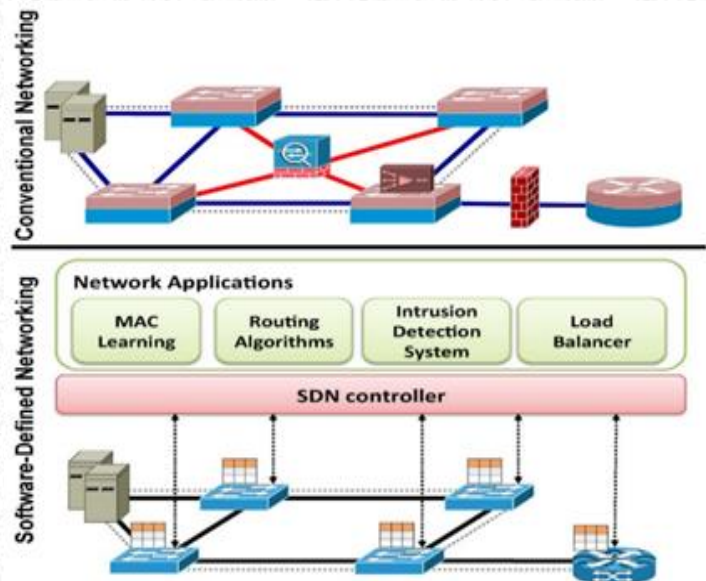


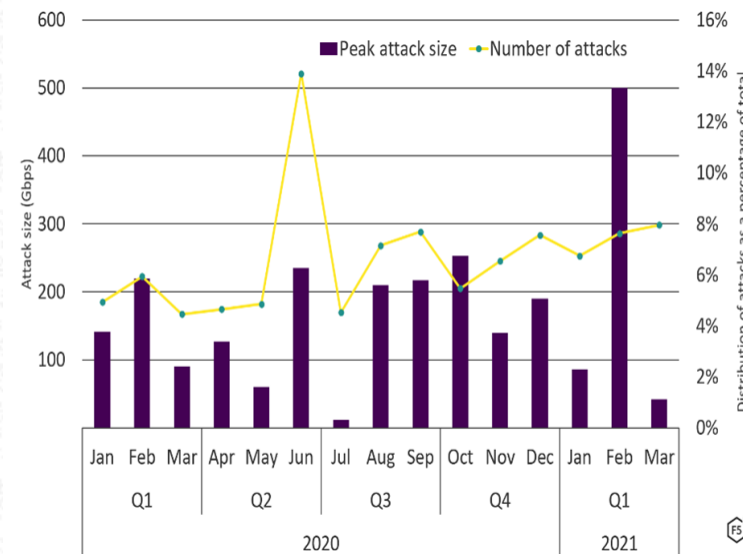
Detecting Abnormal Data Traffic in a simulated Software Defined Network

Introduction

Given SDN's vulnerabilities, SDNs may be subject to assaults that likewise target conventional networks. However, because traditional defences assume switches to be intelligent, whereas separation of control and data planes forces SDN switches to forward packets in accordance with the rules set up by the SDN controller, solutions that work for traditional networks may not be directly applicable for SDNs. many traditional attacks, such as Distributed Denial of Service attack, ARP poisoning and LLDP spoofing, will continue to manifest in SDNs. [1]



SDN vs Conventional Network Architecture. [2]

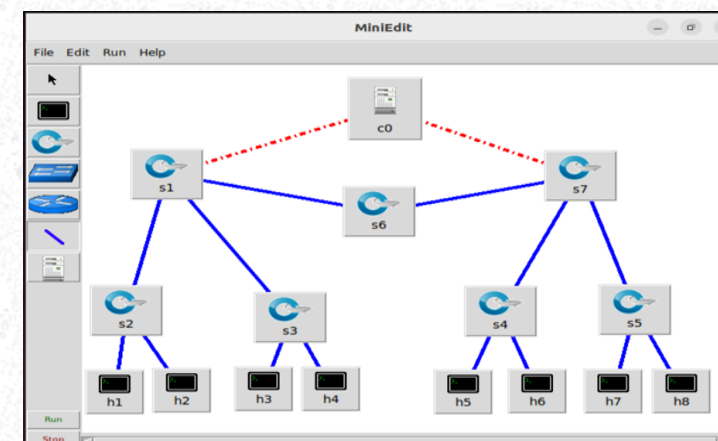


DDoS Attack Frequency Compared To Peak DDoS Attack Sizes. [3]

Aims

The Research provides a thorough analysis of the current Software Defined Network(SDN) architectures and discusses the most pressing issues that a integrated SDN architecture could address. Also covered are the many security concerns, such as threats and assaults, which limit the development of software-defined networking. Therefore, the primary goal of this research study is to examine previous works to address the complex and challenging difficulties of DDoS attacks on Software Defined Networks. [2]

Traditional IP networks are difficult to administer and are complex. Network administrators must configure each individual network device separately using low-level, frequently vendor-specific instructions to express the necessary high-level network policy. In addition to configuration complexity, network environments also need to withstand fault dynamics. [2]



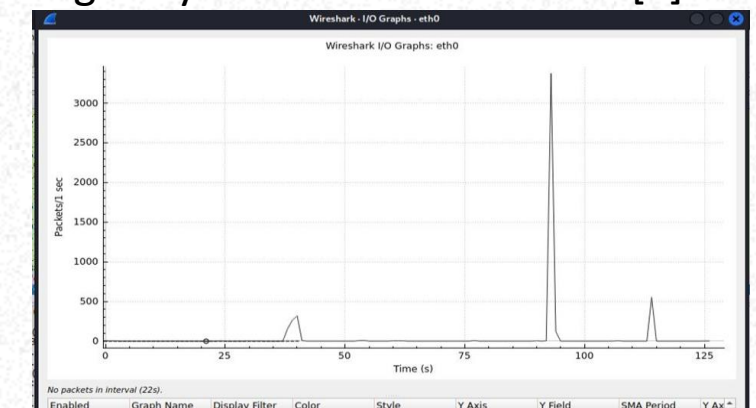
Simulation Network Topology created for sending and capturing Network Packets



Hafiz Uddin
1807533@student.uwtsd.ac.uk

Conclusion

A new networking paradigm called software-defined networking (SDN) offers hope for changing the limits of existing network infrastructures. By separating the network's control logic (the control plane) from the underlying routers and switches that forward traffic (the data plane), it first destroys vertical integration. Second, the separation of the control and data planes reduces the complexity of network configuration and development by turning network switches into straightforward forwarding devices and implementing the control logic in a logically centralised controller. [4]



Graph that illustrates the sudden spike in incoming network traffic from a DDoS attack.

References

- [1](Dhawan et al., 2015)
- [2] (Kreutz et al., 2015)
- [3](DDoS Attack Trends for 2020 | F5 Labs, n.d.)
- [4](Tan et al., 2020)