Research paper analysis

Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques

Overview

- Abstraction
- Introduction
- Related Work
- Proposed Work
  a. Machine Learning
  b. DDoS attack identification
- Experimental Setup
- Performance Metrics
- Conclusion

Abstraction

Software-defined network (SDN) is a network architecture that used to build, design the hardware components virtually. SDN is a good approach but still is vulnerable to DDoS attacks.

They propose a machine learning technique namely Decision Tree and Support Vector Machine (SVM) to detect malicious traffic.

Their test outcome shows that the Decision Tree and Support Vector Machine (SVM) algorithm provides better accuracy and detection rate.

Back to Overview

Introduction

Back to Overview

SOFTWARE-DEFINED NETWORK (SDN)

Three Planes

- Data Plane
  - carries the network traffic based on the decision made by controller.
- Control plane
  - decides the flow of traffic by computing the routing tables.
- Application plane
  - manages the other applications like load balancer, firewalls, Quality of Service (QoS) applications etc.

SDN cont...

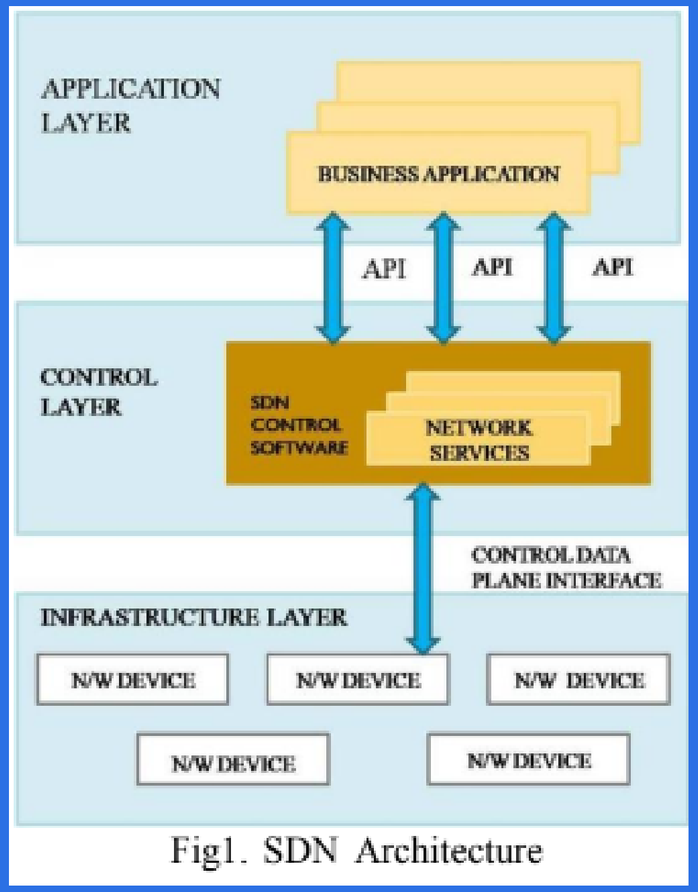


Fig1. SDN Architecture

Back to Overview

CONTROL LAYER

- Brain of the SDN architecture
- Since huge amount of traffic is passing through the controller, proper security mechanism is essential to analyze and identify suspicious traffic.

- They propose machine learning-based mechanism to identify the malicious activities in the SDN by investigating the traffic features.

Related Work

Back to Overview

ANALYSIS

RANDOM FOREST, NAIVE BAYES, KNN, NEURAL NETWORK, SVM, SOM.

KNN ALGORITHM

PREDICTION RATE OF 0.912

K-MEANS – HYBRID FEATURE SELECTION (SKM-HFS)

PERFORMANCE LEVEL OF 80%.

SVM ALGORITHMS

ACCURACY OF 0.998.

Proposed work

Back to Overview

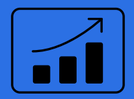
SVM and Decision tree algorithm to detect the attacks due to its accurate classification and less complexity.

Volume-based attacks	Protocol Attacks	Application Layer attacks
• UDP floods • ICMP floods which is mainly used to drench the internet pipe of targeted server	• SYN flood • fragmented packet • ping of death • smurf DDoS which mainly focus on extracting the server resources	GET/POST floods which focus on web applications and its goal is to crash the web server.

Proposed work

Machine Learning

Back to Overview



SVM

SVM is a machine learning technique supervised and used for the purpose of classification and regression.

Compared with other machine learning methods, SVM is more stable.

DECISION TREE

The decision tree is used for the classification of different traffic and to differentiate between normal and malicious traffic.

DATASET

- Training data
- Testing data

Proposed work

Back to Overview

DDoS attack identification

INITIAL PHASE	the dataset is divided into training and test dataset
FEATURE EXTRACTION PHASE	essential features are identified and selected for further detection process.
THIRD PHASE	dataset is passed through the SVM classifier and Decision tree module.
CLASSIFIER OUTPUT	Classifiers output the traffic dataset into two classes either attack or normal based on the flag value (0 or 1). In case of attack instance (flag=1), it alerts the controllers to drop the particular flow from the flow table. Otherwise, controller will formulate the routing path for the normal traffic packets
FORWARDING	The controller will send the forwarding table to process such payload whenever the DDoS issue is detected through using SVM classifier and decision tree. The SVM has high robust that it uses a kernel trick technique to gives out the possible outputs.

EXPERIMENT SETUP

- **MININET**

  standard simulation tool

- **100 HOSTS, 9 SWITCHES, AND 3 CONTROLLERS.**

During SYN flooding attack, one host is assigned as victim and 4 hosts as attacker. In each case, the traffic will be generated towards the data plane devices and the traffic flow information will be manually collected from each switch.

- **KDD99 DATASET**

  for training and testing the proposed model.

Back to Overview

Performance Metrics

Performance of their proposed work is analyzed using precision, recall, accuracy and f-measure metrics are used.

The SVM has an 80 percent of precision and recall whereas the decision tree is slightly differing in both precision and recall. SVM is more precise than the decision tree.

Algorithm	Accuracy Rate
Decision Tree	0.78
SVM	0.85

Fig 5. Accuracy rate

Fig 7 Recall of machine learning algorithms

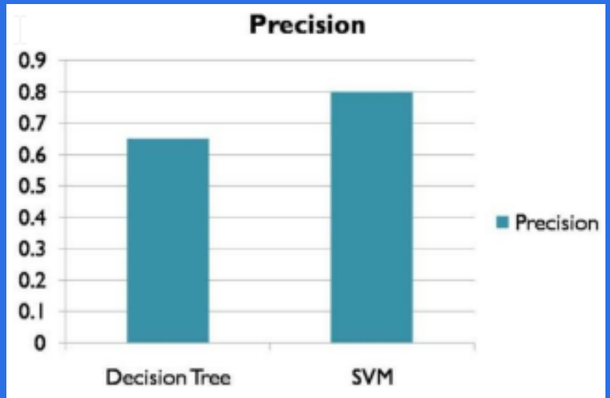


Fig. 6 Precision of machine learning algorithms

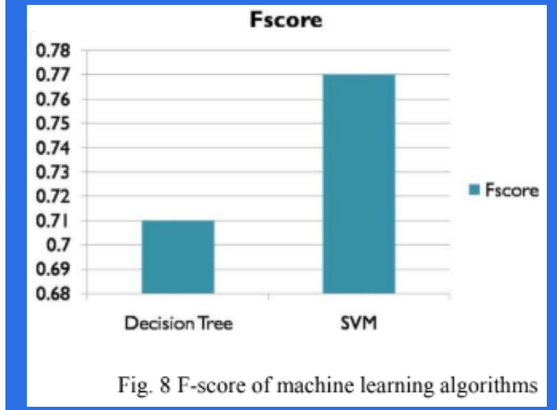
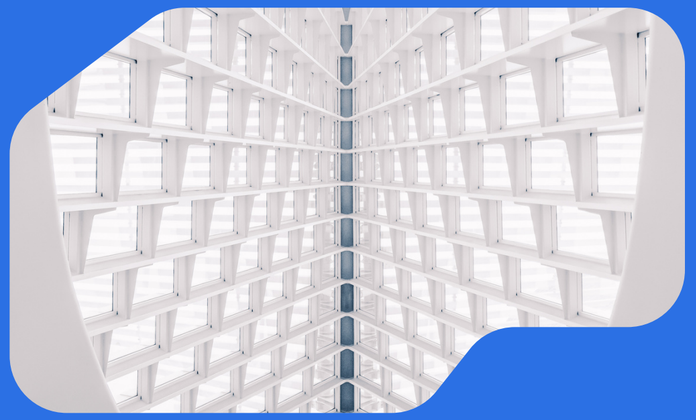


Fig. 8 F-score of machine learning algorithms

Back to Overview

CONCLUSION AND FUTURE WORK

Back to Overview



SVM AND DECISION TREE ALGORITHM

used to distinguish between normal and malicious traffic data.

SVM WORKS BETTER

Their experimental data shows that, SVM
works better than Decision tree technique in their simulated environment.

FUTURE TARGET

They plan to implement Advanced Support Vector Machine (ASVM) to detect DDoS attacks by analyzing the kernel vectors.

References

Back to Overview

Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques
- 2021 International Conference on Computer Communication and Informatics (ICCCI -2021), Jan. 27 - 29, 2021, Coimbatore, INDIA

Authors

K.Muthamil Sudar
k.muthamilsudar@klu.ac.in

M. Beulah
beulahlakshmi@gmail.com

P.Deepalakshmi
deepa.kumar@klu.ac.in

P.Nagaraj
nagaraj.p@klu.ac.in

P. Chinnasamy
chinnasamyponnusamy@gmail.com

Q&A Session

THANK YOU FOR LISTENING!

Back to Overview