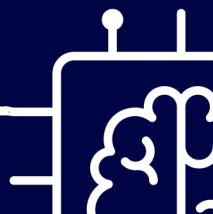
DDOS Detection & Mitigation using Statistical and ML in SDN

Intelligent Detection Securing SDNs Empowering Systems



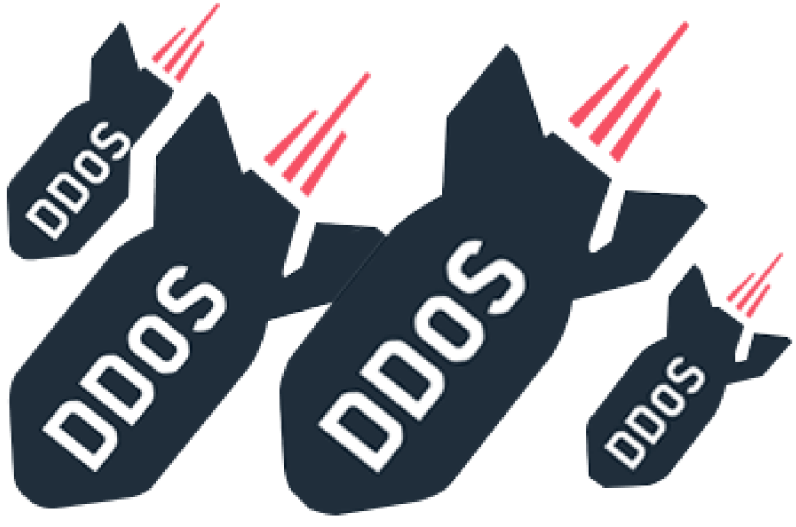
Presenting to You by AMAN

TABLE OF CONTENT

This project aims to improve the security of Software-Defined Networking (SDN) by detecting and mitigating Distributed Denial of Service (DDoS) attacks. By utilizing machine learning and statistical methods, the goal is to create effective solutions that accurately identify and counteract DDoS threats, ensuring the stability, performance, and resilience of SDN environments against such malicious activities.

DDoS attacks occur due to various reasons, often driven by different motivations and exploiting specific vulnerabilities. Here are some common causes:

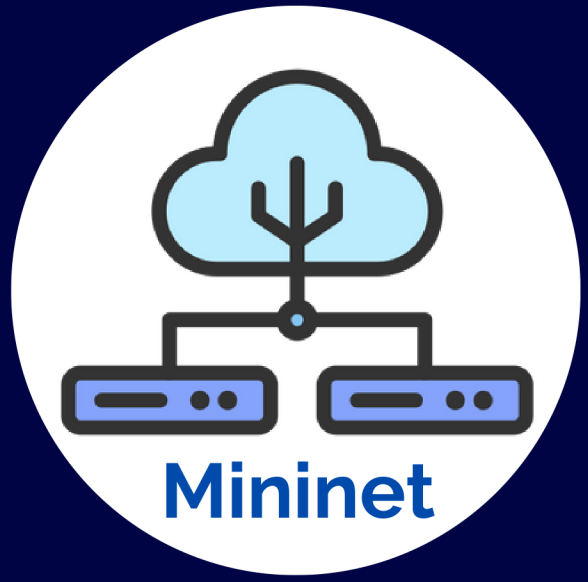
- Competitive Advantage
- Ransom DDoS
- Inexperienced Hackers
- Exploitation of Vulnerabilities
- Political or Ideological Reasons
- Testing and Learning
- Revenge or Grudge



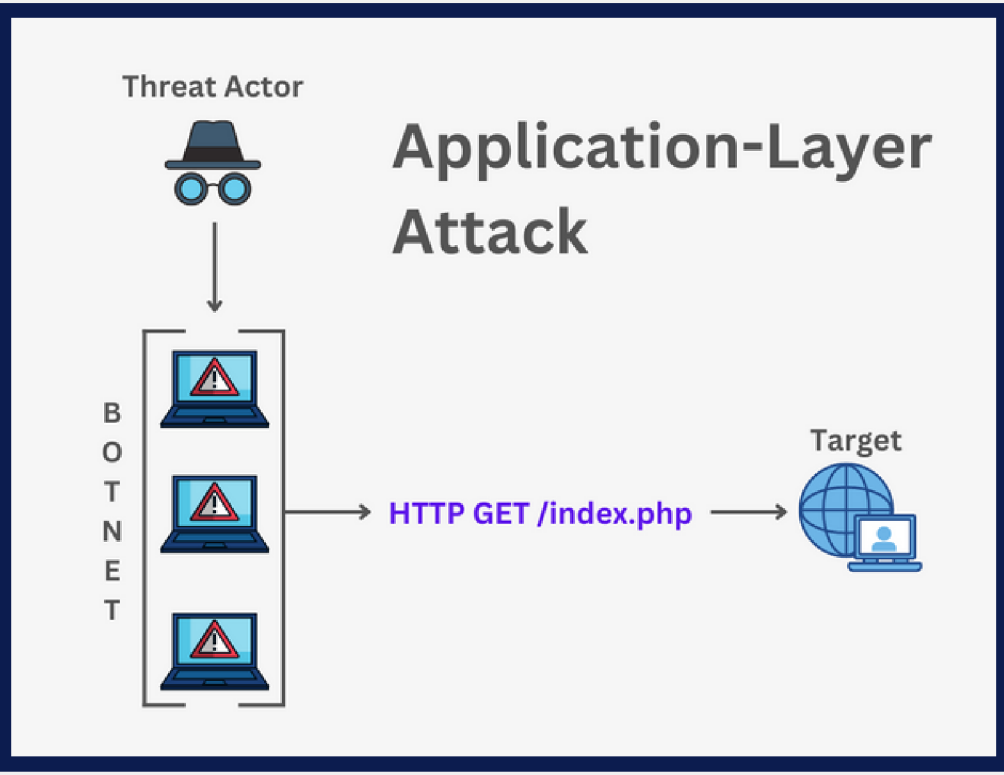

Openflow

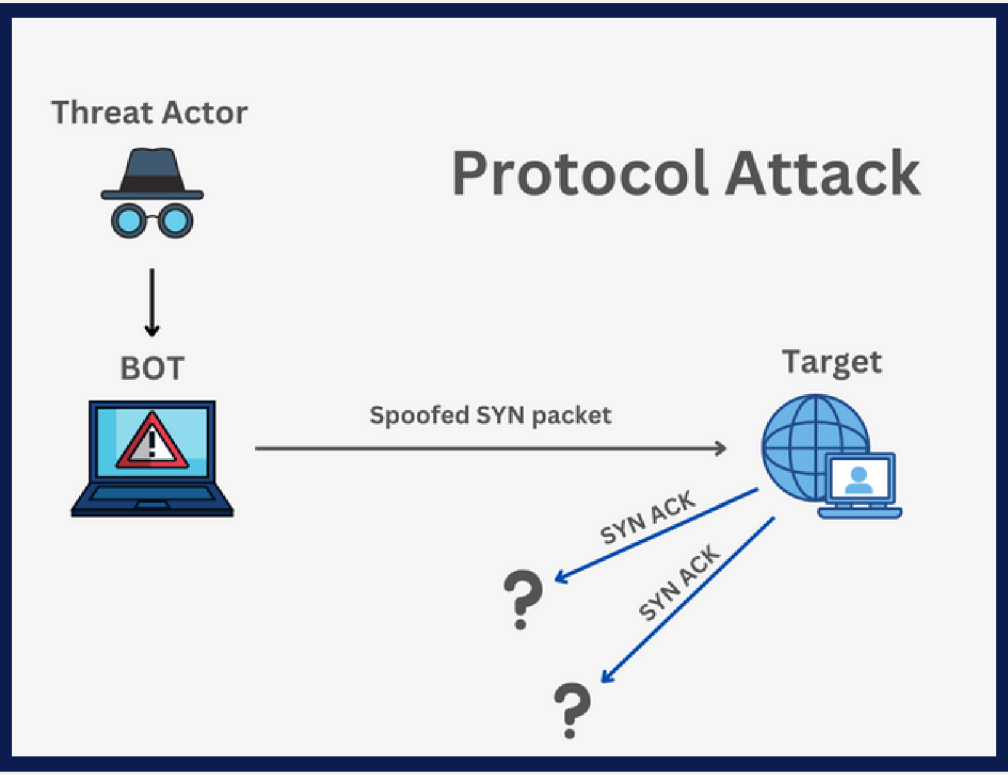

hPing


iPerf


Mininet


debian

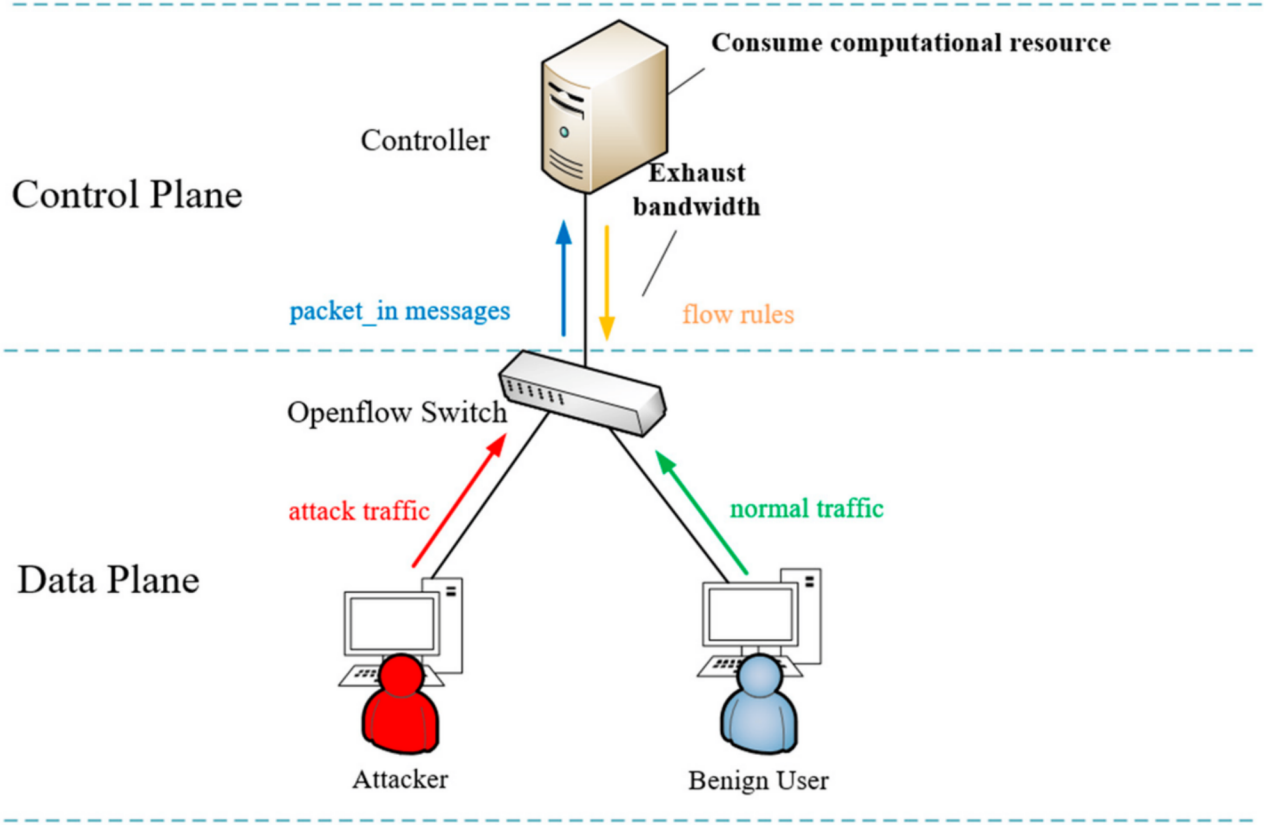




***Application Layer* :** aim to exhaust the resources of the targeted application or server by overwhelming it with a high volume of requests. (Ex: HTTP flood)

***Protocol Layer* :** target vulnerabilities in the network protocols to exhaust network resources and disrupt connectivity. (Ex: SYN flood, UDP flood)

- Data Collection of the statistical features.
- Normal traffic
- Attack traffic



SVM will be using this dataset to train itself and to predict the traffic as normal or DDOS attack traffic.

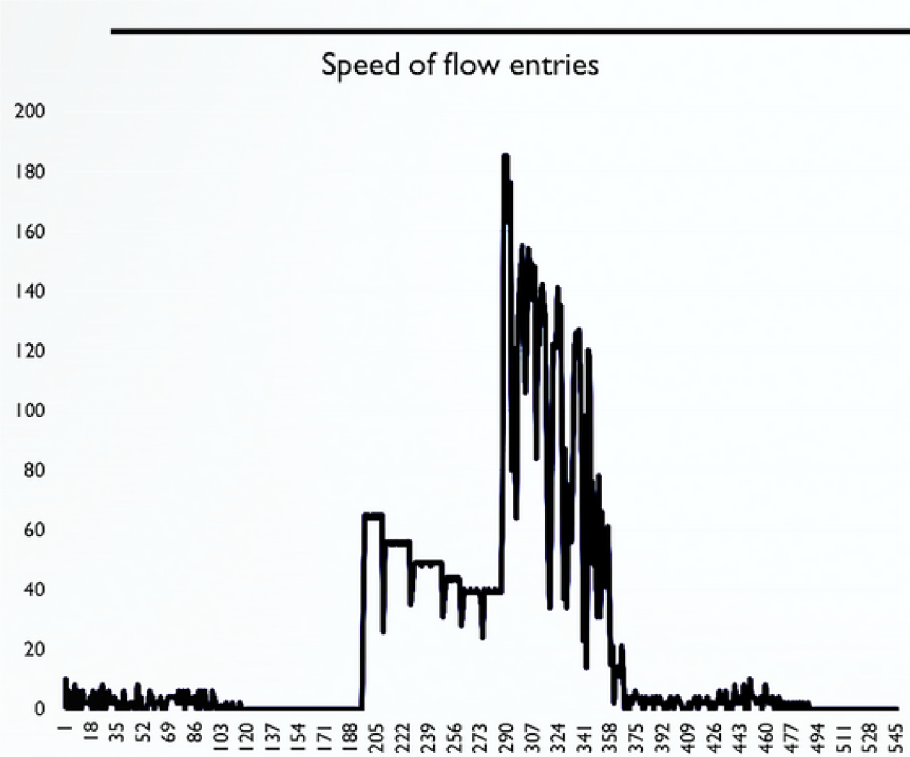
Statistical Analysis of Traffic Features

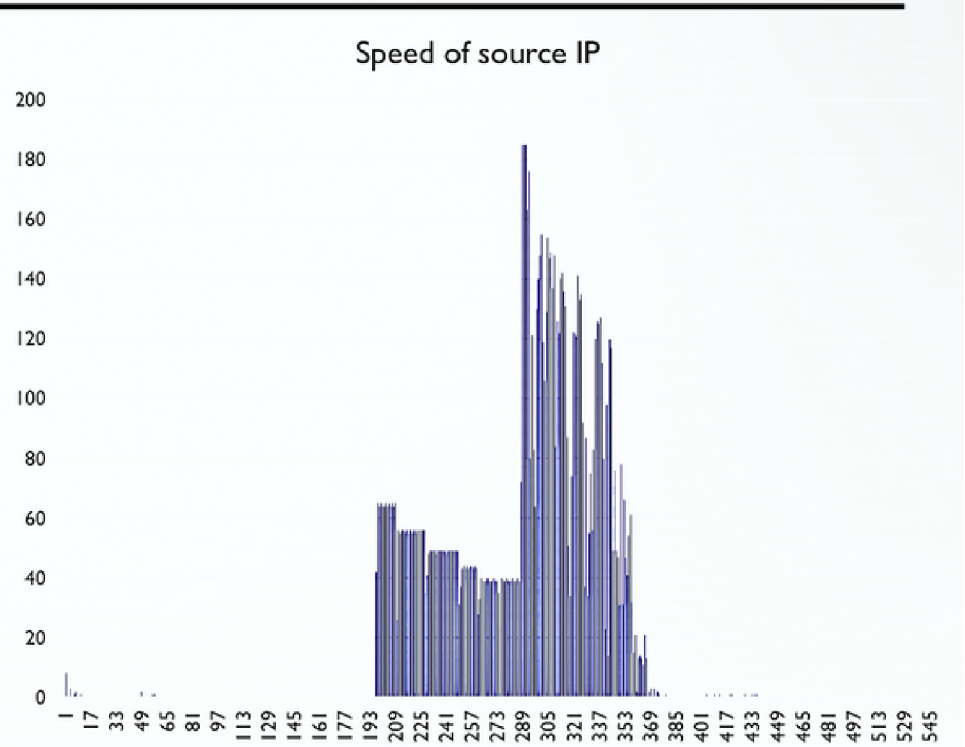
- Speed of IP sources
- Flowcount
- Speed of flow entries
- Ratio of pair-flow entries

Machine Learning Methods

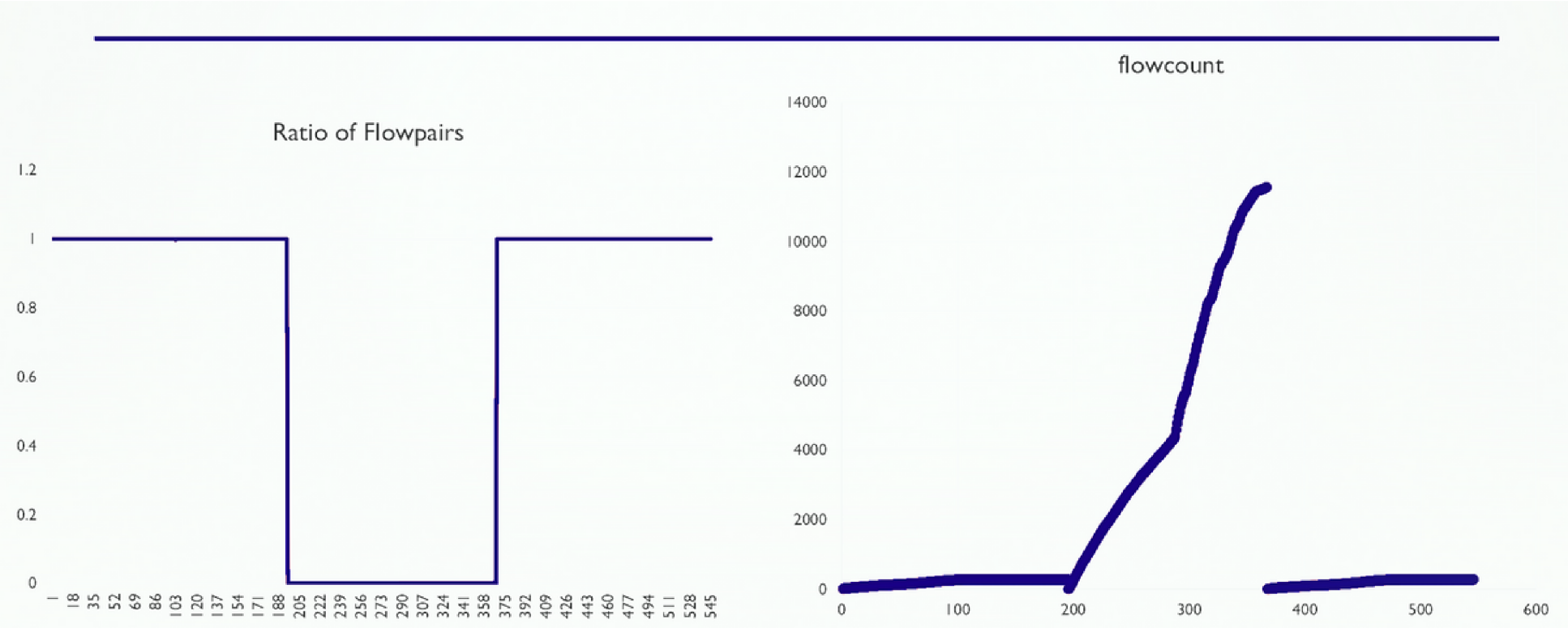
- Support vector machine used for Evaluation
- Decision tree

Tri-Idea

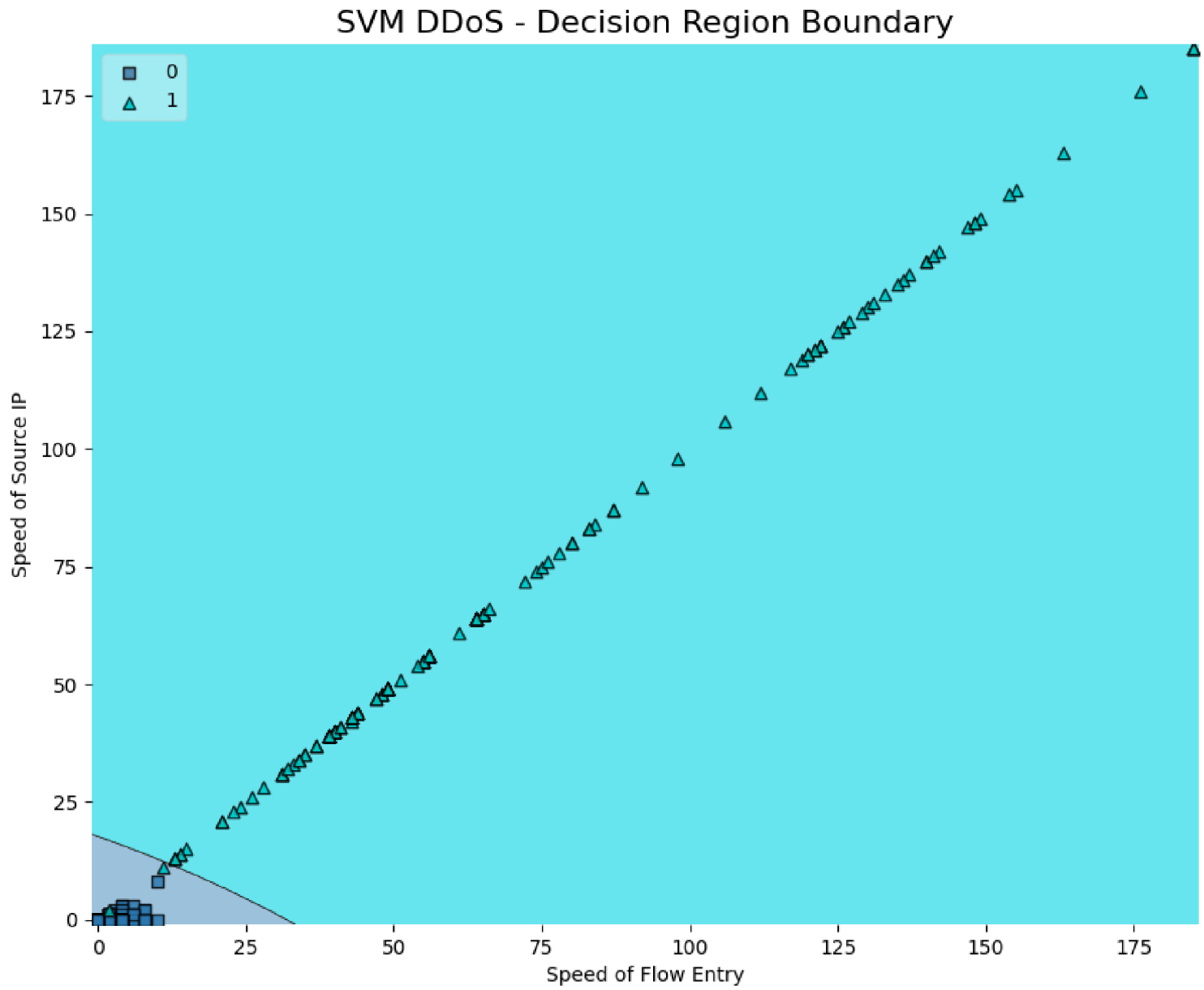

Speed of flow entries
200
180
160
140
120
100
80
60
40
20
0
1 18 35 52 69 86 103 120 137 154 171 188 205 222 239 256 273 290 307 324 341 358 375 392 409 426 443 460 477 494 511 528 545


Speed of source IP
200
180
160
140
120
100
80
60
40
20
0
1 17 33 49 65 81 97 113 129 145 161 177 193 209 225 241 257 273 289 305 321 337 353 369 385 401 417 433 449 465 481 497 513 529 545

Tri-Idea

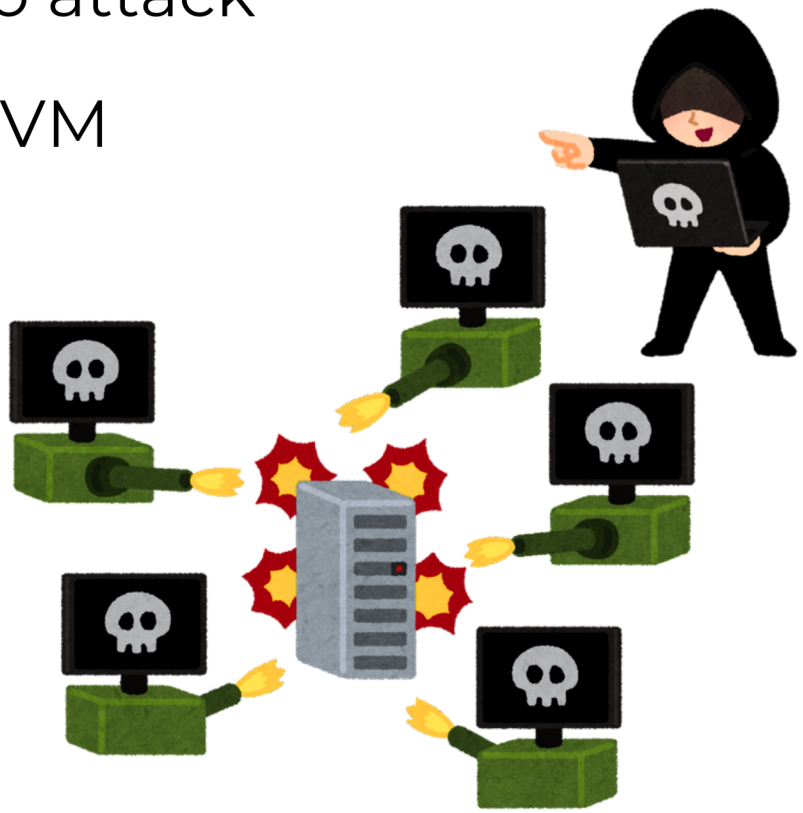

Ratio of Flowpairs
1.2
1
0.8
0.6
0.4
0.2
0
1
18
35
52
69
86
103
120
137
154
171
188
205
222
239
256
273
290
307
324
341
358
375
392
409
426
443
460
477
494
511
528
545
flowcount
14000
12000
10000
8000
6000
4000
2000
0
0
100
200
300
400
500
600

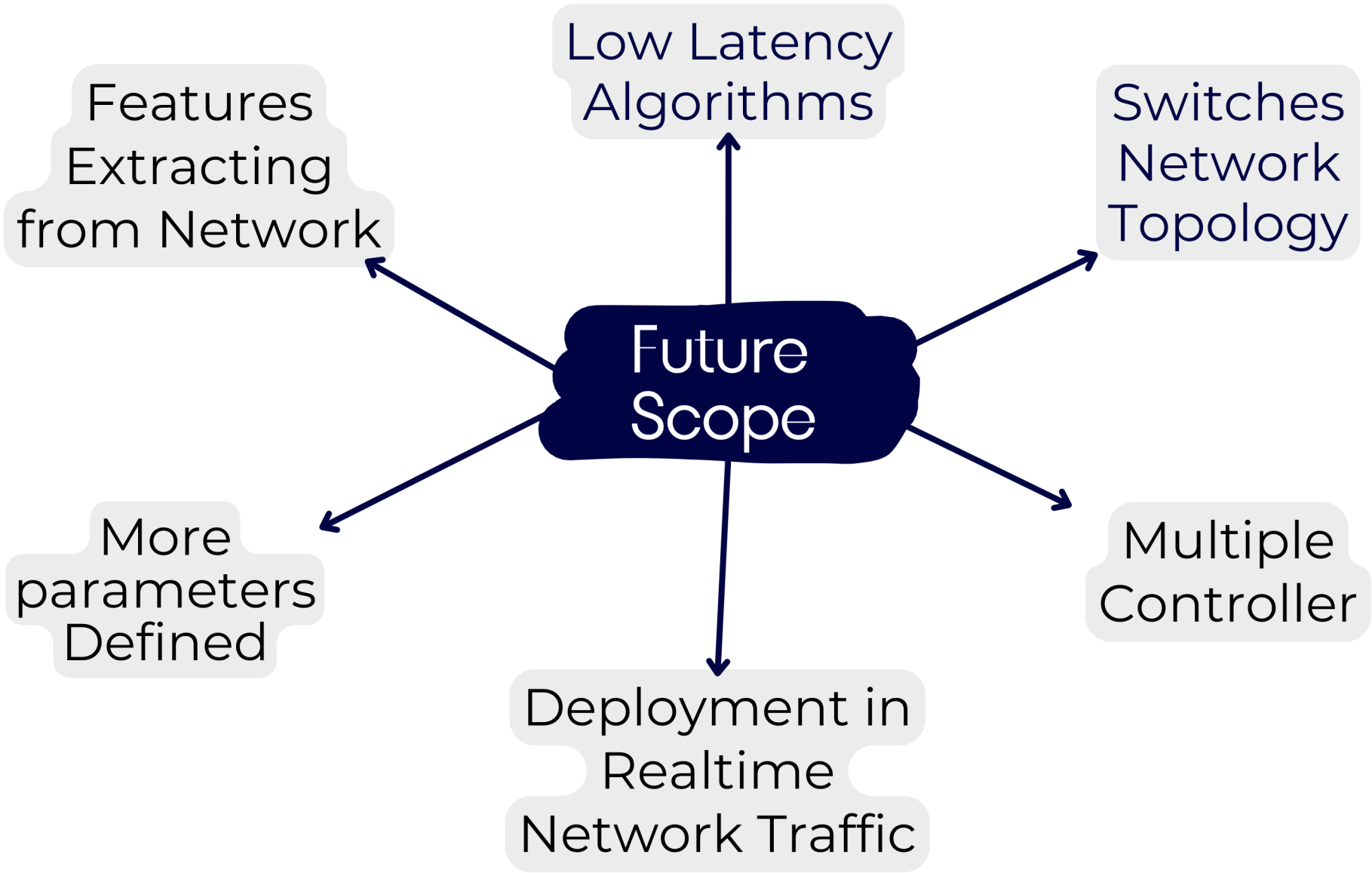
EVALUATED RESULTS



- Faulty dataset trained to the SVM

- Trusted IP can be used to attack the network which the SVM would not detect.




Low Latency Algorithms
Features Extracting from Network
Switches Network Topology
Future Scope
More parameters Defined
Multiple Controller
Deployment in Realtime Network Traffic

Conclusion

This project successfully demonstrates the potential of machine learning and statistical methods in detecting and mitigating DDoS attacks within SDN environments. By leveraging advanced algorithms and real-time analytics, we developed robust solutions that enhance network security and resilience.

BIBLIOGRAPHY

- DDOS Attacks: Real-World Detection, Prevention and Mitigation

  by Yuri Diogenes, Erdal Ozkaya

- Practical Machine Learning for Cybersecurity

  by Soma Halder, Sinan Ozdemir

- Serverius IT infrastructure YouTube Channel

Thank you for your time!