that analyzes performance impact in a network slicing environment. To fill this gap, this paper presents a study to show the impact of DDoS attacks on slice users' performance metrics such as bandwidth and latency.

Many data sets including CICDoS, CICIDS2017, CSE-CICIDS2018 [3], and CIC-DDoS2019 [4] are available for DoS/DDoS attacks. To the best of our knowledge, there is no available data set specially for DoS/DDoS attacks in 5G network slices. For this purpose, we generated a new dataset for benign traffic and DoS/DDoS attacks traffic with the simulated 5G network slices and made it publicly available. Then, we implemented a deep learning based SliceSecure model to detect DoS/DDoS attacks in our dataset using a Bidirectional Long Short-Term Memory (LSTM) network [5]. Once an attack is detected, the compromised UE can be moved to a sinkhole slice to mitigate the impact of the attack [6]. This also shows the benefit of network slicing where some attacks can be contained within a network slice without impacting co-existing slices.

The main contributions of this paper are as follows:

- We simulated a 5G network slice testbed using Free5GC [1] and UERANSIM [2] and showed the impact of DoS/DDoS attacks on performances of 5G network slices.
- We generated novel data sets for benign traffic and DDoS attack traffic using the 5G network slice testbed.
- Then, we extracted relevant features from .pcap file to .csv file and implemented the **SliceSecure** model.
- Lastly, we evaluated the SliceSecure model to detect DDoS attacks using the newly generated dataset.

The rest of the paper is organized as follows: Section II discusses the related works, Section III elaborates on the impact of DoS/DDoS attack, Section IV discusses detection technique, Section V shows the results and comparison, and lastly, Section VI concludes the paper.

II. Related Work

The majority of previous work have used statistical, machine learning, and cryptography-based methods for identifying DDoS attacks in different networks. A combination of volume-based detection techniques and entropy methods are discussed by the authors in [7] to mitigate DDoS attacks. Entropy-based approach to defending against DDoS attacks in Software Defined Networking (SDN) is discussed in [8].

Several recent work have focused on addressing DDoS attacks in 5G and beyond mobile networks. For example,

[1] "free5GC." https://www.free5gc.org/ (accessed May 27, 2022)

[2] "aligungr/UERANSIM", https://github.com/aligungr/UERANSIM/ (accessed May 27, 2022)

the authors in [9] described a mathematical model based on slice isolation to mitigate DDoS attacks in 5G network slicing. The work in [10] demonstrates how volume and botnet based DDoS attack can be performed in 5G network slices. In [11], the authors suggested a method for detecting DDoS attacks in 5G networks based on the bidirectional LSTM model. In [12], the authors introduced DeepSecure model, a deep learning framework, to detect and mitigate DDoS attacks using existing datasets. A 5G prototype is demonstrated in [6] to mitigate DDoS attack by moving malicious UEs to a sinkhole-type quarantined slice. However, existing works, unlike this paper, neither analyze the impact of DDoS attacks on slice performance nor consider attack data sets collected from network slices.

III. Impact of DoS/DDoS Attack

This section provides an overview of components deployed in the 5G testbed for network slicing. The main components are as follows:

Virtual Machine (VM): All the network functions used in this document are deployed as virtual machines with different Internet Protocols (IPs).

Server: We used two VMs as servers in this paper. One server is used for measuring performance and another server is used to do DDoS attacks from UEs.

Mobile Core: To implement 5G mobile core networks, Free5GC is used. The 5G core network (5GC) defined in 3GPP Release 15 (R15) and beyond can be implemented using Free5GC which includes : Core Access and Mobility Management Function (AMF), NF Repository Function (NRF), Session Management function (SMF), and UPF.

RAN Emulation: It is used to simulate 5G network UE and RAN (gNodeB). In basic terms, it is used as a 5G mobile phone and a base station.

5G allows UEs to access several slices simultaneously, but only one AMF will be used for all slices. In our paper, we considered four experiment phases as follows: (1) Network slice implementation. (2) Network slice performance measuring before DDoS attacks. (3) Doing DDoS attacks in server2. (4) Network slice performance measuring after DDoS attacks.

The experimental setup for 5G network slicing is displayed in Fig 1 that consists of two network slices called slice1 and slice2. To experiment with DDoS attacks in network slicing, we implement network slicing using 12 VMs. For each VM, RAM is 2048 MB and two processors are used. We used Ubuntu 20.04.3 LTS (5.4.0-104-generic) operating system, Free5GC version v3.0.5, and UERANSIM version v3.1.0. The 5G network core function is deployed in 5GC VM, and User Plane Functions (UPF1 and UPF2) are deployed in UPF1 VM, and UPF2 VM consecutively. In addition, we used two servers, including server1 for measuring performance and server2 to do DDoS attacks. The main idea behind is to overload UPF1 with lots of attack traffic destined for server2 and show the performance. Furthermore, UEs (UE1-UE6) are deployed in six different VMs. Lastly, gNB is deployed in gNB1 VM. To simulate all UEs and gNB, UERANSIM is

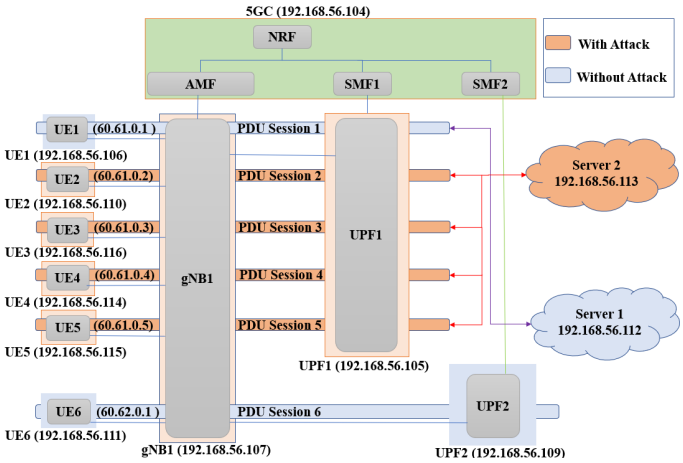

Fig. 1. The experimental setup for 5G Network Slicing

used. The UE1-UE5 are connected to slice1 via UPF1, and UE6 is connected to slice2 via UPF2. First, we measure the performance from UE1 to server1. That is the normal performance measurement before the DDoS attack. Then, we will conduct the DDoS attack from UE2-UE5 to server2 using UPF1, and simultaneously, we measure the performance during the DDoS attack from UE1 to server1.

A. Experiments Scenarios

We implemented two 5G network slices which are connected to Network1 (IP= 60.61.0.0/16) and Network2 (IP= 60.62.0.0/16). We connected five UEs (UE1-UE5) to UPF1 which has five Protocol Data Unit (PDU) sessions named PDU Session1 to PDU Session5, respectively. Then, UE6 is connected with UPF2 using PDU Session6. We performed DDoS attack scenarios using hping3 from UE2 to Server2 using two parameters namely i and d where i is the interval between sending each packet in microseconds and d refers to packet body size in bytes. Furthermore, the network performance in terms of bandwidth and latency is measured using qperf tool in the 5G network slice from UE1 to server1. On server1, qperf runs without arguments. On the other hand, on a client, we run qperf to obtain measurements in terms of bandwidth and latency.

To calculate the results for different scenarios, each scenario is repeated 5 times, and after 5 repetitions, the average results are taken.

Scenario-I: First, we measure performance from UE1 to server1 in terms of bandwidth and latency for the normal state of the network. The average values in the normal state for bandwidth and latency are 50.5 MB/sec and 178 microseconds, respectively.

Scenario-II: In Fig 2, we demonstrate the DDoS attack from UE2-UE5 to server2 and measure the performance between UE1 and server1. We considered increasing the interval (i) between sending each packet with various packet sizes (d). Fig 2 shows that by sending more DDoS packets (by decreasing intervals between DDoS packets from 600 to 150 microseconds and using varying packet sizes in the same range), the bandwidth between UE1 to server1 is decreased substantially, and the corresponding latency has increased.

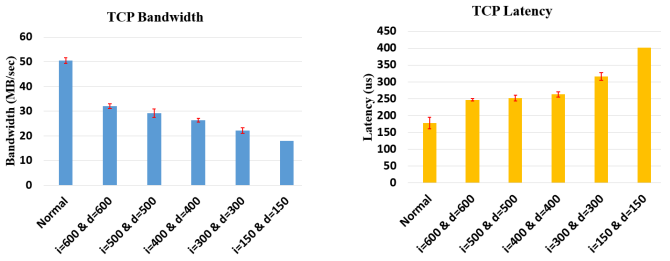

Fig. 2. TCP Bandwidth and Latency after attack with i (interval time) in range of 150 to 600 microseconds and d (packet size) in range of 150 to 600 bytes

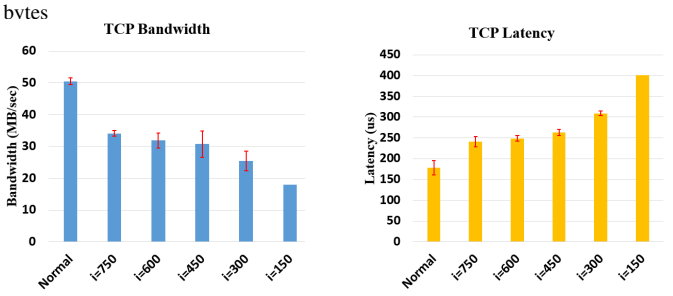

Fig. 3. TCP Bandwidth and Latency after attack with i in range of 150 to 750 microseconds and fixed d=150 bytes

Scenario-III: In this scenario, the performance is measured from UE1 to server1 while the attack is going on between UE2-UE5 to server2. We assigned a fixed packet size of 150 bytes and varied the interval between sending the packet in the range of 150 to 750 microseconds. In Fig 3, the result shows that the bandwidth is decreasing and latency is increasing as we increase DDoS attack traffic by reducing interval i.

IV. DoS/DDoS Attack Detection using SliceSecure

A. Creating Data sets

Publicly available datasets for DDoS attacks are CICDoS, CICIDS2017, CSECICIDS2018 [3], and CIC-DDoS2019 [4] which are not for 5G network slices. That's why we have implemented 5G network slices using Free5GC and UERANSIM simulator to create our new data sets. After implementing the 5G network slices, we send different types of traffic mentioned in Table I. We send benign traffic in both slice1(between UE1-UE5 and server1 via UPF1) and slice2(between UE6 and server1 via UPF2).Lastly, We used hping3 tool to generate DoS/DDoS attacks as shown in Table I. We captured the .pcap file using Wireshark [13] and made those publicly accessible for researchers and industry[3].

TABLE I
List of experiment traffic that sends through network slices

Serial	Benign Traffic	Dos/DDoS Traffic
1	ICMP ping	UDP flooding
2	ACK scan	TCP sync attack
3	UDP scan	TCP push
4	Collecting Initial Sequence Number	TCP fin
5	Firewalls and Time Stamps	TCP srt
6	SYN scan	
7	FIN, PUSH AND URG scan	
8	Determine number of pings	
9	Copy files between UEs and server	
10	Sending emails between user and server	

[3]https://gitlab.com/sajidkhan382067/ddos-data-sets-2022

B. Extracting Features from data sets

We converted the .pcap files into a .csv that consists of 84 features of the traffic using CICFlowMeter [14]. We used 11 features (Flow duration, Destination IP, Destination Port, Fwd Packet Length Std, Source IP, Source Port, ACK Flag Count, Protocol, Total Fwd Packet, MinSegSizeForward, and Slice) following the paper [4] except the feature called "Slice" which we inserted for slice.

C. Detection and Evaluation

Our proposed SliceSecure model is a bidirectional long-term memory network - commonly referred to as "LSTM" - which is a special type of Recurrent Neural Network (RNN) based on deep learning and efficient enough to learn the long-term dependencies. It was developed by Hochreiter and Schmidhuber (1997) and has been improved and familiarized by many people. It has been developed explicitly to skip the problem of long-term dependency. Memorizing information for a long time is their normal behavior, not something they struggle to learn. All cyclic neural networks take the form of a sequence of repeating modules of the neural network. In standard RNNs, this iterative module will have a very simple structure, such as a 'tanh' layer [15]. We used the Bidirectional LSTM model to detect DoS/DDoS attacks with the previously mentioned 11 features from the collected data sets. In our first evaluation, we used 20000 rows benign and attack traffic from the newly created data sets. In another evaluation, we combine 20000 rows of benign traffic with varying number of attack traffic(between 4000 to 20000 rows). In both evaluations, we split the whole dataset into 80/20 manner for training and testing purposes. Our activation function is 'tanh' and epochs = 40. We evaluated our model based on well-known metrics including Accuracy, Precision, Recall, F1 Score, Mean Squared Error (MSE) and Area under the curve of ROC (AUC) [16], [8].

V. Result and Discussion

Our proposed SliceSecure model can detect attack with an Accuracy of 99.99% for new data sets as shown in TABLE II. Its Recall is 99.98%, Precision 99.99%, F1 score 99.99%, MSE is 0.000123, and AUC is 99.99%. Our approach converges within 40 epochs, unlike the DeepSecure [12] model.

In Fig 4, Epoch versus Accuracy graph is plotted for training and validation. The test accuracy and the validation accuracy are more than 99% from the first epoch of the experiment. In some of the epochs, there are some fluctuations. As the accuracy in every epoch is more than 0.99, the value of the fluctuations is not so high in terms of the values. Other than that, most of the time the graph is stable.

In Fig 5, Epoch versus Loss graph is plotted. The loss in training and validation time is quite linear. But, some of the time there are a few differences that can be negligible. We used this Bidirectional LSTM model because in [11], the authors used a Bidirectional LSTM model with an accuracy of about 97.99%, and in [12], the authors used the LSTM model with

TABLE II
COMPARISON OF VARIOUS METRICS OF VARIOUS DETECTION MODELS

Model Name	Data set Used	Number of Epochs	Accuracy (%)	AUC (%)	Precision (%)	Recall (%)	F1 Score (%)
DeepDefence [11]	ISCX2012 [17]	40	97.99	99.28	98.10	97.88	97.99
DeepSecure [12]	CICDDoS 2019 [4]	100	99.97	99.85	99.95	99.98	99.97
SliceSecure	Our data set	40	99.99	99.99	99.99	99.98	99.99

TABLE III
IMPACT ON ACCURACY WITH THE INCREASE OF ATTACK TRAFFIC

Attack Traffic(%)	20%	40%	60%	80%	100%
Accuracy(%)	99.87%	99.91%	99.97%	99.99%	99.99%

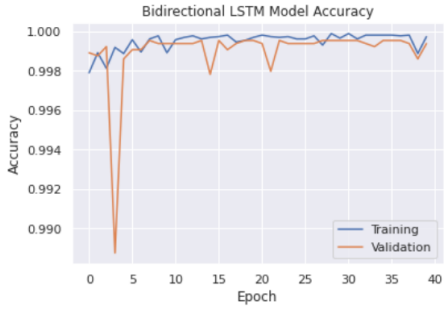

Fig. 4. Epoch versus Accuracy of Training and Validation

an accuracy of 99.97% on different data sets. The performance metrics of those three models are given in the Table II.

Lastly, we did another experiment by changing the attack traffic volume in different percentages of normal traffic in our training data set. We took 20% to 100% of attacking traffic in terms of benign traffic every time by varying 20% in each test set. Suppose, the number of rows of benign traffic is 20000, So 20% of attack traffic is 4000 rows used in the first test set. As the attack traffic volume is increased the detection accuracy becomes higher slowly and it is shown in Table III.

VI. CONCLUSION

In this paper, we simulated a 5G network slice testbed using Free5GC and UERANSIM and showed the impact of DoS/DDoS attacks on performances of 5G network slices. We also generated a new dataset by injecting variety of benign and DoS/DDoS attacks traffic on different network slices. The new data set is used to evaluate our SliceSecure model that can classify benign and DoS/DDoS attack traffic with a success rate of 99.99%. Additionally, the malicious UE can also be detected from that model.

In the future, more slices can be created rather than two slices in the 5G network which will make the network more realistic. Except for the mentioned DoS/DDoS attacks traffic, different types of attack traffic can be added to the data set to make it more robust.

ACKNOWLEDGEMENT

This work was supported in part by funding from the Innovation for Defence Excellence and Security (IDEaS) program from the Department of National Defence (DND).

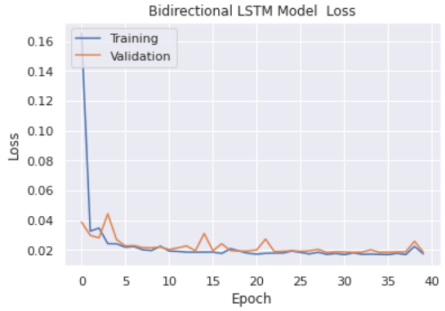

Fig. 5. Epoch versus Loss of Training and Validation

REFERENCES

[1] Ruxandra F. Olimid and Gianfranco Nencioni. 5G Network Slicing: A Security Overview. *IEEE Access*, 8:99999–100009, 2020.

[2] Vipin N Sathi and C Siva Ram Murthy. Distributed slice mobility attack: A novel targeted attack against network slices of 5g networks. *IEEE Networking Letters*, 3(1):5–9, 2020.

[3] Iman Sharafaldin et al. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization:. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, pages 108–116, 2018.

[4] Iman Sharafaldin et al. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In *2019 International Carnahan Conference on Security Technology (ICCST)*, pages 1–8, October 2019.

[5] Alex Sherstinsky. Fundamentals of Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) network. *Physica D: Nonlinear Phenomena*, 404:132306, March 2020.

[6] Badre Bousalem et al. Deep learning-based approach for ddos attacks detection and mitigation in 5g and beyond mobile networks. In *2022 IEEE 8th International Conference on Network Softwarization (NetSoft)*, pages 228–230, 2022.

[7] Dong Li, Chang Yu, Qizhao Zhou, and Junqing Yu. Using SVM to Detect DDoS Attack in SDN Network. *IOP Conference Series: Materials Science and Engineering*, 466:012003, December 2018.

[8] Matheus P. Novaes et al. Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment. *IEEE Access*, 8:83765–83781, 2020.

[9] Danish Sattar and Ashraf Matrawy. Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices. In *2019 IEEE Conference on Communications and Network Security (CNS)*, pages 82–90, June 2019.

[10] Anurag Thantharate et al. Secure5G: A Deep Learning Framework Towards a Secure Network Slicing in 5G and Beyond. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 0852–0857, January 2020.

[11] Xiaoyong Yuan, Chuanhuang Li, and Xiaolin Li. Deepdefense: Identifying ddos attack via deep learning. In *2017 IEEE International Conference on Smart Computing (SMARTCOMP)*, pages 1–8, 2017.

[12] Noble Arden Elorm Kuadey et al. DeepSecure: Detection of Distributed Denial of Service Attacks on 5G Network Slicing—Deep Learning Approach. *IEEE Wireless Communications Letters*, 11(3):488–492, March 2022.

[13] Wireshark· go deep." https://www.wireshark.org/(accessed jul. 28, 2022).

[14] Applications | Research | Canadian Institute for Cybersecurity | UNB https://www.unb.ca/cic/research/applications.html (accessed jul. 28, 2022.

[15] Understanding lstm networks – colah's blog, url = https://colah.github.io/posts/2015-08-Understanding-LSTMs/,urldate = 2022-07-28.

[16] Kshira Sagar Sahoo et al. An evolutionary svm model for ddos attack detection in software defined networks.

[17] Ali Shiravi, Hadi Shiravi, Mahbod Tavallaee, and Ali A. Ghorbani. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Computers Security*, 31(3):357–374, 2012.