Deep Learning-based Approach for DDoS Attacks Detection and Mitigation in 5G and Beyond Mobile Networks

Badre Bousalem, Vinicius F Silva, Rami Langar, Sylvain Cherrier

Deep Learning-based Approach for DDoS Attacks Detection and Mitigation in 5G and Beyond Mobile Networks

Badre Bousalem*, Vinicius F. Silva*, Rami Langar*†, Sylvain Cherrier*
*University Gustave Eiffel, LIGM-CNRS UMR 8049, F-77454, Marne-la-Vallée, France
†Software and IT Engineering Department, École de Technologie Supérieure (ÉTS), Montréal, QC H3C1K3, Canada
E-mails: {badre.bousalem, vinicius.fonsecaesilva, rami.langar, sylvain.cherrier}@univ-eiffel.fr

***Abstract*—In this demo, we present a 5G prototype for attacks detection and mitigation in sliced networks leveraging Machine Learning (ML). Our prototype, based on *OpenAirInterface*, allows creating network slices on demand and managing physical resources dynamically according to the users' behavior, while considering the inputs from a northbound Software Defined Network (SDN) application. We focus here on Distributed Denial of Service (DDoS) attacks, where one or multiple malicious users generate attacks on the 5G Core Network. Based on our developed ML module, we show that our prototype is able to detect such attacks, then automatically creates a sinkhole-type slice with a small portion of physical resources, and isolates the malicious users within this slice to mitigate the attackers' action. We demonstrate the effectiveness of our approach by showing the decrease in the network throughput for the malicious users by a factor of 15, while maintaining a high network throughput for benign users.**

***Index Terms*—5G, Slicing, Cybersecurity, Deep Learning.**

I. Introduction

5G networks powered by network slicing features uncover several challenges in the cybersecurity context, which have not been properly addressed yet by 5G standards. In such a context, heterogeneous nodes demand different network services and present intermittent connections, where traditional security approaches are not always accurate.

Several research works have been conducted in the last two decades to optimize security solutions whilst considering 5G network requirements. However, there is still a lack of works that consider the network slicing context along with Machine Learning (ML) based approaches, in order to protect 5G networks from cyber attacks such as Distributed Denial of Service (DDoS).

Network slicing allows to create multiple logical instances of the physical network, the so-called "network slices", ensuring traffic isolation among them, and tailoring the network resources of each slice to a specific class of applications, by leveraging the concepts of Software Defined Networking (SDN) and Network Function Virtualization (NFV). Network slicing has the potential to enable the coexistence of a wide range of mobile services in the same network infrastructure.

A number of prototypes have been proposed in the literature to address the challenges imposed by sliced 5G networks. In view of this, authors in [1] described how to use *FlexRAN* [2] and *OpenAirInterface* (OAI) [3] to deploy a Cloud Radio Access Network (C-RAN) architecture in an automated and virtualized way. Authors in [4] described their experience building a 5G prototype that uses dynamic network slicing for Internet of Things (IoT) and Enhanced Mobile Broadband (eMBB) services. Authors in [5] presented their prototyping platform called SCOPE, that integrates an open source container for instantiating softwarized and programmable cellular network elements, accompanied with an emulation module for testing new solutions in real-world deployments. SCOPE also has a data collection module that can be used for ML-based solutions, with multiple APIs that allow users to control network functionalities in real-time.

In the ML context, relevant works include the application of Deep Learning (DL) and Deep Reinforcement Learning to predict the network load [6] [7], classify traffic [8] [9], control and configure 5G platforms automatically [10], and detect and mitigate cross-layer attacks in wireless networks through Bayesian Learning [11]. More specifically, in the DDoS attacks context, authors in [12] propose an optimization model to proactively mitigate DDoS attacks in the 5G Core Network (CN) through on-demand intra/inter slice isolation, hence guaranteeing network performance requirements for 5G CN slices. Similarly, authors in [13] propose *DeepSecure*, a framework that uses a Long Short Term Memory (LSTM) DL-based model to classify users' network traffic as DDoS or benign, as well as a slice prediction model that predicts the appropriate slice for users previously classified as benign.

Given the above context, in particular the lack of proposals in the literature that assess cybersecurity solutions in a realistic scenario, it is of paramount importance having a simple, yet controlled environment that focuses on 5G cybersecurity applications and leverages network slicing to detect and mitigate attacks from malicious users. To achieve this, we present in this paper a 5G prototype that allows creating network slices on demand and managing physical

resources dynamically according to the users' behavior, while considering the inputs from a northbound SDN application. Different from the works presented above, our proposal mainly focuses on ML-based solutions to protect 5G networks from security threats leveraging real-time network slicing. Specifically, we develop a DL model for DDoS attacks detection and mitigation, which is integrated to the SDN application as one of the network slicing policies. Based on our developed DL model, we show that our prototype is able to detect such attacks, then instantaneously creates a sinkhole-type slice with the smallest possible portion of physical resource blocks (PRBs), and isolates the malicious users within this slice to mitigate their actions. We demonstrate the effectiveness of our approach mainly by showing the decrease in the network throughput for the malicious users, while maintaining a high network throughput for benign users.

The remainder of this paper is organized as follows: Section II describes our 5G prototype highlighting the hardware and software applied, as well as our proposed approach for DDoS attacks detection and mitigation. Section III describes the steps of our demo.

II. Prototype and Proposed Approach Description

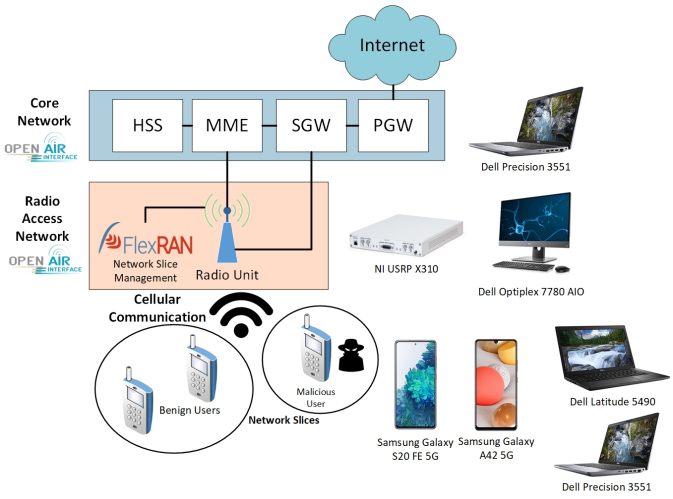

Fig. 1. 5G prototype's base hardware/software resources.

Fig. 1 shows the base hardware/software resources deployed in our 5G prototype. To emulate the cellular network elements (i.e., the Core Network – CN – and the Radio Access Network – RAN), we use *OpenAirInterface* (OAI). OAI is an open-source software developed by Eurecom to support mobile telecommunication systems like 4G Long Term Evolution (LTE) and 5G New Radio (NR). To deploy the CN elements, composed in this scenario by the Home Subscriber Server (HSS), the Mobility Management Entity (MME), the Serving Gateway (SGW) and the Package Gateway (PGW), we use a Dell Precision 3551 laptop, which provides access to the Internet. On the other hand, for

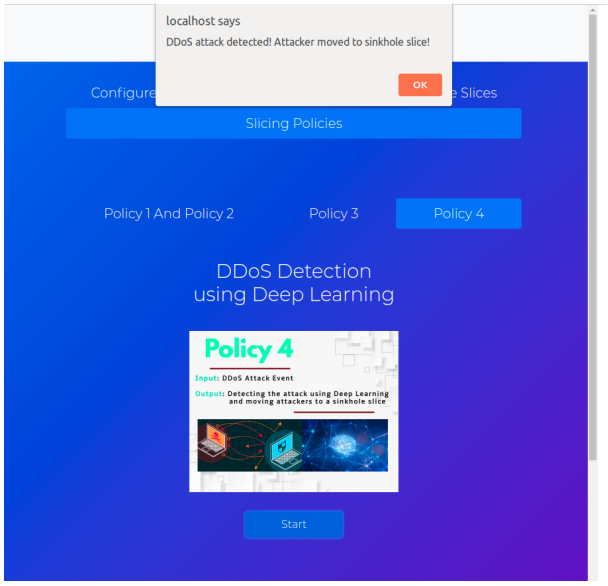

Fig. 2. DL-based DDoS attacks detection and mitigation triggering screenshot.

the RAN part, we use a Dell Optiplex 7780 AIO desktop PC, which in turn is connected to a USRP X310 card. The USRP card is responsible to emulate the Radio Unit (RU), thus creating a communication interface between the RAN and the users, represented here by two different Commercial Off-The-Shelf (COTS) smartphone models: Samsung Galaxy S20 FE 5G and Samsung Galaxy A42 5G.

To emulate the attacks, we use one Dell Latitude 5490 and one Dell Precision 3551, each connected to a Wi-Fi hotspot, created by the smartphones, which in turn are connected to the 5G network. The attacks are generated using the *Mausezahn* tool [14].

Our prototype makes also use of the SDN *FlexRAN* controller [2], that enables remote control of the OAI MAC layer, through a specific southbound interface (SBI), based on Google Protobuf [2]. On the top of *FlexRAN*, we have developed a northbound "Slicing APP" application, which enables the network administrator to deploy network slicing policies in a user-friendly and abstracted way. The network slicing policies have a dedicated tab, where the network administrator can configure and trigger the proper policy according to network changes and end-to-end service requirements.

In particular, in the 5G security context, we have developed a network slicing security policy leveraging ML techniques. Specifically, a DL model based on Convolutional Neural Networks is implemented using *Lucid* [15], to allow detecting and mitigating DDoS attacks (cf. triggering screenshot in Fig. 2). To train and test our DL model, we built a custom dataset by using our 5G prototype, based on synthetic DDoS attack samples generated by the *Metasploit* framework [16] and the *Mausezahn* tool, as well as benign traffic samples generated through the *iperf3* tool.

Once the above-mentioned slicing security policy is

triggered, the DL model continuously observes the malicious users' behavior, in order to detect their actions. Once an attack event is detected, a sinkhole-type slice is automatically created by the *FlexRAN* controller, while allocating the smallest possible portion of PRBs. Then, malicious users will be moved to this particular slice, thus mitigating their actions. The demo details of our network slicing security policy will be given in the following section.

III. Demo Overview and Results

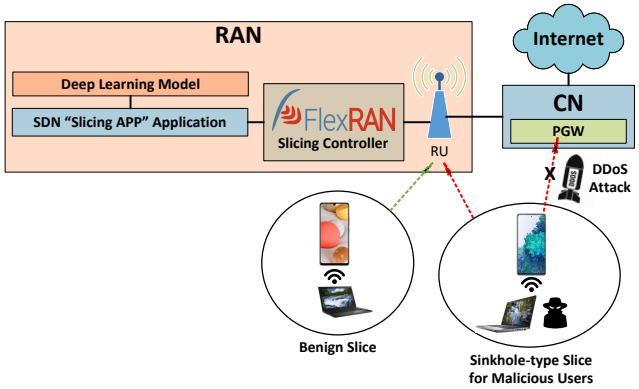

Fig. 3. Demo scenario.

Fig. 3 presents our demo scenario, with one benign user and one DDoS attacker, whose target is the CN's PGW. Our demo consists of the following steps. Firstly, we deploy our Mobile Virtual Network Operator (MVNO) by starting the CN, the RAN elements and the *FlexRAN* controller. Then, through our SDN "Slicing APP" application, we create a slice to which all available PRBs are allocated. Initially, both smartphones are associated to this default slice after establishing a successful connection with the MVNO. Then, we activate their respective Wi-Fi hotspots to allow connecting the two laptops, being one laptop for each Wi-Fi hotspot.

In this stage, the whole prototype is ready to receive network traffic, including DDoS attacks. The laptop linked to the benign user first starts to send regular traffic to the PGW through the *iperf3* tool. At the same time, the laptop linked to the malicious user starts a DDoS attack through the *Mausezahn* tool, also having the PGW as target. Through our SDN "Slicing APP" application, we then activate the network slicing security policy, which triggers a network analysis using our DL model. Once the DL model detects a DDoS attack, it automatically creates a sinkhole-type slice to which the malicious device is moved. Note that a minimum of 3 PRBs are allocated to this particular slice. By using the *Speedtest* tool, we observed that the network throughput for the malicious user is downgraded from ∼30 Mbps to ∼2 Mbps (i.e., a decrease by a factor of 15), while that of the benign user is maintained high at ∼30 Mbps. A short video describing each step of our proposed demo and showing the above throughput results can be found at [17].

In addition, according to our experiments using our 5G prototype, we found that the average delays for sinkhole-type slice creation and transfer of a malicious user to such a slice is of ∼5.6 milliseconds each (with a 95% confidence interval ranging between 4.92 and 6.28 milliseconds). Concerning the DL model's performance, our model is able to achieve an accuracy of almost 97%, and a false positive rate (i.e., the probability that a benign traffic will be classified as malicious) of less than 4%.

Acknowledgment

This work was supported by the ANR 5G-INSIGHT project (Grant no. ANR-20-CE25-0015).

References

[1] R. Schmidt, C.-Y. Chang, and N. Nikaein, "FlexVRAN: A Flexible Controller for Virtualized RAN Over Heterogeneous Deployments," in *IEEE International Conference on Communications (ICC)*, 2019.
[2] Mosaic 5G. FlexRAN. [Online]. Available: https://mosaic5g.io/flexran/
[3] Eurecom. OpenAirInterface. [Online]. Available: https://openairinterface.org/
[4] S. Costanzo, S. Cherrier, and R. Langar, "Network Slicing Orchestration of IoT-BeC^3 applications and eMBB services in C-RAN," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2019, pp. 975–976.
[5] L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "SCOPE: An Open and Softwarized Prototyping Platform for NextG Systems," in *Proc. of ACM Intl. Conf. on Mobile Systems, Applications, and Services (MobiSys)*, Virtual Conference, June 2021.
[6] N. Salhab, R. Langar, R. Rahim, S. Cherrier, and A. Outtagarts, "Autonomous Network Slicing Prototype Using Machine-Learning-Based Forecasting for Radio Resources," *IEEE Communications Magazine*, vol. 59, no. 6, pp. 73–79, 2021.
[7] D. Bega, M. Gramaglia, M. Fiore, A. Banchs, and X. Costa-Pérez, "DeepCog: Optimizing Resource Provisioning in Network Slicing With AI-Based Capacity Forecasting," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 2, pp. 361–376, 2020.
[8] Y. Li, B. Liang, and A. Tizghadam, "Robust Online Learning against Malicious Manipulation and Feedback Delay With Application to Network Flow Classification," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 8, pp. 2648–2663, 2021.
[9] T. N. Weerasinghe, I. A. M. Balapuwaduge, and F. Y. Li, "Supervised Learning based Arrival Prediction and Dynamic Preamble Allocation for Bursty Traffic," in *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2019.
[10] T. A. Khan, A. Mehmood, J. J. Diaz Rivera, and W.-C. Song, "Machine Learning Approach for Automatic Configuration and Management of 5G Platforms," in *20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2019.
[11] L. Zhang, F. Restuccia, T. Melodia, and S. M. Pudlewski, "Learning to detect and mitigate cross-layer attacks in wireless networks: Framework and applications," in *Proc. of IEEE Conference on Communications and Network Security (CNS)*, 2017, pp. 1–9.
[12] D. Sattar and A. Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," in *Proc. of IEEE Conference on Communications and Network Security (CNS)*, 2019, pp. 82–90.
[13] N. A. E. Kuadey *et al.*, "DeepSecure: Detection of Distributed Denial of Service Attacks on 5G Network Slicing—Deep Learning Approach," *IEEE Wireless Communications Letters*, vol. 11, no. 3, pp. 488–492, 2022.
[14] Netsniff-ng. Mausezahn. [Online]. Available: http://netsniff-ng.org/
[15] R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martínez-del Rincón, and D. Siracusa, "Lucid: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, 2020.
[16] Rapid7. Metasploit. [Online]. Available: https://www.metasploit.com/
[17] B. Bousalem, V. F. Silva, R. Langar, and S. Cherrier. Deep Learning-based Approach for DDoS Attacks Detection and Mitigation in 5G and Beyond Networks (Demo Video). [Online]. Available: https://www.youtube.com/watch?v=YBx22va56N0