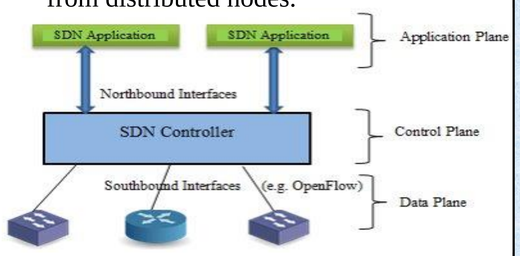
Intrusion Detection Framework For Distributed Denial of Service Attacks In Software Defined Network

Carmen Villalobos Garcia, Sathish Kumar
Washkewicz College of Engineering, Cleveland State University
c.villalobosgarcia@vikes.csuohio.edu

Introduction

- SDN separates the control plane from the data plane, centralizing network management in a software-based controller. The controller acts as the "brains" of the network, making decisions on how to forward packets. Offers new level of flexibility and control.
- Distributed Denial of Service (DDoS) is a malicious attack that disrupt the functioning of a computer network or service by overwhelming it with an excess of illegitimate traffic generated from distributed nodes.



Research Objective

- Detect and classify DDoS attacks in a SDN environment.
- Evaluation of performance of ML algorithms when detecting the DDoS attack in SDN environment.

Dataset and Preprocessing

Data cleaning.

Dataset contains 21 features.

Dataset for detecting DDoS vs Benign:

- Sampled dataset for training contains 400000 benign and 100000 DDoS.
- Sampled dataset for testing contains 200000 benign and 200000 DDoS.

Dataset for classifying specific DDoS type:

- Sampled dataset for training contains 400000 benign and 300000 DDoS.
- Sampled dataset for testing contains 150000 benign and 150000 DDoS.

Feature Reduction:

- PCA vs Fast ICA.

Data Standardization:

- Normalization of the dataset (0,1).

Methodology – Detecting DDoS attack

- Generation of benign traffic using iperf, ping and web-server.
- Generation of illegitimate traffic using hping3 tool.
  ICMP Flood, UDP Flood, TCP-SYN Flood.
- Collection of benign and illegitimate traffic in a csv file.
- Data preprocessing of the dataset.
- Detection approach for DDoS with ML algorithms,
  Logistic Regression, K-Nearest Neighbors, Support Vector Machine, Naive Bayes, Decision tree and Random Forest.
- Training and testing using ML algorithms to generate prediction model and confusion matrix.
- Use confusion matrix to get accuracy of the model.
- Both dataset models and real-time traffic captures have been utilized to evaluate the effectiveness of models in detecting DDoS traffic.

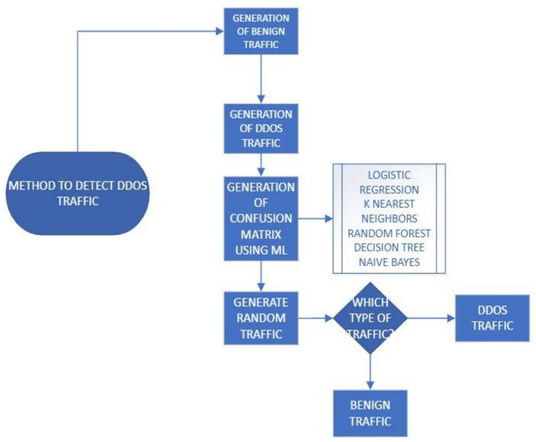
Methodology – Classifying DDoS attack type

Once we detect that the traffic is DDoS, we will need to check what type of protocol is.

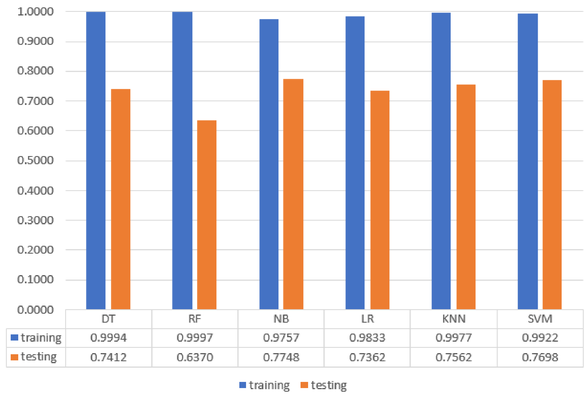
The IP protocol is the 7th feature that we collect.

- DDoS attack Performing ICMP Flood
  IP_PROTO = 1
- DDoS attack Performing UDP Flood
  IP_PROTO = 6
- DDoS attack Performing TCP-SYN Flood
  IP_PROTO = 17

DDoS Detection Process Overview

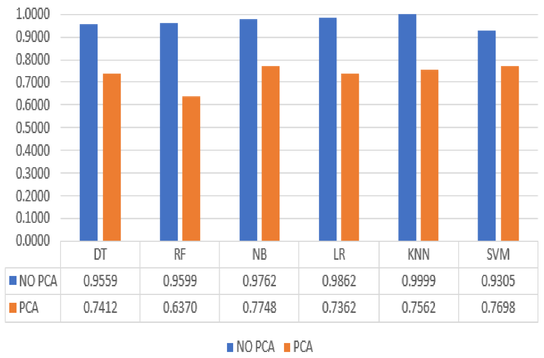


Evaluation Results for ML models in Detecting DDoS attack using 12 features



	DT	RF	NB	LR	KNN	SVM
training	0.9994	0.9997	0.9757	0.9833	0.9977	0.9922
testing	0.7412	0.6370	0.7748	0.7362	0.7562	0.7698

Evaluation Results for ML models in Detecting DDoS attack using 6 features (obtained from PCA)



	DT	RF	NB	LR	KNN	SVM
NO PCA	0.9559	0.9599	0.9762	0.9862	0.9999	0.9305
PCA	0.7412	0.6370	0.7748	0.7362	0.7562	0.7698

Evaluation of Specific Types of DDoS Attack Using the Best Performing Model (K-Nearest Neighbor)

Parameters	6	21	21	21
Normalization	Yes	Yes	Yes	Yes
PCA	Yes 3 components	Yes 12 components	Yes 18 components	No
UDP accuracy	1.0	0.83486	0.49378	1.0
ICMP accuracy	0.99996	1.0	1.0	1.0
TCP accuracy	0.99988	0.83746	0.53126	0.12288

Conclusions

- K-Nearest Neighbor is the best model when detecting and classifying different types of DDoS attacks.
- By selecting six carefully curated features: IP source, packet count, packets per second, packets per nanosecond, bytes per second, and bytes per nanosecond, the accuracy experiences a significant enhancement, achieving an average of 96.81%.
- PCA performs better than FastICA in identifying features.
- ML models have been tested through real time traffic capture, giving close to 100% effectiveness.
- Accuracy improves on balanced datasets.
- If a DDoS attack occurs in a SDN and isn't mitigated, the controller will be affected.

Future Work

- Mitigation of DDoS attack in SDN environment.
- Generation of different types of attack in SDN environment.
- Evaluation of attack detection model in different types of SDN controllers (POX, OpenDaylight, NOX, etc.) for DDoS attacks and different types of attacks.

Literature cited

- H. Bisht, M. Patra and S. Kumar, " Detection and Localization of DDoS attack during Inter-Slice Handover in 5G Network Slicing", 20th IEEE International Conference on Consumer Communications, January 2023
- Jeeva Chelladhurai, Pethuru Raj Chelliah and Sathish A.P. Kumar, "Securing Docker Containers from Denial of Service (DoS) Attacks" in 13th IEEE International Conference on Service Computing (IEEE SCC), pp. 856-859, 2016
- Kumari, K., Mrunalini, M. Detecting Denial of Service attacks using machine learning algorithms. J Big Data 9, 56 (2022). https://doi.org/10.1186/s40537-022-00616-0