IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

Real -Time Network Packet Classification Exploiting Computer Vision Architectures

Pradeep Nayak[1] , Sudeep Rathod[2], Surabhi[3], Sukanya[4]
Alva's Institute of Engineering and Technology Mijar, Moodubidri Mangalore, India[1,2,3,4]

Abstract: *The upcoming 6G and NextG networks underscore the necessity of sophisticated security methods based on Artificial Intelligence (AI) in order to detect malicious activity and adjust to new threats. Because computer vision techniques may be used to recognize complex patterns, their incorporation into the cybersecurity industry is a promising development. In this work, we present a computationally effective categorization technique that enforces the real-time conversion of packets into pictures by directly acting upon the raw packets gathered at base stations. The suggested solution's novel features include its lightweight implementation, which well satisfies the requirements of upcoming 6G networks, and its network edge operation, which permits early threat detection as near to the packet origin as feasible. We examine the efficacy of this methodology in terms of F1-score and prediction time by employing cutting-edge computer vision architectures and a customized Convolutional Neural Network (CNN) to tackle an intrusion detection task utilizing a substantial 5G dataset. The CNN design is superior than complicated models, as demonstrated by the results of experiments. The CNN consistently beats the other cutting-edge computer vision models over several packet window sizes N (i.e., 10, 50, and 100 packets), reaching very high F1-scores (0.99593, 0.99860, and 0.99895). A scalability investigation reveals a trade- off between the performance and scalability of CNN, with higher N values resulting in longer prediction times. However, the scalability of the other computer vision models is superior, allowing for an ideal model selection free of compromises.*

Keywords: S DoS, computer vision, artificial intelligence, 6G networks, packet classification, convolutional neural networks

I. INTRODUCTION

In order to meet the demands of applications for the upcoming decade, industry and academia are already concentrating on 6G/NextG even as 5G network infrastructures are being installed, with a more widespread expansion anticipated in the coming years [1]. In fact, a number of situations demonstrate the shortcomings of 5G networks with regard to latency, data throughput, worldwide coverage, etc. [2]. The implementation of 6G network infrastructures will be important in realizing the full potential of applications like digital twins, holographic communications, and extended reality [3]. Extreme capacity, dependability, and efficiency are just a few advantages of 6G networks. In order to meet these demanding performance goals, 6G networks are anticipated to include sophisticated network management and orchestration techniques [4]. Therefore, in addition to The Authors in 2024. An Attribution-Non Commercial No Derivatives 4.0 License is applicable to this work. PAOLINI and Associates: Real-time classification of network packets AI will be a fundamental technology that enables the shift from linked items to collective network intelligence, allowing for the simplicity of networks through computer vision architectures and the convergence of Radio Access Network (RAN) and Core Network (CN) [5], [6]. A promising avenue for advanced pattern recognition tactics in the quickly changing field of network security is the use of computer vision techniques for cybersecurity applications. The goal of complicated pattern recognition is actually where DoS and computer vision techniques overlap. To identify complex patterns in photos and videos, computer vision algorithms analyze visual data. Numerous levels of abstraction are involved in this process; upper layers combine simple information, such edges, to recognize complex objects or scenes, while lower layers detect more fundamental aspects. Similar to this, network traffic analysis deals with finding unusual patterns in the context of DoS attack detection. The goal of pattern recognition is to discern between harmful activity and typical network behaviour.

II. RELEVANT WORKS

One of the main issues with 5G networks has been network security in order to handle mission-critical applications and the Internet of Things (IoT) while also offering enhanced user privacy and new trust and service models [7], [8]. For the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

various 6G verticals to be deployed safely, network security needs to be improved and reinforced [9]. In order to address some of the new security issues brought about by innovative network architectures, scientists have concentrated on developing innovative strategies that are appropriate for 6G networks. Because of its capacity to extract high-level information, Deep Learning (DL) algorithms have demonstrated encouraging results in threat mitigation [10]. Its utilization in 5G/6G situations is hindered by the first, which operates on features taken from entire traffic flows. With regard to the latter, a PCAP-to- Embeddings approach is put forward, in which Long Short-Term Memory Autoencoders are employed to generate embeddings, and a Fully-Connected network is then employed for classification purposes. Its use in 5G/6G scenarios is limited by the first, which uses characteristics extracted from whole traffic flows. Concerning the latter, a PCAP-to-Embeddings method is proposed, whereby Long Short-Term Memory Autoencoders are utilized to produce embeddings, and a Fully-Connected network is then trained for classification. The study that is suggested in this paper is different in many ways from all of the previously described publications.

Initially, we look at several computer vision architectures, which gives us the opportunity to look into a wider range of options. We address the practicality of transforming network packets into pictures in real time through the use of preprocessing methods

III. RECOMMENDED ARCHITECTURE

First, we go over how network packets may be converted into pictures in this part, emphasizing the characteristics that are utilized and the associated preprocessing methods.

Next, we provide an overview of how the suggested approach may be integrated into a next-generation eNB(gNB), demonstrating how it might be compatible with upcoming 6G/NextG wireless infrastructure.

FROM NETWORK TRANSACTIONS TO IMAGES:

The fundamental data unit delivered over a computer network is represented by a packet. A portion of the entire message is included in each packet, along with information that aids in determining the traffic flow. A 5-tuple consisting of source and destination ports, source and destination IP addresses, and the protocol being used can be used to identify the latter.

An encoding strategy to convert packet characteristics into a structured format, such as matrices, is presented in this study using the idea of network traffic flow. A spatial data representation is produced by organizing the input into packet matrices.

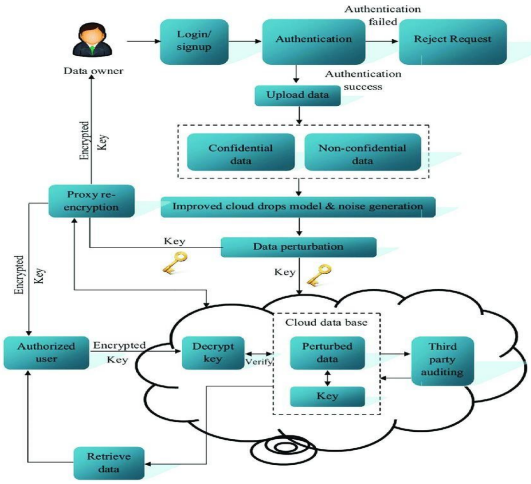

Fig: Proposed Architecture Diagram

Convolutional filters that glide across the input and pick out important patterns allow the Neural Network (NN) to learn the characteristics of both benign traffic and DoS assaults thanks to this representation. In particular, the method entails (i) determining the characteristics (F) that may be derived from packets of a certain flow (e.g., Time-to-live and packet

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

length); and (ii) establishing a maximum number of packets (N) for each flow that can be sent within a time frame (T) [12]. Which means that N × F will be the largest size of the input matrices. A real-time method involves padding the matrix with 0s if N packets are not collected within the allotted period.

INTEGRATION WITH BASE STATIONS

We go into depth in this part on how a future 6G base station may use the suggested architecture. Because 5G networks include a variety of protocols, interfaces, and management techniques, the RAN and CN functions are rigorously segregated. As a result, it was difficult for 5G designs to integrate these components into a converged network and create a single, streamlined network architecture. But there is a once-in-a-lifetime chance to reconsider network architectures with the arrival of developing technologies and the move to 6G networks. A simpler, more effective network infrastructure may be created thanks to the move towards a converged RAN-CN design [6].

Utilizing user data, the NWDAF may be used for intelligent threat prevention. It may collect User Plane Function (UPF) data coming from User Equipments (UEs) and supply it to a Deep Learning (DL) system so that malicious traffic may be identified. For example, the NWDAF can include a threat detection and mitigation system that will recognize and automatically discard packets that have been flagged as harmful. By directly identifying any threats at the base station level, this design eliminates the need to spread them throughout the network. The idea behind this strategy is to position security measures as near to probable threat sources as feasible. In this case, real-time detection is especially crucial because of the projected cost of service disruption [11].

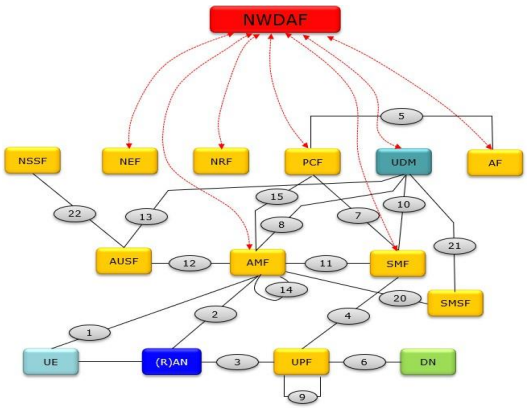

Fig: The proposed system's architecture, which lists the primary NFs employed. A local CN is also installed with the NextG base station. To handle packets received from the UPF, the suggested method makes use of NN that is implemented inside the NWDAF. You can recognize malicious packets and dispose of them immediately at your neighbourhood NWDAF.

IV. METHODOLOGY

The sixth generation of cellular technology, or 6G, is currently under development and aims to bring ultra-high speeds, very little latency, and revolutionary connection capabilities to completely transform wireless communication. It aims to improve machine-to-machine (M2M) communication and support a wider range of applications, building on the foundation set by 5G.

NETWORK INTRUSION DETECTION

The quality of the dataset and the degree to which the behavior of an ML-based cybersecurity system approximates actual network conditions have a major impact on the accuracy and effectiveness of the system. Large datasets that reflect the intricacies of 5G and 6G network operations are hard to come by in AI-based security research. Because most public datasets were gathered before significant technological breakthroughs, such as UNSW-NB 15 and CTU-13 [14], they are out of date for contemporary networks. A significant class imbalance and a large number of redundant records are two further issues with recent online datasets, such as CIC-DDoS2019 [13].Furthermore , as discussed in Section II, the simulation platform or testbeds used to generate these datasets exhibit behavior that differs significantly

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

from that of 5G/6G networks. This issue was addressed by the authors of [24], who just released 5G-NIDD, a network intrusion detection dataset that was taken from an actual 5G test network. In Oulu, Finland, this dataset was collected using the 5G Test Network (5GTN). In a variety of attack scenarios, 5G-NIDD provides both attack and benign traffic. The traffic was produced by real mobile devices connected to the 5GTN. Data was stolen from one attacker node and two base stations that were connected to a number of innocuous 5G UEs. DoS attacks and port scanning are two possible attack methods. Several types of DoS attacks are included in the dataset, including SYN Flood, HTTP Flood, UDP Flood, ICMP Flood, and Slow rate DoS. SYN, TCP Connect, and UDP are some of the port searches it offers. This dataset is available to the public in both pcapng and csv formats. Although the entire packet can be viewed in the pcapng format, CSV files include statistical summaries for each traffic flow.

This study evaluated the proposed architectures using the 5G- NIDD dataset. Every assault that was part of the dataset is detailed in Table 2, along with information about each one. Following the preprocessing of the dataset into matrices, insufficient samples were available to test for the type of ICMP flood assault. Nonetheless, nine classes remain in use because the HTTP flood was carried out using two distinct programs, Slowly is and Tors hammer.

NEURAL NETWORK ARCHITECTURES

This section discusses the computer vision models that were evaluated using network traffic packet matrices.In addition to employing well-known, sophisticated models, we have developed a unique Convolutional Neural Network (CNN) that is intended to detect any security risks in the traffic data. The model architecture known as the Residual Network, or ResNet, is one of the major advancements in computer vision. Training very deep neural networks, which might have problems like vanishing or exploding gradients, is a challenge that ResNet attempts to solve. ResNet presents Residual Blocks as a solution to this problem. Instead of the network simply trying to learn the function F(x)F(x)F(x), where xxx is the input to a layer, the network learns H(x)=F(x)+xH(x) = F(x) + xH(x)=F(x)+x. This means that the output of a layer includes the original input as well as the result from the previous layers, making it easier for the network to learn deeper features and reducing the training challenges of very deep networks. In simpler terms, ResNet helps the model learn better by keeping the original input signal as part of the process, which makes it easier to train networks with many layers. This approach is especially useful for recognizing complex patterns in tasks like threat detection in network traffic data. The Efficient Net model was presented by the authors in [16] with the goal of improving the accuracy and efficiency of convolutional neural networks (CNNs).

Conventional CNN enhancement techniques typically entail haphazard modifications or numerous manual tweaks, which can be laborious and inefficient. On the other hand, EfficientNet takes a more intelligent, structured strategy. Three key components of the model are adjusted by this technique, known as compound scaling: the breadth of the layers, the depth of the network, and the resolution of the input images. Using a predetermined ratio, EfficientNet scales these variables collectively in a balanced manner rather than altering them at random. By doing this, the network's performance is improved without growing overly complicated or ineffective. This method is simpler, more effective, and requires less manual effort compared to traditional ways of improving the model. DenseNet [17], in contrast to MobileNet and EfficientNet, adopts a different strategy that is not intended to be computationally efficient. In Dense Net, every layer is forward connected to every other layer, thus the output of every layer before it serves as the input for the layer that comes after it. In order to process so numerous connections, Dense Net needs more resources, which increases its processing demands.

V. CONCLUSION

6G/NextG networks will require intelligent systems to identify and manage various types of malicious traffic and to adapt to emerging threats. Our study offers a new method that transforms network data packets into picture-like formats for classification utilizing advanced computer vision models. Determining whether network activity was malicious or benign and detecting intrusions were the objectives of the investigations. In order to demonstrate how raw network packets can be quickly converted into matrices that are prepared for processing by cutting-edge computer vision models, we described a custom CNN built for this purpose. Based on the findings, our customized CNN model outperformed more complex models. With F1-scores of 0.99593, 0.99860, and 0.99895, respectively, the CNN performed better than other state-of-the-art computer vision techniques for all values of N (10, 50, and 100). We

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

additionally assessed our method's scalability. As N increases, we found that the time required to produce forecasts increases as well. While modern models initially have longer prediction times, they scale better as N increases. You can choose the best model for a specific value of N as a result, without sacrificing speed for performance. Our developed technique is only the first step in applying computer vision to network data analysis. By employing convolution-based models, we are able to identify more complex patterns in the packet data. We could, for example, design a system that actively detects new types of cyberattacks. The future will be devoted to distributed learning methods like split or federated learning that can improve model performance while protecting data privacy. We also want to look at running these models on FPGAs and other specialized hardware. This would allow us to reduce the computational strain on the network's main processing unit (gNB) without rendering it lag-free.

REFERENCES

[1]. Y. Siriwardhana, P. Porambage, M. Liyanage and M. Ylianttila, "AI and 6G security: Opportunities and challenges", *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, pp. 616-621, 2021.H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.

[2]. C. De Alwis et al., "Survey on 6G frontiers: Trends applications requirements technologies and future research", *IEEE Open J. Commun. Soc.*, vol. 2, pp. 836-886, 2021.

[3]. .W. Jiang, B. Han, M. A. Habibi and H. D. Schotten, "The road towards 6G: A comprehensive survey", *IEEE Open J. Commun. Soc.*, vol. 2, pp. 334-366, 2021.

[4]. P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov and M. Ylianttila, "The roadmap to 6G security and privacy", *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094-1122, 2021.

[5]. W. Saad, M. Bennis and M. Chen, "A vision of 6G wireless systems: Applications trends technologies and open research problems", *IEEE Netw.*, vol. 34, no. 3, pp. 134-142, May/Jun. 2020.

[6]. V. Ziegler, H. Viswanathan, H. Flinck, M. Hoffmann, V. Räisänen and K. Hätönen, "6G architecture to connect the worlds", *IEEE Access*, vol. 8, pp. 173508-173520, 2020.

[7]. H. Moudoud, L. Khoukhi and S. Cherkaoui, "Prediction and detection of FDIA and DDoS attacks in 5G enabled IoT", *IEEE Netw.*, vol. 35, no. 2, pp. 194-201, Mar./Apr. 2021.

[8]. M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov and M. Ylianttila, A Comprehensive Guide to 5G Security, Hoboken, NJ, USA:Wiley, 2018.

[9]. S. A. A. Hakeem, H. H. Hussein and H. Kim, "Security requirements and challenges of 6G technologies and applications", *Sensors*, vol. 22, no. 5, pp. 1969, 2022.

[10]. X. Yuan, C. Li and X. Li, "DeepDefense: Identifying DDoS attack via deep learning", *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, pp. 1-8, 2017.

[11]. B. de Neira, B. Kantarci and M. Nogueira, "Distributed denial of service attack prediction: Challenges open issues and opportunities", *Comput. Netw.*, vol. 222, Feb. 2023.

[12]. R. Doriguzzi-Corin, S. Millar, S. Scott-Hayward, J. Martinez-del Rincon and D. Siracusa, "LUCID: A practical lightweight deep learning solution for DDoS attack detection", *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 2, pp. 876-889, Jun. 2020.

[13]. I Sharafaldin, A. H. Lashkari, S. Hakak and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy", *Proc. Int. Carnahan Conf. Security Technol. (ICCST)*, pp. 1-8, 2019.

[14]. S. Garcia, M. Grill, J. Stiborek and A. Zunino, "An empirical comparison of botnet detection methods", *Comput. Secur.*, vol. 45, pp. 100-123, Sep. 2014

[15]. S. Samarakoon et al., "5G-NIDD: A comprehensive network intrusion detection dataset generated over 5G wireless network", *arXiv:2212.01298*, 2022.

[16]. M. Tan and Q. Le, "EfficientNetv2: Smaller models and faster training", *Proc. 38th Int. Conf. Mach. Learn.*, pp. 10096-10106, 2021.

[17]. G. Huang, Z. Liu, L. Van Der Maaten and K. Q. Weinberger, "Densely connected convolutional networks", *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, pp. 4700-4708, 2017