2 Days International Workshop on Cyber-Physical Systems Security
at
Indian Institute of Information Technology Allahabad

Detection and Mitigation of DDoS Attack in SDN

By

Dr. Shashank Srivastava

(Associate Professor)

MNNIT Allahabad

21st and 22nd August 2023

Agenda

- Introduction
- Cyber Physical Systems (CPS)
  - Components of CPS
  - CPS Security
- DDoS Attack
  - Evolution of DDoS Attack
  - History of DDoS Attack
  - Types of DDoS Attack
- Limitations of Traditional Networks
- Software Defined Networking (SDN)
  - SDN as a solution to DDoS attack
  - Features Making SDN Vulnerable to DDoS
  - SDN Layered Architecture
  - Need for SDN
  - Security Challenges in SDN

- DDoS Detection and Mitigation Challenges
- Roadmap for DDoS App Creation
- DDoS Solution: Tools & Techniques
- Dataset Generation
- Detection and Mitigation flow module
- DDoS Detection features
- Feature Selection Techniques
- Detection and Mitigation Application
- Conclusion
- References

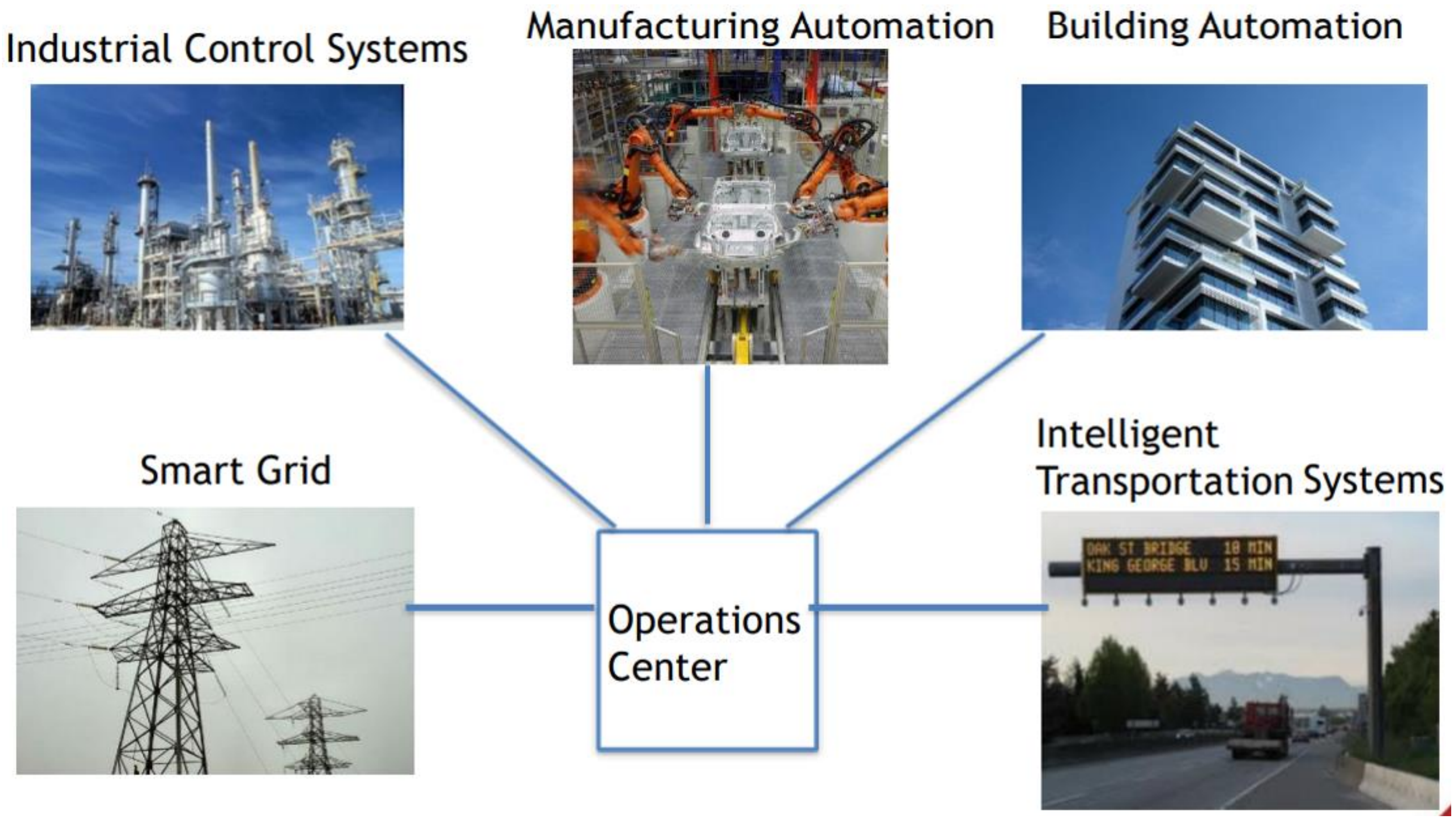
Introduction

- **Problem:** DDoS Attack Detection and Mitigation
- **Deliverable:** DDoS Detection & Mitigation Application for SDN Controller

This presentation is based on the outcome of research funded by
DST - Interdisciplinary Cyber Physical Systems

Project Staff: Naziya Aslam

Cyber Physical Systems



Industrial Control Systems

Manufacturing Automation

Building Automation

Smart Grid

Operations Center

Intelligent Transportation Systems

Fig: Smart Physical Infrastructures

Component of CPS

- Physical Components
- **Communication Component**
- Computational Component

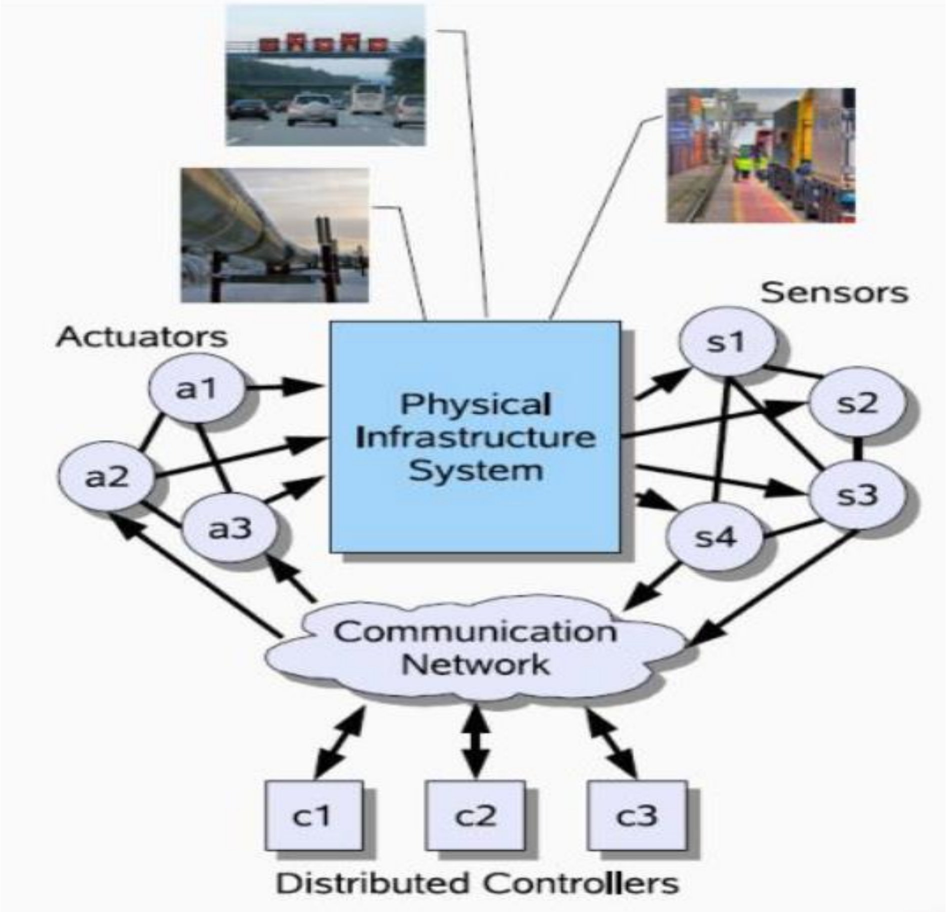
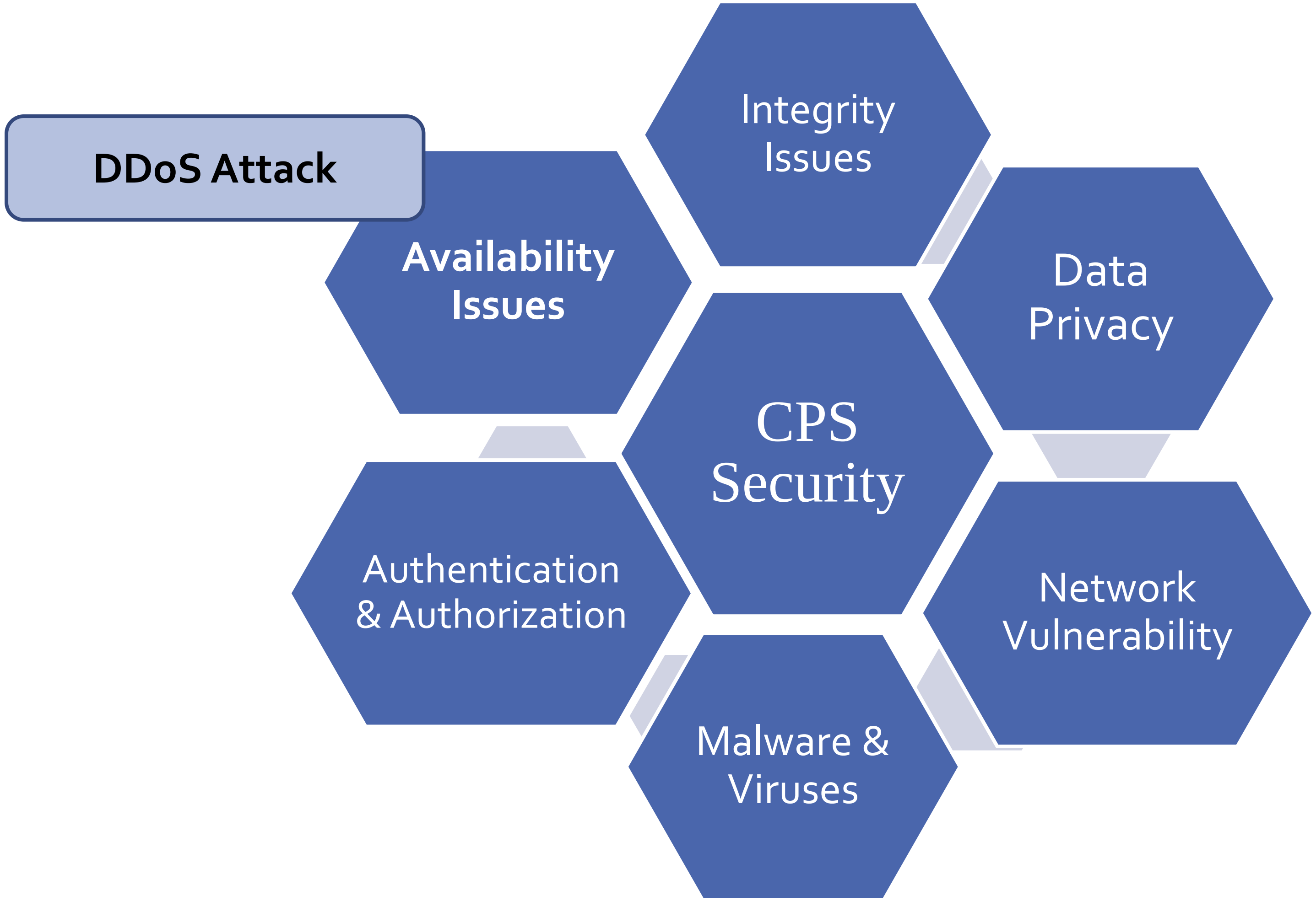


Fig: **CPS Components**

https://www.cybok.org/media/downloads/Cyber-Physical_Systems_Security_KA_webinar_-_slides.pdf

Cyber Physical System Security



DDoS Attack

- Attackers bombard their target with a massive amount of requests or data exhausting its **network (Bandwidth)** or **computing resources** and preventing legitimate users from having access.
- Considered as most destructive attack [1].
- Source of traffic distributed over a large span.
- Detection & Mitigation is hard and time consuming.

Evolution of DDoS Attack

- The first ever DoS attack occurred in **1974** and was carried out by David Dennis, a 13-year-old student at the University of Illinois Urbana-Champaign.
- He wrote a program that would send the “ext” command to many PLATO terminals at the same time. One morning, he went over to CERL and tested his program; it resulted in all 31 users having to power off at once.

History of DDoS Attack

- **1998:** Cybercriminals used **Smurf attacks**, which leveraged the ICMP to prompt other servers to ping a target
- **1999: Trinoo bot**, made of **227 infected Solaris servers**, was used to attack the University of Minnesota
- **2000:** 15-year-old boy, brought down major corporations, including Amazon, eBay, Yahoo!, and Dell
- **2005: 8 Gbps** DDoS attack traffic hit Worldwide Infrastructure Security Report (WISR)
- **2011:** Sony fell victim to a massive DDoS attack
- **2016:** A massive DDoS attack (**Mirai Botnet**) left much of the internet inaccessible on the U.S. east coast

Last 5 years Major DDoS Attacks

S. No.	Ref.	Year	Attack target	Attack rate	Description
1.	[3]	Feb 2023	USA-based NFL Super Bowl weekend	71 million rps	NFL Super Bowl weekend in the United States in February 2023, hundreds of hyper-volumetric DDoS attacks with 71 million requests per second were launched
2.	[4]	June 2022	Cloud Armor customer	46 million rps	A Cloud Armor customer was hit by DDoS attack of 46 million requests per second
3.	[5]	June 2022	Customer website	26 million rps	A HTTP DDoS attack of 26 million targeting the customer websites was mitigated by Cloudflare
4.	[6]	August 2021	Azure customer	2.4 Tbps	DDoS attack of 2.4 Tbps affected Azure cloud computing service's customer that lasted for 10 minutes
5.	[7]	February 2020	Customer of AWS	2.3 Tbps	One of the customer of Amazon Web Services suffered a massive DDoS attack of 2.3 Tbps
6.	[8]	April 2019	Client of Imperva	580 pps	One of the client of Imperva faced DDoS attack peaked at 580 million packets per second

Types of DDoS attack

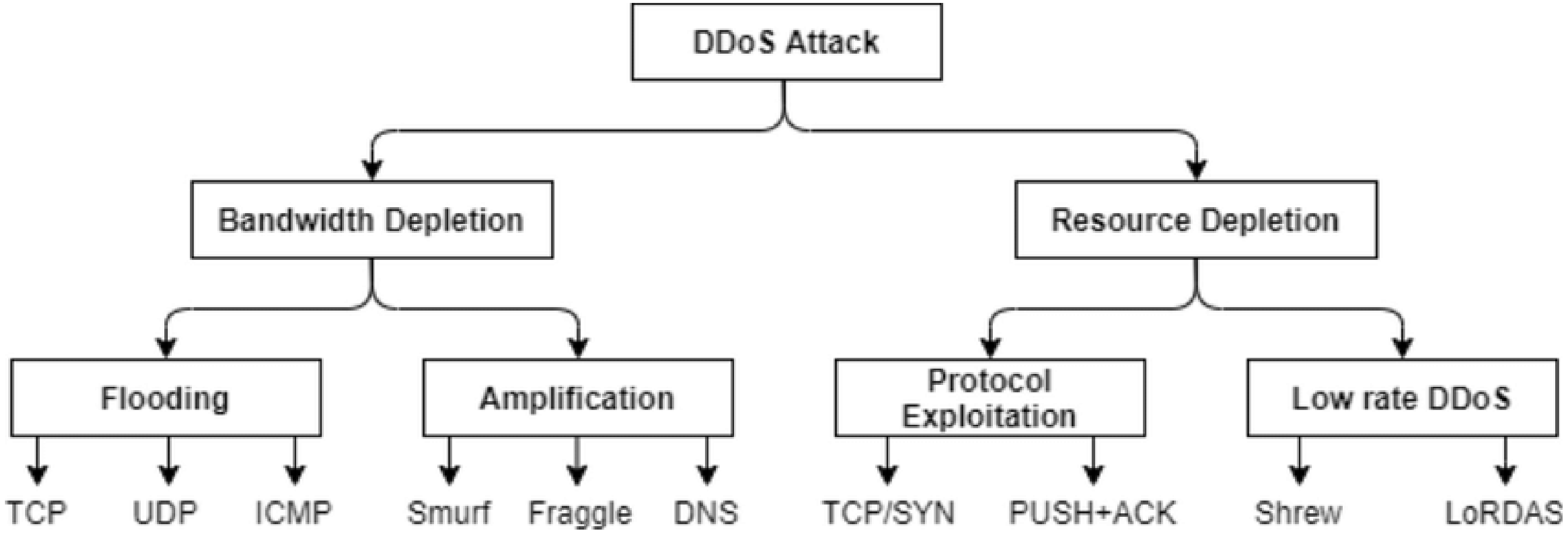


Fig: Types of DDoS attack [2]

Limitations of Traditional Networks

- Technology was not designed keeping today in mind
  - Massive Scalability
  - Multi Tenant Networks
  - Virtualization
  - Mobility (Users/Devices/VM)
- Difficult to configure correctly (consistency)
- Difficult to add new features (upgrades)
- Difficult to debug (look at all devices)

SDN (Software Defined Networking)

- **SDN as a solution**
  - Jay Turner [9], declared **2017 as the year of widespread SDN** adoption and DDoS attack mitigation
  - New approach for **network programmability**.
  - Concept of **separation** between a controlled entity and a controller entity.
  - The controller manipulates the controlled entity via an interface.
  - An administrator can shape traffic from centralized control.
  - Emphasizes the role of software in running networks

SDN as a solution to DDoS attack

- **Features Making SDN Resilient to DDoS**

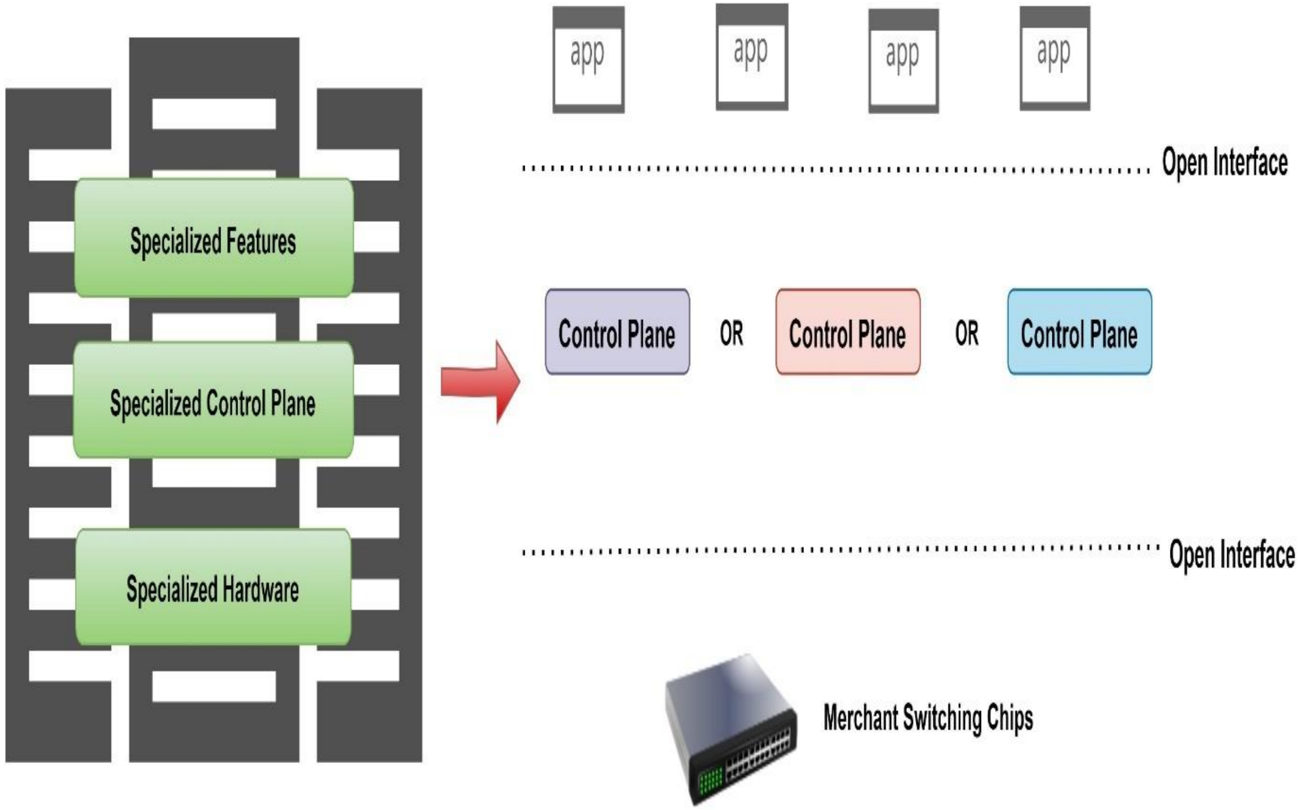
  - **Centralized monitoring of anomalous traffic** - All the anomalous activities going on in the network are observed by the controller.

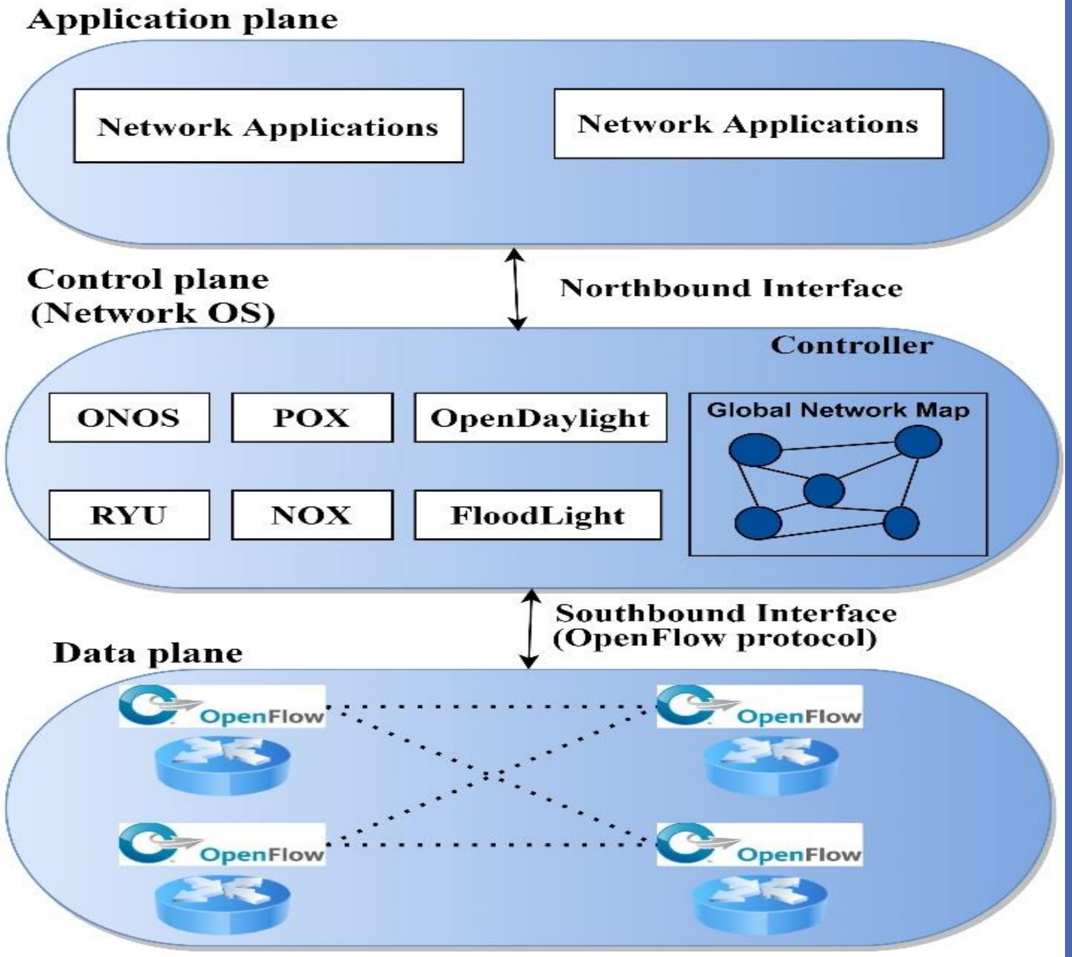
  - **Programmable configuration** - Whenever any malicious behavior is detected in the network, new programs are configured immediately to deal with the anomalies.

Features Making SDN Vulnerable to DDoS

- **Limited memory -** SDN switches have limited space of memory in their flow tables.
- **Decoupling of control and data plane -** An attacker can disturb the communication among the planes by implementing DDoS.
- **Dumb switches -** Switches rely on the controller for taking an appropriate action to forward packets. This may reduce the performance of controller and control plane bandwidth because of a large amount of traffic.

Software Defined Network :Disaggregation of Network Industry and Network Planes





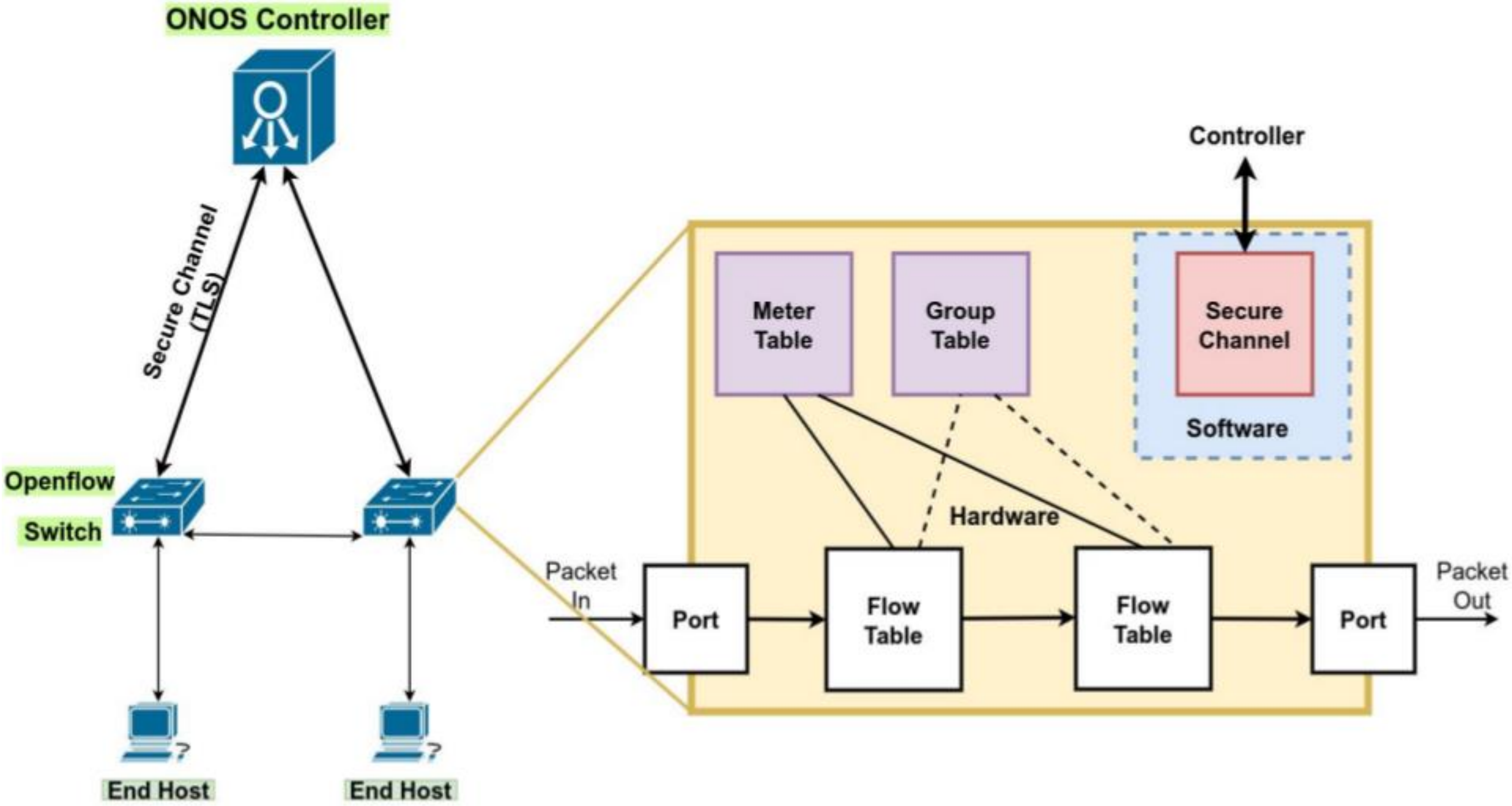
Need For SDN

- Facilitate innovation in network
- Layered architecture with standard Open interfaces
- Experiment and research using non-bulky, non-expensive equipment
- More accessibility since software can be easily developed by more vendors
- More flexibility with programmability
- Ease of customization and integration with other software applications

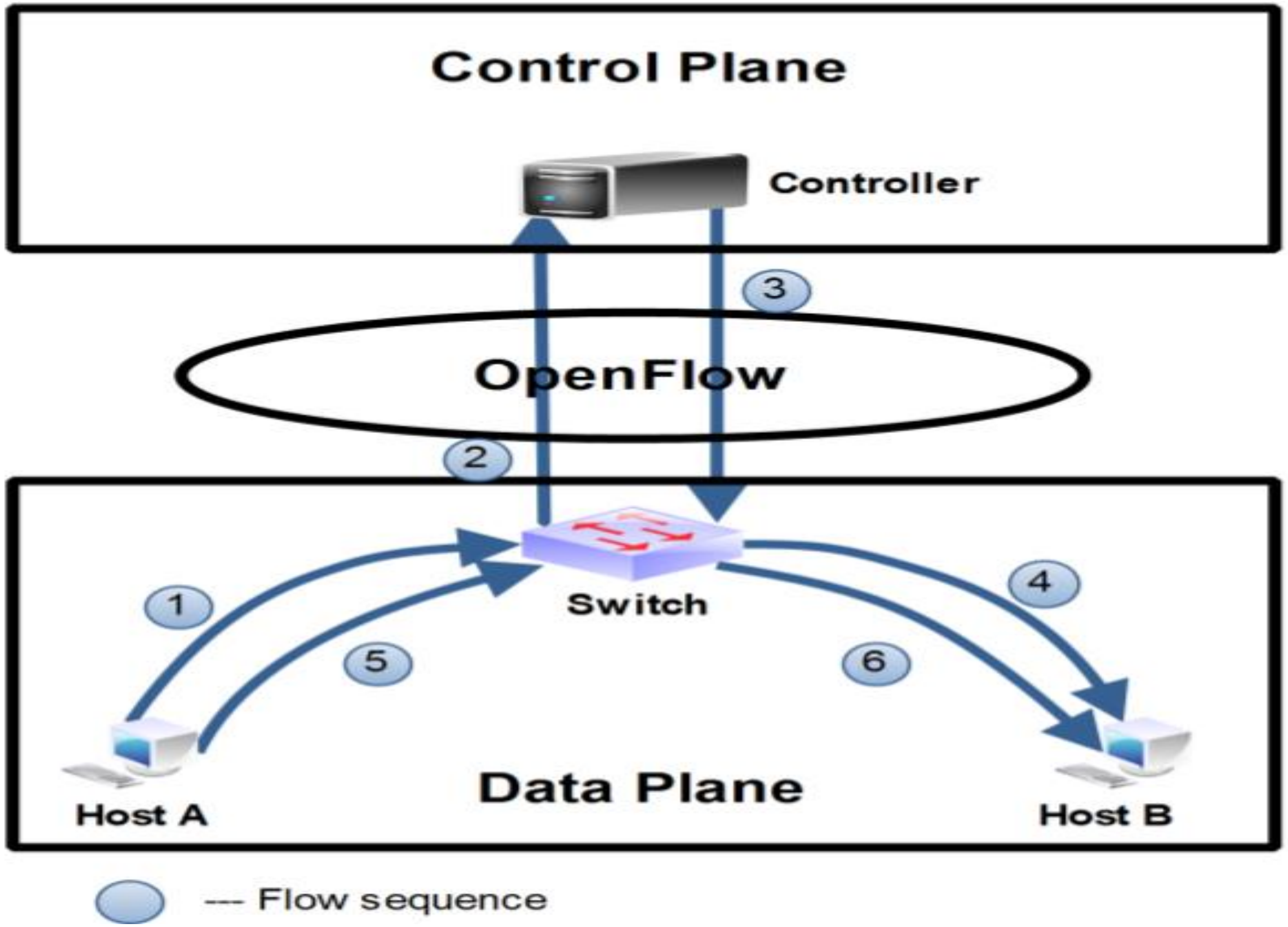
OpenFlow Protocol

- For the southbound interface of SDN.
- Leading SDN communication protocol.
- Decouples control and data plane by giving controller the ability to install flow rules on switches.
- Hardware or software switches can use OpenFlow.
- Separates switch programming from underlying hardware.

OpenFlow switch working



Data flow in SDN



Security challenge in SDN

- Security risks
  - Controller hijacking
  - Data modification
  - ARP poisoning
  - **Distributed Denial of service attack**

Biggest security concern

SDN’s control being centralized is prone to being threatened with **Distributed Denial of Service (DDoS) attack**

DDoS Detection and Mitigation Challenge

1. Selecting set of features for optimal classification of DDoS attack traffic and normal traffic
2. Unavailability of standard SDN specific dataset
3. Early mitigation of DDoS attack is necessary to reduce impact on end users
4. Distinguishing network traffic during congestion and network traffic during DDoS attack
5. Unavailability of detection and mitigation application for SDN on ONOS controller

Roadmap for DDoS App Creation

1. Identified various possibilities of DDoS attacks in SDN environment with the help of attack tree and an attack model.
2. Analyzed the traffic pattern of various kinds of DDoS attack through performing real time attack in our lab environment.
3. Finding set of features for optimal classification of traffic pattern as DDoS attacks and normal traffic.
4. Develop a system model that can distinguish between heavy loads of legitimate traffic in network from that of DDoS attacks.
5. Built DDoS detection and mitigation engine based on machine learning algorithms and integrate the engine in the SDN controller.
6. Implemented the proposed system model, and verified the use of detection model with the SDN controller for handling the attacks at initial phase itself and to lower the risk for legitimate users.
7. Identified the sources of DDoS attack.

DDoS Solution: Tools & Techniques

- Created an ONOS Flood Defender Application
- Detection by ML algorithms
- Mitigation by tracebacking technique
- **SDN controller:** ONOS
- **Dataset size:** 10 lakh (60% normal traffic, 40% attack traffic)
- **Attack performed:** HTTP flood, TCP SYN flood, UDP flood, ICMP flood
- **Topology taken:** GEANT Zoo topology
- **Emulator:** Mininet
- **Normal traffic generation tool:** D-ITG
- **Attack traffic generation tool:** hping3, mausezahn, HULK (HTTP Unbearable Load King)

System Setup

- **System Configuration:** PARAM SHAVAK DLGPU system running the 64-bit LTS version of Ubuntu 18.04, 96 GB RAM, Dual Socket Intel Skylake Processor with 2 GHz × 40 frequency

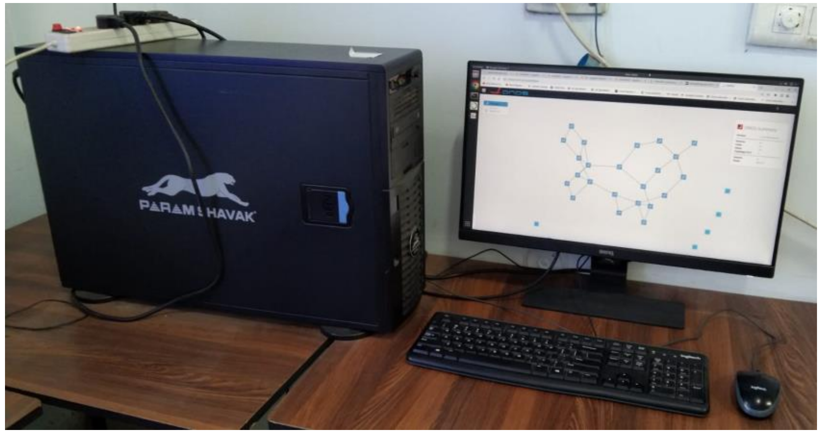


Fig: **PARAM Shavak DL-GPU High Performance Computer**

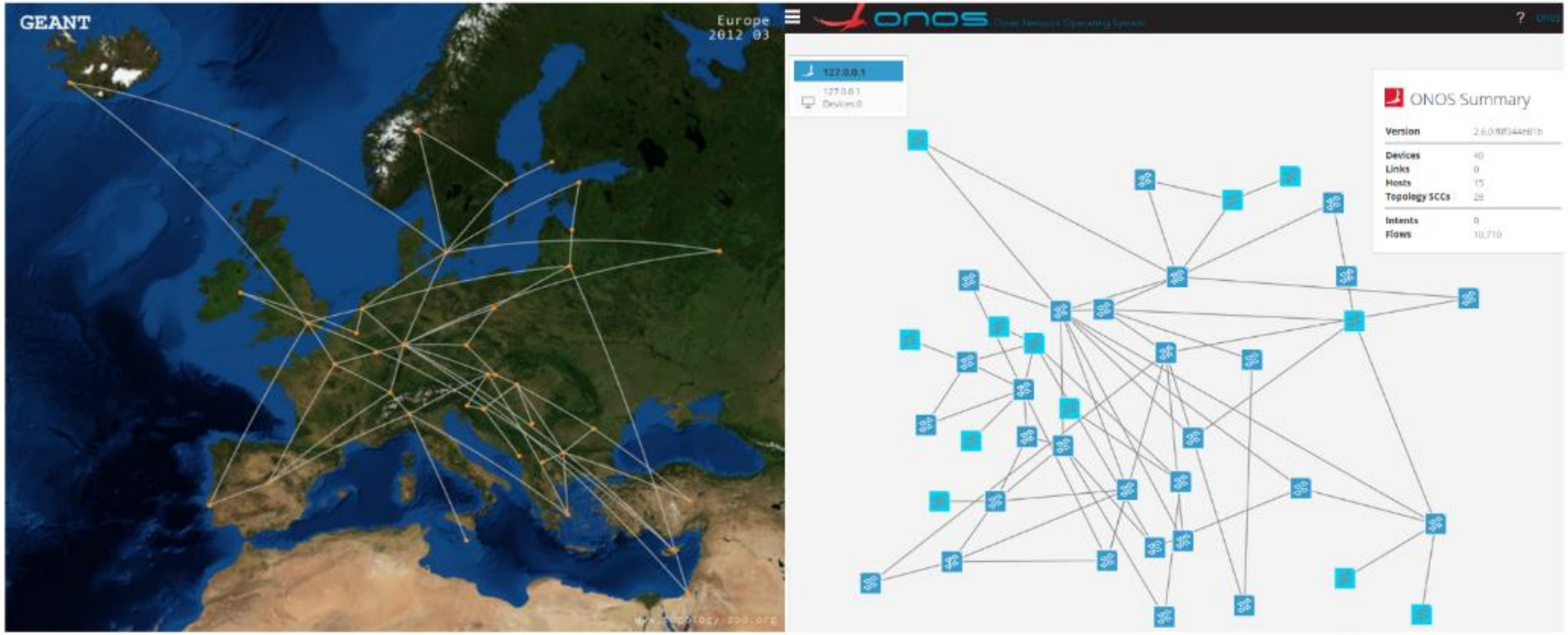
Git hub link: https://github.com/naziya22/Intelligent-detection-and-mitigation-of-DDoS-attack-in-SDN.git

Dataset Comparison

Dataset and Year	Labeled Data	Realistic Traffic	No. of Features	Format	Network Type	Attack Variety	Network Environment
KDD'99, 1998	Yes	No	41	Other	Small	Yes	Traditional
Kyoto, 2006-2009	Yes	Yes	24	Other	Honey pots	No	Traditional
NSL-KDD, 2009	Yes	No	41	Other	Small	Yes	Traditional
CICIDS2017, 2017	Yes	Yes	83	Packet, Flow	Small	Yes	Traditional
CSE-CIC-IDS2018, 2018	Yes	Yes	83	Packet, Flow	Small	Yes	AWS Platform
InSDN, 2020 3 3 3	Yes	Yes	83	Packet, Flow	Small	Yes	SDN Network
Our Dataset, 2023	**Yes**	**Yes**	**11**	**Packet, Flow**	**Large**	**Yes**	**SDN Network**

Table: Qualitative comparison of our dataset with public datasets

Topology



ONOS Summary

Version	2.6.0.f8f344e81b
Devices	40
Links	0
Hosts	15
Topology SCCs	28
Intents	0
Flows	10,710

(a) GEANT topology

(b) Mininet implementation of GEANT

Detection and Mitigation flow module

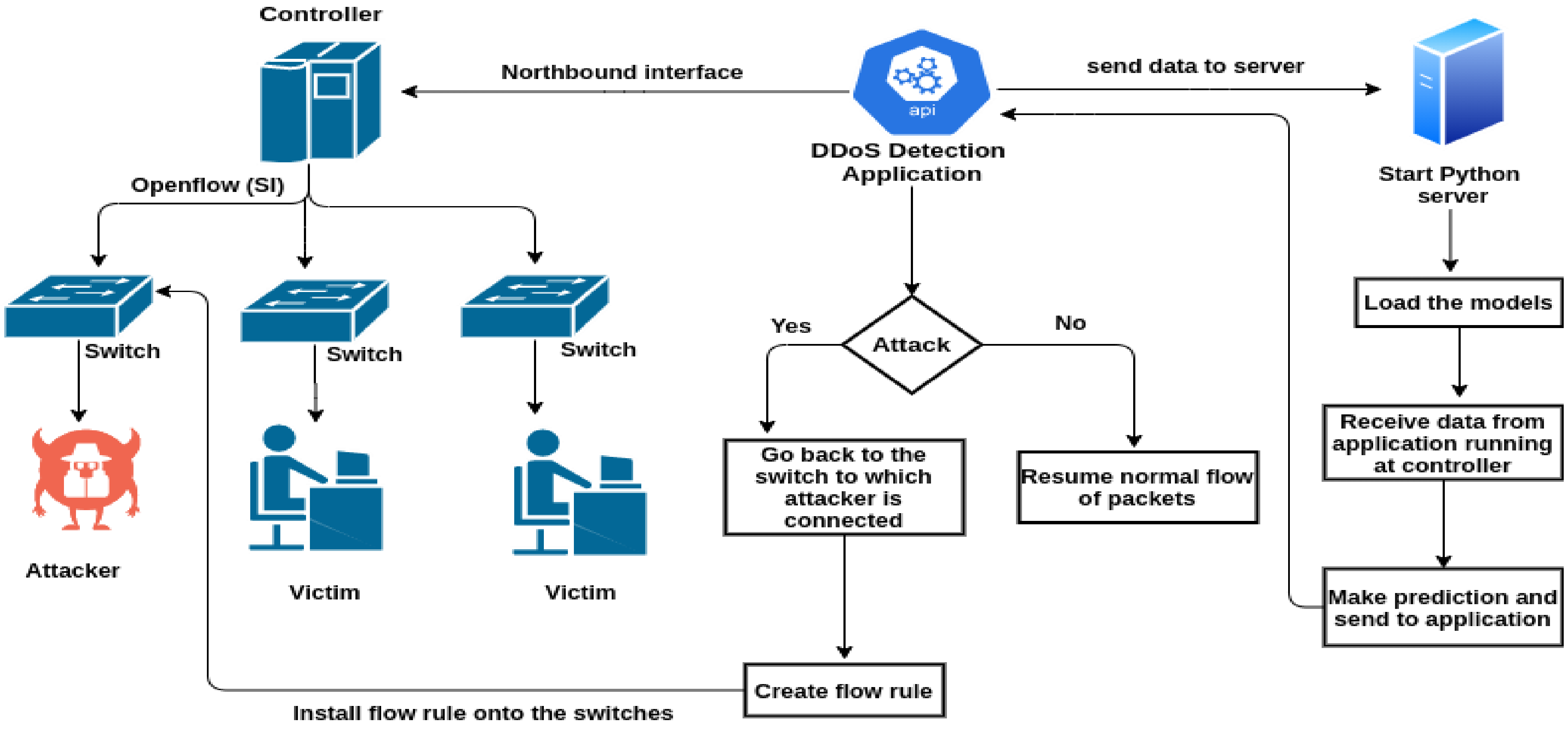

Controller
Northbound interface
api
DDoS Detection Application
send data to server
Start Python server
Openflow (SI)
Switch
Switch
Switch
Attacker
Victim
Victim
Yes
Attack
No
Go back to the switch to which attacker is connected
Resume normal flow of packets
Load the models
Receive data from application running at controller
Make prediction and send to application
Create flow rule
Install flow rule onto the switches

Fig: Detection and mitigation flow module

DDoS Detection Features

- **Features taken for dataset generation are:**
  - Length of the packet
  - Average bytes per flow
  - Number of frames per second
  - Number of flows per second
  - Entropy of destination IP addresses per second
  - Entropy of source IP address per second
  - Entropy of IP protocol per second
  - Packet count per source
  - Byte count per source
  - Number of bits transferred per second
  - Number of bits received per second

Feature Selection Techniques

- Correlation Matrix
- Decision Tree
- Information Gain
- Extra Trees Classifier
- ANOVA F-Test
- Chi Square Test
- BORUTA Test
- Relief
- I-Relief
- Random Forest

Detection and Mitigation Application

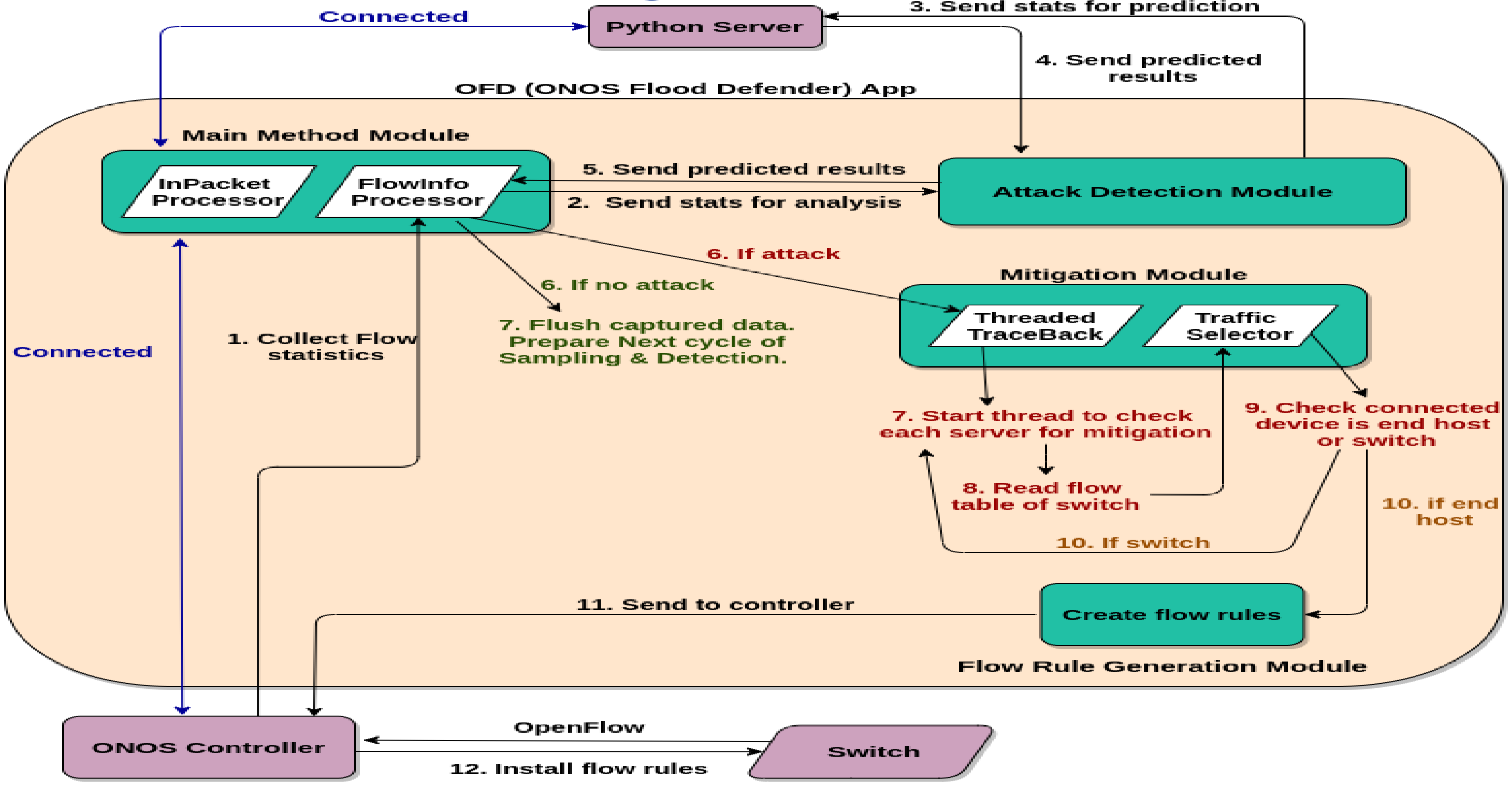

Connected
Python Server
3. Send stats for prediction
4. Send predicted results
OFD (ONOS Flood Defender) App
Main Method Module
InPacket Processor
FlowInfo Processor
5. Send predicted results
2. Send stats for analysis
Attack Detection Module
6. If attack
6. If no attack
Mitigation Module
Threaded TraceBack
Traffic Selector
Connected
1. Collect Flow statistics
7. Flush captured data. Prepare Next cycle of Sampling & Detection.
7. Start thread to check each server for mitigation
9. Check connected device is end host or switch
8. Read flow table of switch
10. if end host
10. If switch
11. Send to controller
Create flow rules
Flow Rule Generation Module
ONOS Controller
OpenFlow
12. Install flow rules
Switch

Fig: OFD (ONOS Flood Defender) Application

Modules in Application

- Main Method Module
- Attack Detection Module
- Mitigation Module
- Flow Rule Generation Module

Main Method Module

- Responsible for setting up application parameters, declaration, and initialization of variables.

- Coordinates between the Attack detection module, Mitigation module, and Flow Rule Generation Module.

- Collects flow data during each thread and passes them to the Attack Detection module for analysis.

Attack Detection Module

- Responsible for detecting ongoing DDoS attack.

- Predicted results are sent by python server to attack detection module which in turn sends the results to Main method module.

- Mitigation module is called in case of attack and when no attack is predicted, the data is flushed and the module waits for the next connection.

Mitigation Module

- Responsible for attack mitigation.

- Called based on the prediction of DDoS attack by Attack Detection Module.

- Identifies the problematic end host (attacker) and blocks the traffic between victim and attacker.

- Traceback traffic to its origin as close as possible based on the network switches’ flow rules.

Flow Rule Generation Module

- Handles the creation and installation of flow rules in the switches in case of attack.

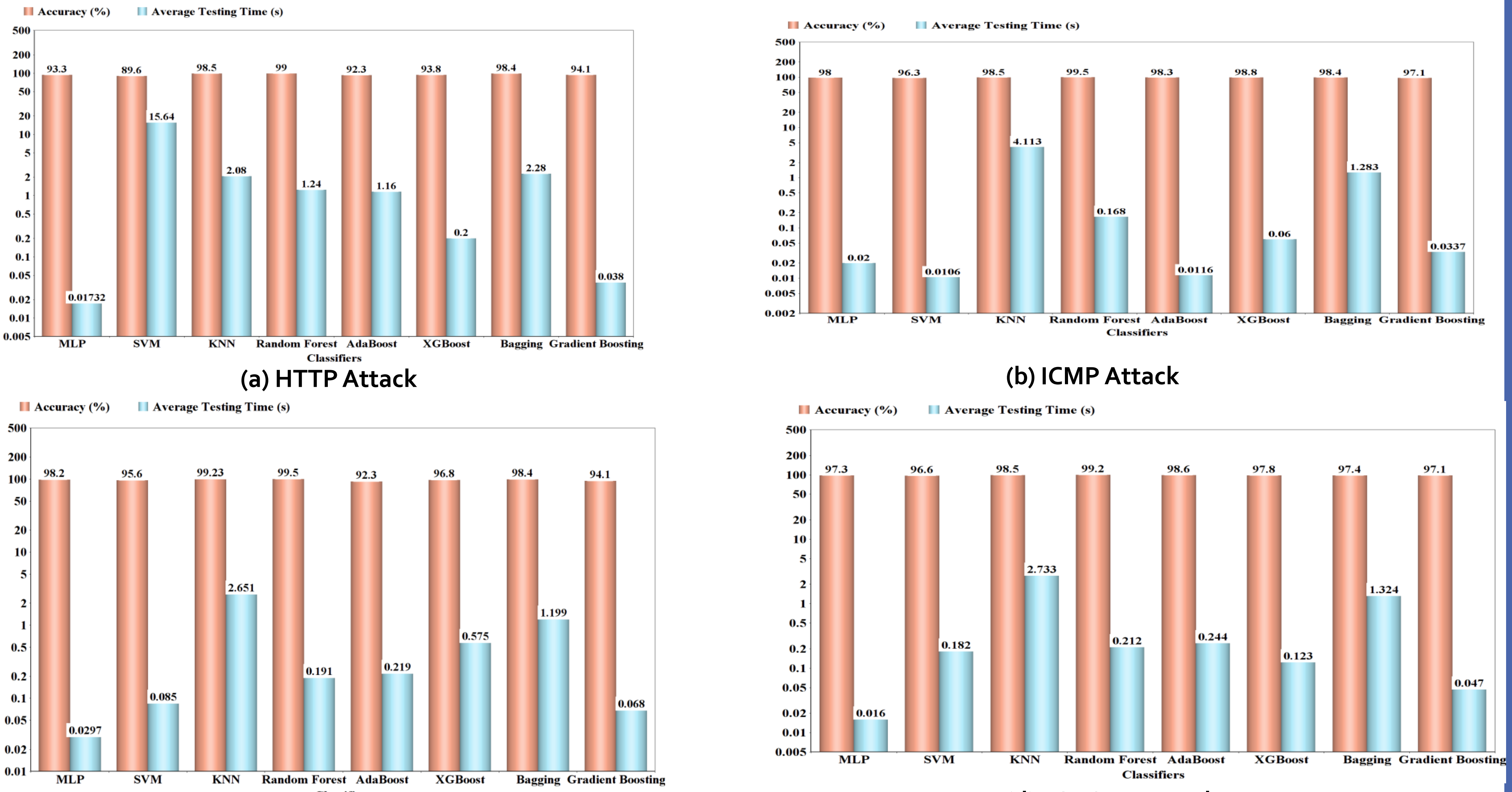
- Called by Mitigation module on attack detection.

- It makes and places flow rule to discard the flow packets based on the source and destination MAC address of the selected flows.

ONOS App Comparison

Ref.	Controller	Application Created	Detection	Mitigation	ML Technique for Detection
Chen et al., 2017 [10]	ONOS	No	Yes	Yes	SVM
Chen et al., 2018 [11]	POX	No	Yes	No	XGBoost
Myint et al., 2019 [12]	OpenDayLight	Yes	Yes	No	ASVM
Polat et al., 2020 [13]	POX	No	Yes	No	SVM, KNN, NB, ANN
Akanji et al., 2021 [14]	RYU	No	Yes	No	SVM
OFD App (Proposed)	**ONOS**	**Yes**	**Yes**	**Yes**	**MLP, KNN, SVM, XGBoost, Adaboost, RFC, Bagging, Gradient Boosting**

Results



(a) HTTP Attack

(b) ICMP Attack

(c) UDP Attack

(d) TCP SYN Attack

Testing time vs Accuracy graph

sFlow-RT Visualization Results

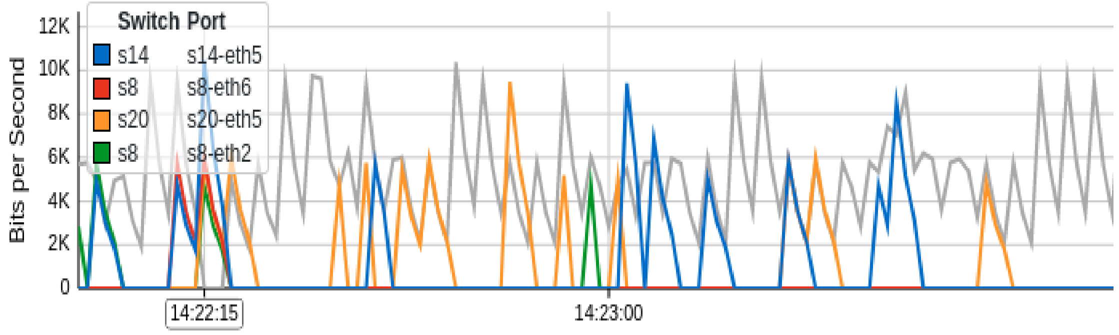


Fig: sFlow visualization during normal traffic

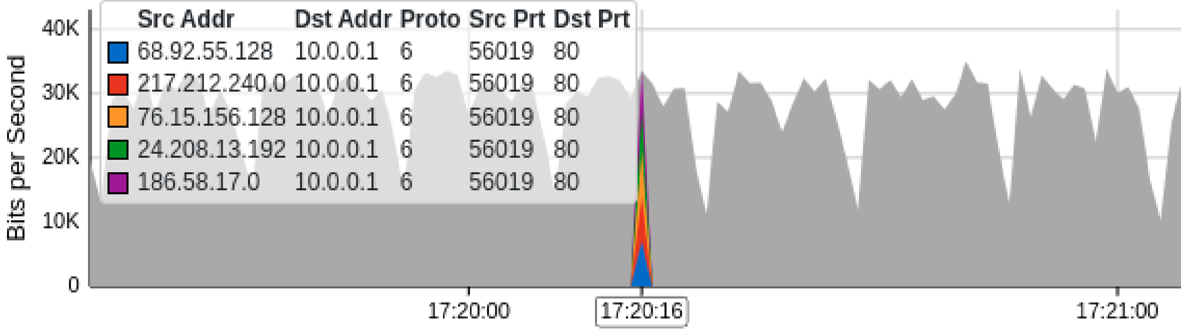


Fig: sFlow visualization during attack traffic

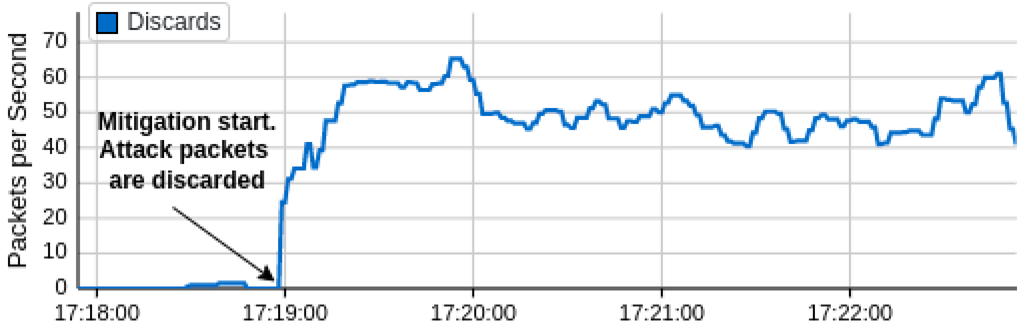


Fig: Packet discard after mitigation

Conclusion

- SDN has introduced many challenges.
- One of the fundamental issues which exposed due to the new architecture of SDN is the security risks.
- Our work focuses on detecting and mitigating DDoS attacks, mainly HTTP flood, UDP flood, ICMP flood, and TCP SYN flood attacks.
- The ONOS application can successfully detect the attacks using the APIs provided by ONOS and mitigate the attacks effectively by tracebacking technique.
- Government servers, websites, ISPs, public and private sector could deploy the product in their network infrastructure to protect themselves from miscreants who try to reduce server performance or sometimes crash the server completely.
- In any case, if attack has already been done then the proposed product would help to trace the locations, to find out from where the DDoS attack is being orchestrated.

Research papers published in Lab

- Neelam Dayal, Shashank Srivastava, **"Analyzing effective mitigation of DDoS attack with software-defined networking"**, *Computer & Security (Elsevier)*, vol. 130, pp. 103269, 2023, **SCIE Indexed**. **(IF 5.6).**
- Naziya Aslam, Shashank Srivastava, M.M Gore, **"A Comprehensive Analysis of Machine Learning- and Deep Learning-Based Solutions for DDoS Attack Detection in SDN"**, *Arabian Journal for Science and Engineering (Springer)*, pp. 1-41, 2023, **SCIE Indexed**. **(IF: 2.9)**.
- Naziya Aslam, Shashank Srivastava, M.M Gore, **"ONOS Flood Defender: An Intelligent Approach to Mitigate DDoS Attack in SDN"**, *Transactions on Emerging Telecommunications Technologies (Wiley)*, pp. e4534, 2022, **SCIE Indexed**. **(IF: 3.31)**
- Neelam Dayal, Shashank Srivastava, **"SD-WAN Flood Tracer: Tracking the entry points of DDoS attack flows in WAN"**, *Computer Networks (Elsevier), vol. 186, pp. 107813, 2021,* **SCIE Indexed**. **(IF:5.6)**
- Prasenjit Maity, Sandeep Saxena, Shashank Srivastava, Kshira Sagar Sahoo, Ashok Kumar Pradhan, Neeraj Kumar, **" An Effective Probabilistic Technique for DDoS Detection in Open- Flow Controller"**, *IEEE Systems Journal*, vol. 16, no. 1, pp. 1345-1354, 2021, **SCIE Indexed**. **(IF. 4.40)**

Research papers published in Lab

- Neelam Dayal, Prasenjit Maity, Shashank Srivastava, Rahamatullah Khondoker, **"Research Trends in Security and DDoS in SDN"**, *Security and Communication Networks, (John Wiley& Sons, Ltd)*, vol. 9, no. 18, pp. 6386-6411, 2016, **SCIE Indexed**. **(IF:1.719).**
- Neelam Dayal, Shashank Srivastava, **"Leveraging SDN for Early Detection and Mitigation of DDoS Attacks"**, *Communication Systems and Networks: 10th International Conference, COMSNETS 2018, Bangalore, India*, pp. 52-75, 2018, Springer International Publishing, 2019.
- Neelam Dayal, Shashank Srivastava, **"An RBF-PSO based approach for early detection of DDoS attacks in SDN"**, *10th International Conference on Communication Systems & Networks (COMSNETS)*, pp. 17-24, 2018.

References

1. C. Douligeris and A. Mitrokotsa, “Ddos attacks and defense mechanisms: classification and state-of-the-art,” Computer networks, vol. 44, no. 5, pp. 643–666, 2004.

2. Verma, Priyanka, Shashikala Tapaswi, and W. Wilfred Godfrey. "A request aware module using CS-IDR to reduce VM level collateral damages caused by DDoS attack in cloud environment." Cluster Computing (2021): 1-17.

3. C. Masolo, “Cloudflare detects a record 71 million request-per-second ddos attack,” 2023, [Accessed: 2023-05-10]. [Online]. Available: https://www.infoq.com/news/2023/02/cloudflare-ddos-attack/

4. P. Anand, “Record for the largest ever https ddos attack smashed once again,” 2022. [Online]. Available: https://www.itpro.co.uk/infrastructure/network-internet/368857/record-for-largest-ever-https-ddos-attack-smashed-again

5. Guru, “Largest https ddos attack on record – 26 million request per second,” 2022. [Online]. Available: https://cybersecuritynews.com/largest-https-ddos-attack/

6. T. Warren, “Microsoft says it mitigated one of the largest ddos attacks ever recorded,” https://www.theverge.com/2021/10/12/22722155/microsoft-azure-biggest-ddos-attack-ever-2-4-tbps, 2021, [Accessed: 2021-10-20].

7. “Aws shield threat landscape report – q1 2020,”https://aws-shield-tlr.s3.amazonaws.com/2020-Q1 AWS Shield TLR.pdf, 2020, [Accessed: 2021-10-20].

8. T. Shani, “Updated: This ddos attack unleashed the most packets persecond ever. here’s why that’s important.” https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/, 2019, [Accessed: 2021-10-20].

References (contd.)

9. J. Turner, “2017: The year of widespread sdn adoption and ddos attack mitigation,” https://www.networkworld.com/article/3156344/2017-widespread-sdn-adoption-and-ddos-attack mitigation.html, 2017, [Online]

Thank You