

DDoS attack detection in SDN environment

Minor Project ESA (Team No: N11)

Team Members:

Madhukeshwar Hegde - 01fe18bcs107

Vinay S Itagi - 01fe18bcs256

Mayur S Javali - 01fe18bcs288

Rashmi - 01fe18bcs281

Under the Guidance of:

Ms. Pooja Shettar

KLE Technological University, Hubli

School of Computer Science and Engineering

Project Overview

- Domain/Problem Space :
 - Network Security
 - Security provided to a network from unauthorized access.
- Problem Definition :

To detect different Distributed Denial of Service(DDoS) attacks using deep learning based algorithms in Software defined networks (SDN) environment.

1. "Detection of DDoS Attacks in Software Defined Networks", [IEEE 2018]

- In this work, a method to detect DDoS attack with two level of security is proposed.
- The two classifier techniques, used are SVM and DNN.
- The results reveal that DNN performs better then SVM.

2. "Detection of DDoS in SDN Environment Using Entropy-based Detection", [Department of Electrical and Computer Engineering, California State Polytechnic University, Pomona]

- In this paper, the effects of DDoS attacks on a SDN environment is being analyzed and proposes an entropy-based approach to detect these attacks.
- The study uses the flexibility of OpenFlow protocol, and an OpenFlow controller (POX) to mitigate the attacks upon detection.

3. “A DDoS AttackDetection Method Based on SVM in Software Defined Network”.[2018]

- Authors presents a flexible modular architecture that identifies and mitigates LR-DDoS attacks in SDN settings.
- Results in this paper demonstrate the usefulness of their architecture in identifying and mitigating LR-DDoS attacks.

4. “A flexible sdn-based architecture for identifying and mitigating low-rate ddos attacks using machine learning” [IEEE 2020]

- The authors have proposed that Low-Rate DDoS (LR-DDoS) attacks are known to be difficult to detect, particularly in a software-defined network.
- The architecture uses six machine learning models i.e., J48, Random Tree, REP Tree, Random Forest, Multi-Layer Perceptron (MLP), and SVM.

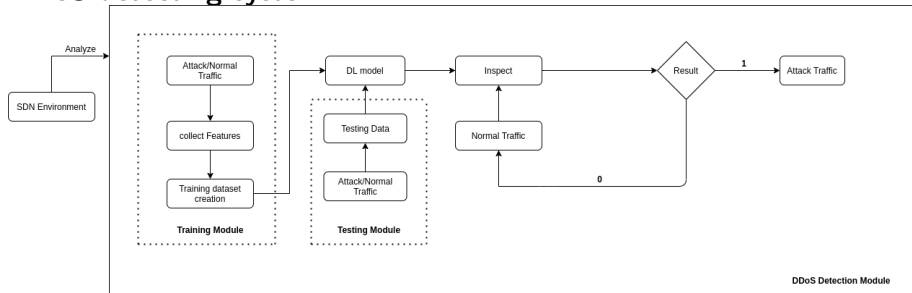
5. “ddos Deep-Defense: Identifying DDoS Attack via Deep Learning”. [2018]

- Authors proposed a deep learning-based DDoS attack detection approach. Deep learning model used to automatically extract high-level features from low-level ones and gain powerful representation and inference capabilities.
- In this paper the experimental results demonstrate that their model performs better than conventional machine learning models.
- Comparing the larger dataset to conventional machine learning, they reduced the error rate from 7.517percent to 2.103percent

Objectives

- To capture the real time traffic(normal and attack) in SDN environment.
- To extract suitable features using feature extraction techniques.
- To detect anomaly based attacks using Deep learning techniques.

DDoS detecting system :



Dataset Details

- Dataset Source/ Generation :
 - DDoS attack SDN dataset.
 - This dataset is created in mininet by creating different topologies and choosing a random topology for sending traffic between the hosts.
- Dataset suitability/ analysis :
 - This dataset consists total 23 features in which some are calculated and some are extracted from the switches.
- Selected Features :
 - Speed of source IP.
 - Standard deviation of flow packets.
 - Standard deviation of flow bytes.
 - Speed of flow entries.
 - Ratio of pair-flow entries.

Steps for collecting data

- 1 Begin
- 2 Send the traffic from two or more hosts to one of the target host.
- 3 Monitors flows of S1.
- 4 Store the flow in text file.
- 5 Convert text file to csv file.
- 6 Put the data of important individual attributes of csv to individual csv file for each attribute.
- 7 use the now created individual csv files to calculate the features.
- 8 Append the values of all the features to dataset.csv file (Final csv).
- 9 Add another attribute value to the file called "target" and add 0 to normal traffic and 1 if the data collected is from the attack.
- 10 Read the processed csv file.
- 11 Feed the processed csv file into trained model.
- 12 End Begin

Implementation

- Training module.
- Data capturing module.
- Testing module.
- DDoS attack detection module.

Results: Comparison of Accuracy and error rate

Table: Comparison of accuracy and Error rate

DL model	Bench Accuracy	Real-time Accuracy	Bench Error-rate	Real-time Error-rate
BRNN	97.17	99.21	2.83	0.79
FFNN	95.43	96.32	4.57	3.68

Results

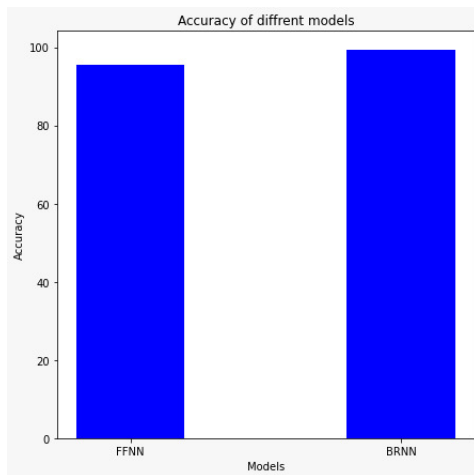


Figure: Accuracy graph

Results

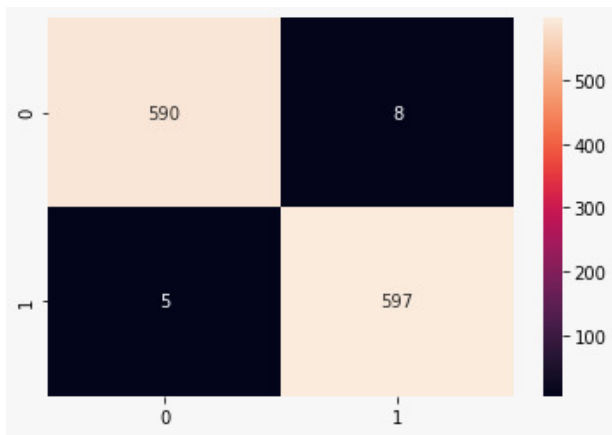
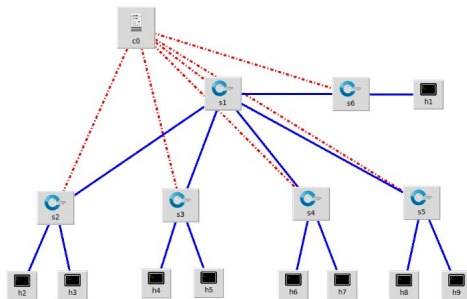


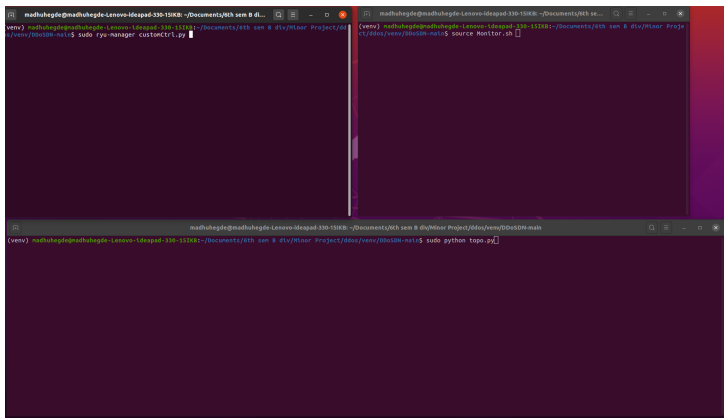
Figure: Confusion matrix for BRNN

Results: SDN environment



- Here we created a topology of 9 hosts and 6 switches and a controller.
- We used RYU controller.

Results:



The image displays three terminal windows from a Linux environment, showing the steps to set up a Ryu-based SDN environment. The first window shows the installation of Ryu and the creation of a custom controller. The second window shows the installation of the Ryu controller and the creation of a custom controller. The third window shows the installation of the Ryu controller and the creation of a custom controller.

```
madhuhegde@madhuhegde-Lenovo-Ideapad-330-15IKB: ~/Documents/4th sem B div/Minor Project/dds
(venv) madhuhegde@madhuhegde-Lenovo-Ideapad-330-15IKB:~/Documents/4th sem B div/Minor Project/dds
$ ./venv/00s0N-main$ sudo ryu-manager customctr/l.py

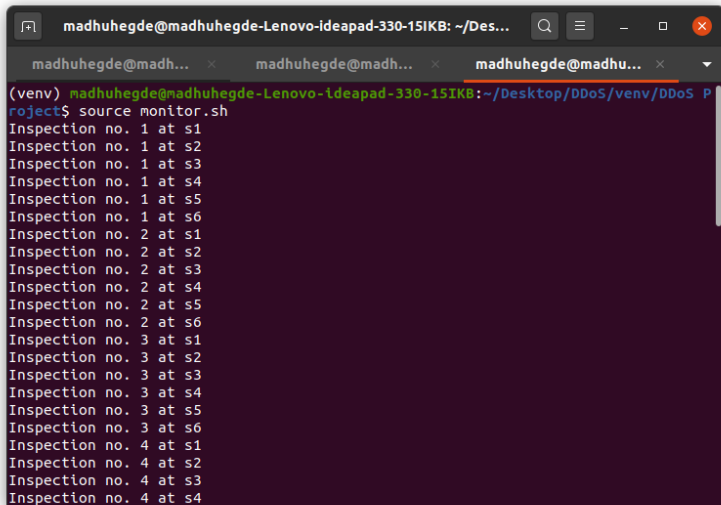
madhuhegde@madhuhegde-Lenovo-Ideapad-330-15IKB: ~/Documents/4th sem B div/Minor Project/dds/venv/00s0N-main
(venv) madhuhegde@madhuhegde-Lenovo-Ideapad-330-15IKB:~/Documents/4th sem B div/Minor Project/dds/venv/00s0N-main$ source Monitor.sh

madhuhegde@madhuhegde-Lenovo-Ideapad-330-15IKB: ~/Documents/4th sem B div/Minor Project/dds/venv/00s0N-main
(venv) madhuhegde@madhuhegde-Lenovo-Ideapad-330-15IKB:~/Documents/4th sem B div/Minor Project/dds/venv/00s0N-main$ sudo python topo.py
```

Results:

```
madhuhegde@madhuhegde-Lenovo-Ideapad-330-15IKb: ~/Documents/With sem B di...  
packet in 1 72:bb:3a:c2:dd:6f 33:33:00:00:00:02 1  
packet in 1 5e:1c:42:b0:b4:19 33:33:00:00:00:02 4  
packet in 6 90:2d:75:aa:fb:06 33:33:00:00:00:02 2  
packet in 6 72:bb:3a:c2:dd:6f 33:33:00:00:00:02 2  
packet in 6 5e:1c:42:b0:b4:19 33:33:00:00:00:02 2  
packet in 3 72:bb:3a:c2:dd:6f 33:33:00:00:00:02 1  
packet in 3 5e:1c:42:b0:b4:19 33:33:00:00:00:02 3  
packet in 2 90:2d:75:aa:fb:06 33:33:00:00:00:02 1  
packet in 2 72:bb:3a:c2:dd:6f 33:33:00:00:00:02 2  
packet in 2 5e:1c:42:b0:b4:19 33:33:00:00:00:02 1  
packet in 5 90:2d:75:aa:fb:06 33:33:00:00:00:02 3  
packet in 5 5e:1c:42:b0:b4:19 33:33:00:00:00:02 2  
packet in 4 90:2d:75:aa:fb:06 33:33:00:00:00:02 3  
packet in 4 72:bb:3a:c2:dd:6f 33:33:00:00:00:02 3  
packet in 2 72:06:e9:a5:5a:b7 a2:6e:dc:a9:1a:c1 2  
packet in 1 72:06:e9:a5:5a:b7 a2:6e:dc:a9:1a:c1 2  
packet in 6 72:06:e9:a5:5a:b7 a2:6e:dc:a9:1a:c1 2  
packet in 6 a2:6e:dc:a9:1a:c1 72:06:e9:a5:5a:b7 1  
packet in 1 a2:6e:dc:a9:1a:c1 72:06:e9:a5:5a:b7 1  
packet in 2 a2:6e:dc:a9:1a:c1 72:06:e9:a5:5a:b7 2  
packet in 6 a2:6e:dc:a9:1a:c1 72:06:e9:a5:5a:b7 1  
packet in 1 a2:6e:dc:a9:1a:c1 72:06:e9:a5:5a:b7 1  
packet in 2 a2:6e:dc:a9:1a:c1 72:06:e9:a5:5a:b7 1  
packet in 2 a2:6e:dc:a9:1a:c1 72:06:e9:a5:5a:b7 1  
packet in 1 72:06:e9:a5:5a:b7 a2:6e:dc:a9:1a:c1 2  
packet in 6 72:06:e9:a5:5a:b7 a2:6e:dc:a9:1a:c1 2  
Inspection no. 4 at s1  
Inspection no. 4 at s2  
Inspection no. 4 at s3  
Inspection no. 4 at s4  
Inspection no. 4 at s5  
Inspection no. 4 at s6  
Inspection no. 5 at s1  
Inspection no. 5 at s2  
Inspection no. 5 at s3  
Inspection no. 5 at s4  
Inspection no. 5 at s5  
Inspection no. 5 at s6  
Inspection no. 6 at s1  
Inspection no. 6 at s2  
Inspection no. 6 at s3  
Inspection no. 6 at s4  
Inspection no. 6 at s5  
Inspection no. 6 at s6  
Inspection no. 7 at s1  
Inspection no. 7 at s2  
Inspection no. 7 at s3  
Inspection no. 7 at s4  
Inspection no. 7 at s5  
Inspection no. 7 at s6  
Inspection no. 8 at s1  
Inspection no. 8 at s2  
madhuhegde@madhuhegde-Lenovo-Ideapad-330-15IKb: ~/Documents/With sem B di/Misc Project/DoS/venom/DoS Project  
64 bytes from 10.0.0.2: icmp_seq=13 ttl=64 time=0.067 ms  
64 bytes from 10.0.0.2: icmp_seq=14 ttl=64 time=0.071 ms  
64 bytes from 10.0.0.2: icmp_seq=15 ttl=64 time=0.099 ms  
64 bytes from 10.0.0.2: icmp_seq=16 ttl=64 time=0.100 ms  
64 bytes from 10.0.0.2: icmp_seq=17 ttl=64 time=0.076 ms  
64 bytes from 10.0.0.2: icmp_seq=18 ttl=64 time=0.096 ms  
64 bytes from 10.0.0.2: icmp_seq=19 ttl=64 time=0.072 ms  
64 bytes from 10.0.0.2: icmp_seq=20 ttl=64 time=0.049 ms  
64 bytes from 10.0.0.2: icmp_seq=21 ttl=64 time=0.089 ms  
64 bytes from 10.0.0.2: icmp_seq=22 ttl=64 time=0.067 ms  
64 bytes from 10.0.0.2: icmp_seq=23 ttl=64 time=0.067 ms  
64 bytes from 10.0.0.2: icmp_seq=24 ttl=64 time=0.051 ms  
64 bytes from 10.0.0.2: icmp_seq=25 ttl=64 time=0.088 ms  
64 bytes from 10.0.0.2: icmp_seq=26 ttl=64 time=0.064 ms  
64 bytes from 10.0.0.2: icmp_seq=27 ttl=64 time=0.060 ms  
64 bytes from 10.0.0.2: icmp_seq=28 ttl=64 time=0.059 ms  
64 bytes from 10.0.0.2: icmp_seq=29 ttl=64 time=0.082 ms  
64 bytes from 10.0.0.2: icmp_seq=30 ttl=64 time=0.084 ms  
64 bytes from 10.0.0.2: icmp_seq=31 ttl=64 time=0.060 ms  
64 bytes from 10.0.0.2: icmp_seq=32 ttl=64 time=0.066 ms  
64 bytes from 10.0.0.2: icmp_seq=33 ttl=64 time=0.089 ms  
64 bytes from 10.0.0.2: icmp_seq=34 ttl=64 time=0.097 ms  
64 bytes from 10.0.0.2: icmp_seq=35 ttl=64 time=0.078 ms
```

Results:Normal traffic



A terminal window titled 'madhuhegde@madhuhegde-Lenovo-ideapad-330-151KB: ~/Des...' displays the output of a script. The prompt is '(venv) madhuhegde@madhuhegde-Lenovo-ideapad-330-151KB: ~/Desktop/DDoS/venv/DDoS P roject\$'. The command 'source monitor.sh' has been executed, resulting in 16 lines of output. Each line represents an inspection at a specific stage (s1, s2, s3, s4, s5, s6) for a given number (1, 2, 3, 4). The output shows a sequence of inspections for each number, with the first inspection for each number occurring at s1 and subsequent inspections occurring at s2, s3, s4, s5, and s6.

```
(venv) madhuhegde@madhuhegde-Lenovo-ideapad-330-151KB: ~/Desktop/DDoS/venv/DDoS P roject$ source monitor.sh
Inspection no. 1 at s1
Inspection no. 1 at s2
Inspection no. 1 at s3
Inspection no. 1 at s4
Inspection no. 1 at s5
Inspection no. 1 at s6
Inspection no. 2 at s1
Inspection no. 2 at s2
Inspection no. 2 at s3
Inspection no. 2 at s4
Inspection no. 2 at s5
Inspection no. 2 at s6
Inspection no. 3 at s1
Inspection no. 3 at s2
Inspection no. 3 at s3
Inspection no. 3 at s4
Inspection no. 3 at s5
Inspection no. 3 at s6
Inspection no. 4 at s1
Inspection no. 4 at s2
Inspection no. 4 at s3
Inspection no. 4 at s4
```

Results: Detecting attack traffic

```
madhuhegde@madhuhegde-Lenovo-ideapad-330-15IKB: ~/Documents/6th se...  
Inspection no. 11 at s5  
Inspection no. 11 at s6  
Inspection no. 12 at s1  
Inspection no. 12 at s2  
Inspection no. 12 at s3  
Inspection no. 12 at s4  
Inspection no. 12 at s5  
Inspection no. 12 at s6  
Inspection no. 13 at s1  
Network is under attack  
Inspection no. 13 at s2  
Network is under attack  
Inspection no. 13 at s3  
Inspection no. 13 at s4  
Inspection no. 13 at s5  
Inspection no. 13 at s6  
Network is under attack  
Inspection no. 14 at s1  
Network is under attack  
Inspection no. 14 at s2  
Network is under attack  
Inspection no. 14 at s3  
Inspection no. 14 at s4  
Inspection no. 14 at s5  
Inspection no. 14 at s6  
Network is under attack
```

References



P. S. Hiremath Karan B. V, Narayan D. G. "Detection of DDoS Attacks in SoftwareDefined Networks". pages 6(6):265–270, 2018.



@21Xiaolin Li Large-scale Intelligent Systems Laboratory University of Florida†Zhejiang Gongshang University Xiaoyong Yuan, Chuanhuang Li†. "ddos Deep-Defense: Identifying DDoS Attack via Deep Learning". pages 8(8):1–8, 2018.



@21Brian Urbina Department of Electrical Tamer Omar, Anthony Ho and PomonaComputer Engineering, California State Polytechnic University. "Detection of DDoSin SDN environment using Entropy-based detection". pages 7(6):1–6, 2019.



@21Feng Xiang Zhixin Sun Yuhua Xu, Houtao Sun. "Efficient DDoS Detection Based onK-FKNN in Software Defined Networks". pages 7(6):160536 – 160545, 01 November2019.



@21Jian Zhu Luting Feng Ling Song Jin Ye, Xiangyang Cheng. "A DDoS AttackDetection Method Based on SVM in Software Defined Network". pages 8:1–8, 24April 2018.

Thank You