9th IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2024) - Workshop of NOMS 2024

Packet Continuity DDoS Attack Detection for Open Fronthaul in ORAN System

Jung-Erh Chang
dept. of Electrical Engineering,
National Taiwan University of Science and Technology,
Taipei, Taiwan.
m11207502@mail.ntust.edu.tw

Yi-Chen Chiu
dept. of Electrical Engineering,
National Taiwan University of Science and Technology,
Taipei, Taiwan.
m11207505@mail.ntust.edu.tw

Yi-Wei Ma
dept. of Electrical Engineering,
National Taiwan University of Science and Technology,
Taipei, Taiwan.
ywma@mail.ntust.edu.tw

Zhi-Xiang Li
dept. of Electrical Engineering,
National Taiwan University of Science and Technology,
Taipei, Taiwan.
m11107511@mail.ntust.edu.tw

Cheng-Long Shao
Kyushu Institute of Technology,
Iizuka, Japan.
shao@csn.kyutech.ac.jp

NOMS 2024-2024 IEEE Network Operations and Management Symposium | 979-8-3503-2793-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/NOMS59830.2024.10575799

***Abstract*—This study develops a deep learning-based Intrusion Detection System (IDS) for the Open Fronthaul (OFH) interface in Open Radio Access Network (O-RAN) architecture, focusing on detecting and mitigating Distributed Denial of Service (DDoS) attacks. It aims to enhance O-RAN network security, particularly in the CUS-Plane of the OFH interface, by employing advanced deep learning techniques for threat prediction and prevention. The research contributes practical insights and solutions to improve the security resilience of O-RAN's open architecture.**

***Keywords*—Open RAN, Open Fronthaul, DDoS detection, DDoS, IDS.**

I. Introduction

O-RAN revolutionizes wireless networks by offering an open, flexible, and interoperable architecture, breaking free from traditional closed systems. It plays a key role in advancing 5G technology.

O-RAN encounters challenges in security and business, with a focus on safeguarding information. Key security practices include authentication, access control, traffic monitoring, and event management. Protecting open interfaces from threats like man-in-the-middle (MITM) and Distributed Denial of Service (DDoS) attacks is essential.

The O-RAN architecture outlines six open interfaces: OFH, A1, O1, O2, E2, and R1, with OFH comprising CUS and M-Plane. The CUS-Plane manages user data communications, while the M-Plane oversees operations like configuration, monitoring, fault detection, and performance within OFH. This paper centers on the OFH interface, assessing its security challenges using O-RAN ALLIANCE specifications and proposing an Intrusion Detection System (IDS) tailored for the OFH environment.

The paper proceeds as follows: Section 2 reviews O-RAN's security specifications for OFH and literature on DDoS attacks. Section 3 details the selection of dataset features and our model's architecture. Section 4 presents our model's training results and analysis. Section 5 summarizes our findings and explores future research directions.

II. Related Works

This section is split into two parts: first, it outlines the O-RAN ALLIANCE's security specifications, and second, it reviews research papers on detecting DDoS attacks with deep learning techniques.

Table 1. Mandatory O-RAN OFH interface security controls.

Potential Goals	C -Plane	U- Plane	S -Plane	M -Plane
Authenticity				TLS/SSH
Confidentiality		PDCP		TLS/SSH
Integrity		PDCP		TLS/SSH
Authorization				NACM
Data Origination				TLS/SSH
Replay Prevention		PDCP		TLS/SSH

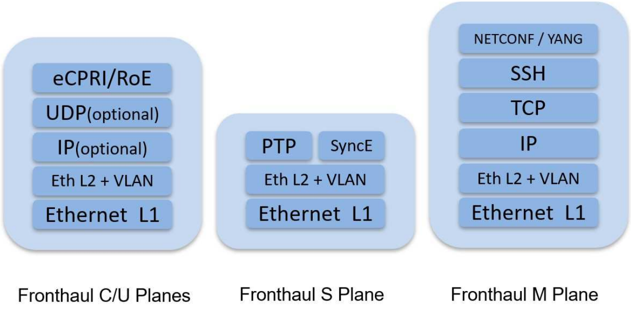


Figure 1. CUS and M-Plane protocol stack.

A. O-RAN Alliance

The O-RAN ALLIANCE's WG 4 details the CUS-Plane [1] and M-Plane [2] protocols in Figure 1. M-Plane uses TCP/IP with NETCONF/SSHv2 and NETCONF/TLS 1.2 for security, while CUS-Plane relies on Ethernet L2 connections, lacking standard security protocols.

At the May 2023 O-RAN ALLIANCE Leaders' Summit, a report on network security considerations was shared, focusing on using O-RAN for modern network architectures [3]. Section 5.3.1.1 highlights security risks in Open Interfaces, as shown in Table 1, pointing out vulnerabilities due to the lack of standard security measures. It's crucial to assess if O-RAN devices can reduce risks with standard security implementations as specified.

The O-RAN organization includes a Testing and Integration Focus Group (TIFG) that outlines the testing and integration methods for O-RAN. As specified in a technical document [4], TIFG focuses on security testing for the OFH interface, particularly on protecting the S-Plane and C-Plane from DoS attacks, which currently lack security measures.

This paper focuses on detecting DoS attacks on the OFH interface. To avoid excessive delays and potential

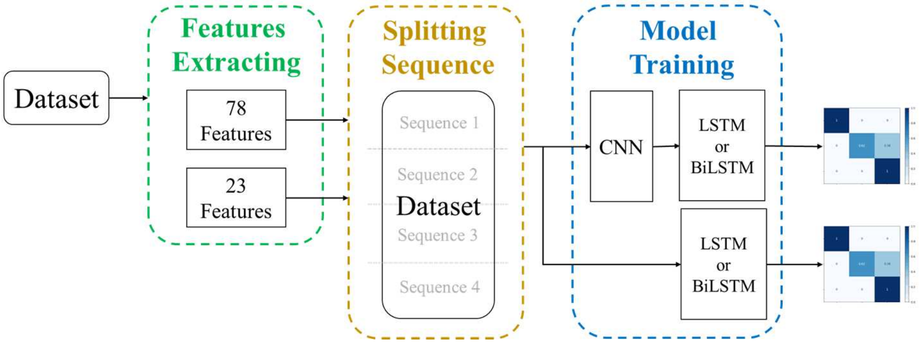


Figure 2. Workflow for experiments.

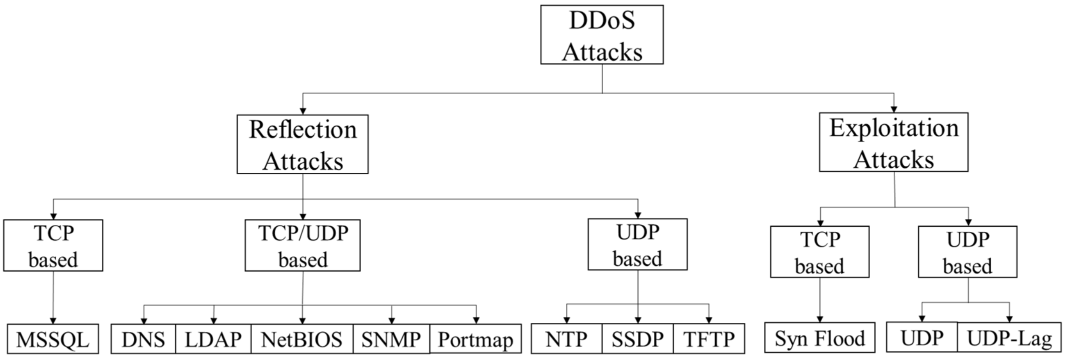


Figure 3. Attack types in CICDDoS2019.

disconnection between O-DU and O-RU due to DoS attacks, we propose setting up an IDS. The goal is to accurately identify attacks on the OFH interface before delays surpass a set threshold.

B. DDoS Attack Detection Research Literature

In IDS, the challenge of finding reliable, varied evaluation datasets has been significant. To tackle problems like limited flow diversity and a range of attack types, Sharafaldin, Lashkari, and Ghorbani introduced the CICIDS2017 dataset [5]. They also presented the CICDDoS2019 dataset [6], improving upon previous datasets' limitations and offering key detection features.

Bashaiwth, Binsalleeh, and AsSadhan [7] classified DDoS attacks using a Long-Short-Term Memory (LSTM) model on the CICIDS2017 and CICDDoS2019 datasets. They identified 51 key features that help detect DDoS attacks. Chu and Yan [8] developed a new method that tracks packet flow to detect attacks in real-time accurately, also using an LSTM model. This method introduces a fresh perspective on network security.

Based on the highlighted important features [6], our research reselects features using 23 attributes for DDoS classification. Compared to other studies, we have significantly reduced the number of features, enabling us to achieve faster processing speeds suitable for time-sensitive S-Plane environments in OFH. Additionally, our study integrates a packet continuity-based detection method proposed by [8] to enhance the data processing of the LSTM model, aiming for real-time and high-precision attack detection.

III. Implementation

Our experiments cover two main areas: data set processing and model training. We start by filtering features and segmenting continuous packet data into sequences. Then, we train and compare different models to see how they perform. The complete process is outlined in Figure 2.

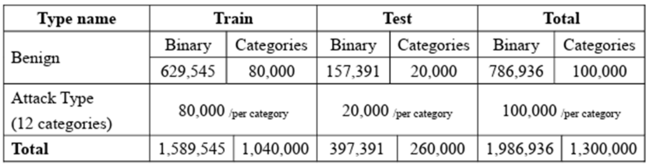
A. Dataset

Our experiment used normal traffic data from the CICDDS2017 dataset and attack traffic from CICDDoS2019, which includes real-world DDoS attacks like **Reflection-based** and **Exploitation-based attacks**, with subtypes such as TCP, UDP, and combined TCP/UDP attacks. The original classification in the dataset did not correctly show the categorization of SSDP and other attack types. Thus, we grouped the attack types ourselves for clearer representation in Figure 3.

Our research analyzed packet data and found uneven distribution across categories in the dataset. To address this, we extracted an equal number of instances for each category, creating a balanced training dataset. We also split the **Benign** category into two datasets—large and small quantities—depending on whether we were using a binary or multi-class approach. The details of the extracted quantities are shown in Table 2.

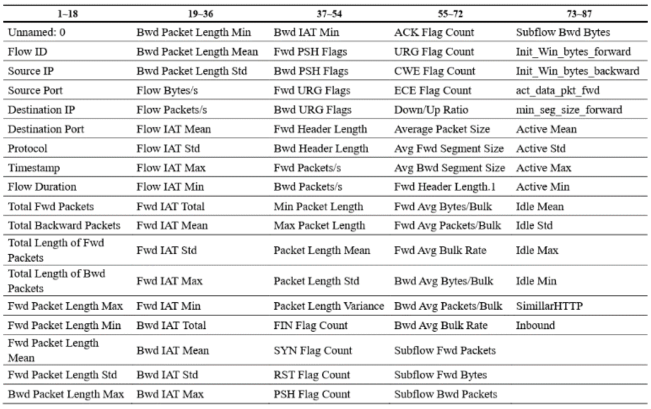
In our binary classification approach, we group all attack types into a single **Attack** category and aim to match the amount of normal traffic data to this combined attack dataset, requiring a large collection of normal data. Conversely, in our multi-class approach, **Benign** is considered a separate category, similar to each attack type. Here, we only need to extract as much normal traffic data as there is for each attack category, leading to a smaller dataset.

Table 2. Number of datasets.



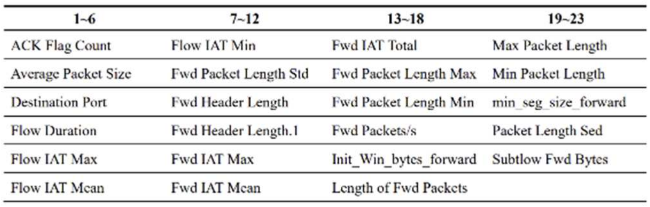
Type name	Train		Test		Total	
Benign	Binary	Categories	Binary	Categories	Binary	Categories
	629,545	80,000	157,391	20,000	786,936	100,000
Attack Type (12 categories)	80,000 /per category		20,000 /per category		100,000 /per category	
Total	1,589,545	1,040,000	397,391	260,000	1,986,936	1,300,000

Table 3. Total features from CICDDoS2019.



1–18	19–36	37–54	55–72	73–87
Unnamed: 0	Bwd Packet Length Min	Bwd IAT Min	ACK Flag Count	Subflow Bwd Bytes
Flow ID	Bwd Packet Length Mean	Fwd PSH Flags	URG Flag Count	Init_Win_bytes_forward
Source IP	Bwd Packet Length Std	Bwd PSH Flags	CWE Flag Count	Init_Win_bytes_backward
Source Port	Flow Bytes/s	Fwd URG Flags	ECE Flag Count	act_data_pkt_fwd
Destination IP	Flow Packets/s	Bwd URG Flags	Down/Up Ratio	min_seg_size_forward
Destination Port	Flow IAT Mean	Fwd Header Length	Average Packet Size	Active Mean
Protocol	Flow IAT Std	Bwd Header Length	Avg Fwd Segment Size	Active Std
Timestamp	Flow IAT Max	Fwd Packets/s	Avg Bwd Segment Size	Active Max
Flow Duration	Flow IAT Min	Bwd Packets/s	Fwd Header Length.1	Active Min
Total Fwd Packets	Fwd IAT Total	Min Packet Length	Fwd Avg Bytes/Bulk	Idle Mean
Total Backward Packets	Fwd IAT Mean	Max Packet Length	Fwd Avg Packets/Bulk	Idle Std
Total Length of Fwd Packets	Fwd IAT Std	Packet Length Mean	Fwd Avg Bulk Rate	Idle Max
Total Length of Bwd Packets	Fwd IAT Max	Packet Length Std	Bwd Avg Bytes/Bulk	Idle Min
Fwd Packet Length Max	Fwd IAT Min	Packet Length Variance	Bwd Avg Packets/Bulk	SimillarHTTP
Fwd Packet Length Min	Bwd IAT Total	FIN Flag Count	Bwd Avg Bulk Rate	Inbound
Fwd Packet Length Mean	Bwd IAT Mean	SYN Flag Count	Subflow Fwd Packets	
Fwd Packet Length Std	Bwd IAT Std	RST Flag Count	Subflow Fwd Bytes	
Bwd Packet Length Max	Bwd IAT Max	PSH Flag Count	Subflow Bwd Packets	

Table 4. Important features of each attack type.



1~6	7~12	13~18	19~23
ACK Flag Count	Flow IAT Min	Fwd IAT Total	Max Packet Length
Average Packet Size	Fwd Packet Length Std	Fwd Packet Length Max	Min Packet Length
Destination Port	Fwd Header Length	Fwd Packet Length Min	min_seg_size_forward
Flow Duration	Fwd Header Length.1	Fwd Packets/s	Packet Length Sed
Flow IAT Max	Fwd IAT Max	Init_Win_bytes_forward	Subtlow Fwd Bytes
Flow IAT Mean	Fwd IAT Mean	Length of Fwd Packets	

This dataset includes 87 features for each attack type, detailed in Table 3. However, not all these features are essential for classification. Considering our goal to use this detection system in the O-RAN S-Plane, where fast attack detection is vital to reduce latency, we aim to decrease the number of features to speed up the decision-making process.

The dataset is split into two subsets based on the number of features. The first subset adopts the method from [7], excluding socket features affected by network changes and features like Unnamed: 0, Source Port, Protocol, SimilarHTTP, and Inbound due to their low relevance to attack types. This leaves us with 78 features for use.

The second subset uses 2-5 key features per attack category, as recommended by [6], totaling 23 features shown in Table 4. We expect these features to effectively identify attacks, hoping for similar classification accuracy as with the full feature set. This approach aims to cut down training and recognition time by using fewer features.

Our dataset is divided into four subsets, based on data quantities and the features selected:

1. Numerous benign instances + 78 features for binary classification
2. Few benign instances + 78 features for multi-class classification
3. Numerous benign instances + 23 features for binary classification
4. Few benign instances + 23 features for multi-class classification

B. Model Architecture

Our study focuses on creating and comparing five different models for detecting DDoS network traffic: LSTM, BiLSTM, CNN, CNN-LSTM, and CNN-BiLSTM. Each model offers unique strengths in handling sequence data and extracting features, providing a thorough comparison of their effectiveness in identifying DDoS attacks.

The CNN model, renowned for its success in image processing, is now applied to DDoS network traffic for feature extraction. It aims to identify local features within the traffic, effectively differentiating between normal and DDoS attack patterns.

The LSTM model, designed for long short-term memory, is adept at managing long-term dependencies in sequential data, which makes it particularly good at recognizing the time-based patterns of DDoS attacks. The BiLSTM model expands on LSTM by processing information in both directions, offering a fuller understanding of sequence context and improving the accuracy of attack detection. To further refine our dataset's handling, we implement a Splitting Sequence operation with n_steps set to 4, allowing for a more effective capture of time-series features characteristic of DDoS attacks.

The CNN-LSTM and CNN-BiLSTM models combine convolutional networks' ability to extract features with the sequential data handling of LSTM networks. This integrated method enables the simultaneous analysis of local and global information, making these models particularly effective for dealing with complex DDoS attack situations.

Our study conducts a comparative analysis of the five models: LSTM, BiLSTM, CNN, CNN-LSTM, and CNN-BiLSTM, assessing their effectiveness in detecting DDoS network traffic. This comparison is designed to highlight the unique strengths and weaknesses of each model, offering insights into their best use cases and providing valuable guidance for real-world applications.

IV. Result and Analysis

Our study performed a two-stage experimental comparison with two feature datasets. First, we compared multi-class training models using datasets 2 and 4, which have fewer benign samples and 78/23 features, respectively. Then, we used datasets 1 and 3, with more benign samples and the same feature counts, for binary classification model comparisons.

We used the confusion matrix as the main tool to assess training outcomes, complemented by Accuracy, Precision, Recall, and F1-Score metrics for a detailed evaluation. This method provides insights into the strengths and weaknesses of each model across different data scenarios, enabling a thorough review of their performance and aiding in the selection of the most suitable model.

In the first phase of our experiments, using a dataset with fewer benign samples and 23 features, the BiLSTM model achieved the highest recall at 74%, outperforming the other models. Despite this, all models faced difficulties in precisely identifying some attack categories, leading to confusion in predictions. Figure 4 shows the confusion matrix for the BiLSTM model. In the next experiment, using a dataset with fewer benign samples and 78 features, the BiLSTM model again led the group with a 78% recall. As with the earlier trial, pinpointing certain attack categories proved challenging

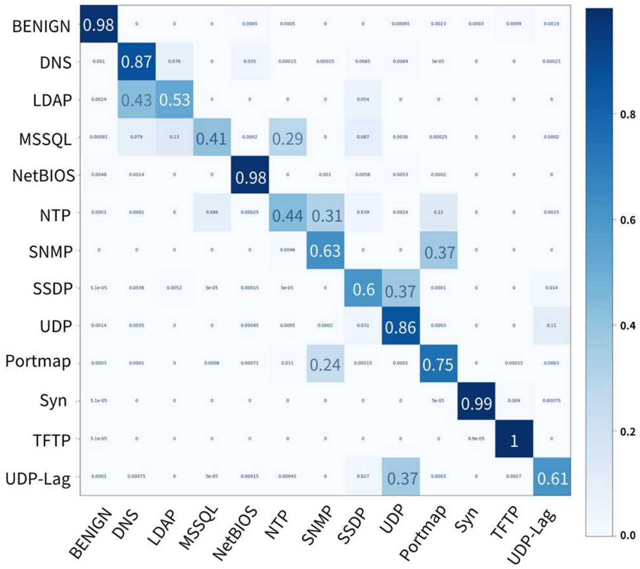


Figure 4. Confusion matrices for BiLSTM using 23 feature datasets

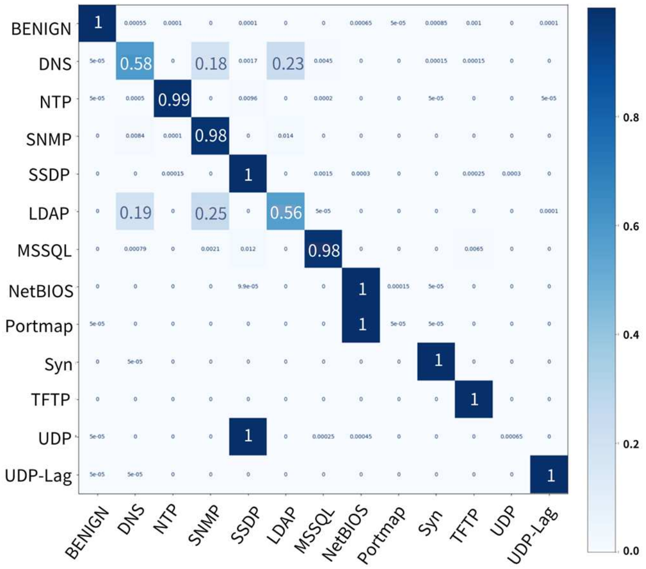


Figure 5. Confusion matrices for CNN-BiLSTM using 78 feature datasets.

because of their resemblance. Figure 5 displays the confusion matrix for the CNN-LSTM model.

Although the first two experiments showed confusion in identifying specific attack categories, it's important to note that this confusion was limited to the attack categories themselves. Consequently, we then applied binary classification to evaluate the models' ability to differentiate between normal and attack packets, choosing the top-performing CNN-LSTM model for this task. The results demonstrated that this model could accurately identify malicious packets with a prediction error rate of only about 0.5% for both 23 and 78 features, as depicted in Figure 6.

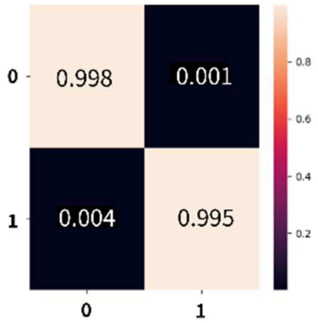


Figure 6. Confusion matrices for dichotomy.

The comprehensive results of our experiments are summarized in Table 5. Our findings confirm that using a CNN+LSTM method, which first extracts features with a CNN, delivers satisfactory outcomes even when training with a larger set of features. Moreover, our research shows that reducing the number of features to 23 still achieves comparable confusion matrix results to other studies, demonstrating efficiency without compromising performance. Despite the results not being exceptional overall, the consistent confusion across certain attack categories enables us to identify and report specific types of attacks to administrators. This consistency does not detract from our objectives. With binary classification, our accuracy nears perfection, ensuring no type of attack goes undetected.

Table 5. The comprehensive training results.

DataSet	Model	Accuracy	Precision	Recall	F1-Score
Dichotomy (23 features)	CNN+LSTM	1	1	1	1
Dichotomy (78 features)	CNN+LSTM	1	1	1	1
Taxonomy (23 features)	CNN	0.56	0.6	0.56	0.51
	LSTM	0.73	0.76	0.73	0.72
	BiLSTM	0.74	0.76	0.74	0.74
	CNN+LSTM	0.73	0.77	0.73	0.72
	CNN+BiLSTM	0.69	0.7	0.69	0.64
Taxonomy (78 features)	CNN	0.67	0.63	0.67	0.61
	LSTM	0.7	0.63	0.7	0.64
	BiLSTM	0.74	0.67	0.74	0.67
	CNN+LSTM	0.78	0.77	0.78	0.72
	CNN+BiLSTM	0.75	0.67	0.75	0.68

V. Conclusion & Future Works

Our study excels in binary classification, accurately distinguishing between normal and DDoS attack packets. This success shows our model's practical applicability in protecting OFH environments against security threats. Moreover, it can precisely identify specific DDoS attacks, enabling administrators to develop targeted response strategies quickly, thus bolstering network security. This adaptability enhances the model's real-world usefulness against diverse threats. Our research offers a valuable, practical solution in network security and insights for future studies.

Looking ahead, we plan to incorporate our IDS into xApps on the Near-Real Time RIC, using E2 or O1 interfaces to send packet feature data for enhanced detection and decision-making. This step will boost the automation and intelligence of the system, allowing the IDS to work more efficiently with other network management and security tools. This approach not only strengthens network security but also addresses the complex and evolving security needs of future networks. For DDoS attacks that are hard to distinguish, we will consider analyzing over 80 features with CICFlowmeter and extracting more packet features for better classification.

References

[1] O-RAN.WG4.CUS.0-R003-v12.00: “O-RAN Working Group 4 (Open Fronthaul Interfaces WG) Control, User and Synchronization Plane Specification”

[2] O-RAN.WG4.MP.0-R003-v12.00: “O-RAN Working Group 4 (Open Fronthaul Interfaces WG) Management Plane Specification”

[3] Open RAN Security Report May 2023: "Outcome from Quad Critical and Emerging Technology Working Group", National Telecommunications and Information Administration, United States Department of Commerce, 2023

[4] O-RAN.TIFG.E2E-Test.0-v04.00: "O-RAN Test and Integration Focus Group End-to-end Test Specification"

[5] I. Sharafaldin, A.H. Lashkari, and A.A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization", Proceedings of the *International Conference on Information Systems Security and Privacy*

[6] I. Sharafaldin, A.H. Lashkari, S. Hakak, and A.A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", Proceedings of the *International Carnahan Conference on Security Technology,* pp. 1-8, 2019

[7] A. Bashaiwth, H. Binsalleeh, and B. AsSadhan, "An Explanation of the LSTM Model Used for DDoS Attacks Classification", *Applied Sciences, 2023*

[8] H.C. Chu and C.Y. Yan, "DDoS Attack Detection with Packet Continuity Based on LSTM Model," Proceedings of the *IEEE Eurasia Conference on IOT, Communication and Engineering*, pp. 44-47, 2021

[9] A.S. Abdalla and V. Marojevic, "End-to-End O-RAN Security Architecture, Threat Surface, Coverage, and the Case of the Open Fronthaul", *arXiv - CS - Cryptography and Security, 2023*

[10] D. Dik and M.S. Berger, "Open-RAN Fronthaul Transport Security Architecture and Implementation", *IEEE Access*, vol. 11, pp. 46185-46203, 2023

[11] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open RAN security: Challenges and opportunities", *Journal of Network and Computer Applications*, vol. 214, 2023