Distributed Denial-of-Service (DDoS) Attack Detection and Mitigation for Internet of Things (IoT)

OPEYEMI PETER OJAJUNI
SMED
Southern University and A&M College

PRESENTATION OUTLINE

Introduction

Proposed Solution

Implementation and Results

Limitation , Conclusion and Future work

Internet of Things (IoT)

- The Internet of Things (IoT) allows different device with Internet Protocol (IP) address, to be connected together via internet to collect, provide, store, and exchange data among themselves.
- The IoT generates large amounts of data that IoT software use for data analysis.
- Cisco projected that by 2022 the global amount of data that will be generated will reach 4.8 Zettabytes, and by year 2030 over 500 billion devices will be connected to the internet.
- These devices are vulnerable to malicious attacks because they have limited computer system resources to support firewall and defense mechanism protocols.

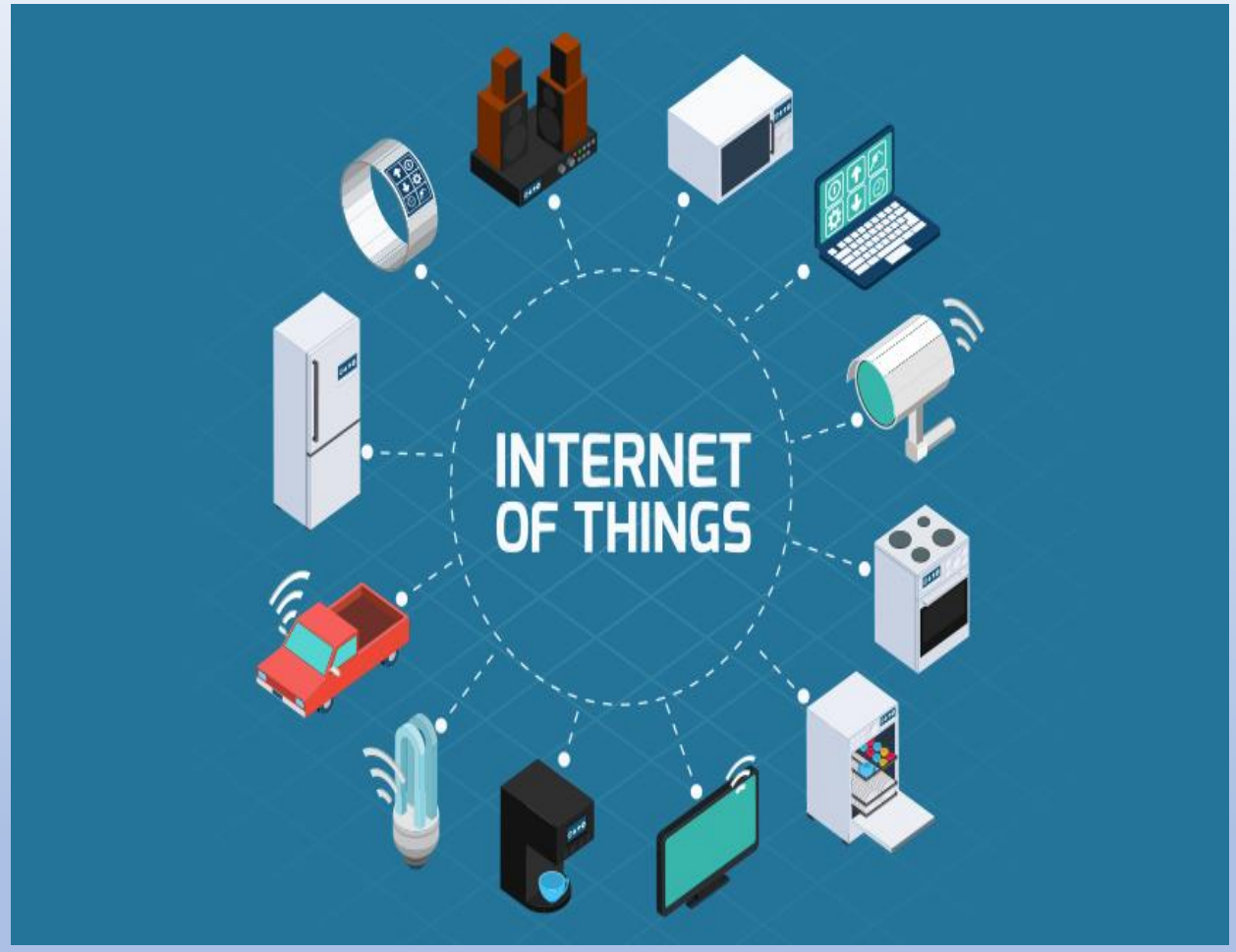

Figure 1 . Internet of things overview

Security and Privacy Issues in IoT

- Machine to machine trust,
- Authorization Authentication and Accounting,
- End- user privacy,
- Data privacy and Data confidentiality.
- Malicious attacks such as, man-in-the-middle attack, denial-of-service attack, Sybil attack, and node capture attack, distributed denial of service (DDoS)

Distributed denial of service (DDoS) Attack

The distributed denial of service is an extensive type denial of service (DoS) attack where the attacker uses more than one Internet Protocol (IP) address to send malicious traffic to its target victim in order to exhaust its computer system resources such as sockets, CPU, memory, disk or database bandwidth therefore, making the victim's service unavailable.

DDoS attack can lead to problems such as

- Loss of confidential data,
- Website service outage,
- Financial loss,
- Brand reputation damage

Major DDoS attacks in the past decade.

- Github attack : peak at 1.35 terabytes per second
- Dyn Domain name Server (DNS) attack : peak at 1.2 terabytes per seconds
- BBC attack: peak at 600 Gigabytes per second
- Spamhaus attack: peak at 400 Gigabytes per second

Types of DDoS attacks are TCP SYN flood (Transmission Control Protocol synchronize flood), ICMP (Internet Control Message Protocol) flood, Ping of death, HTTP(Hyper Text transfer Protocol) flood

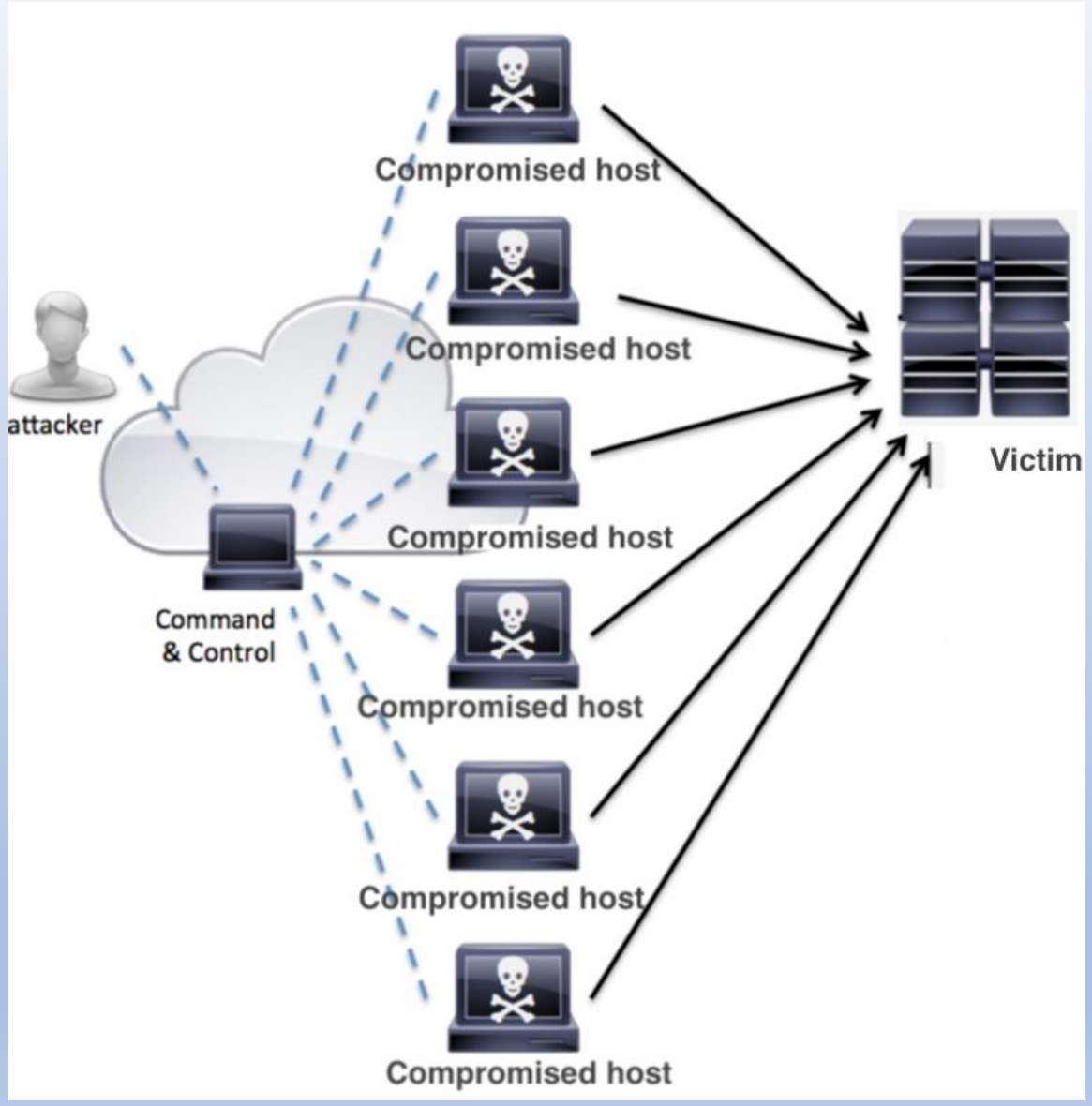

Figure 2. DDoS attack

PROPOSED SOLUTION

Software Defined Networks (SDN)

- SDN is a new architecture that offers a new chance in defeating DDoS attacks.

Why SDN over Traditional firewall?

- Software-based real-time traffic analysis,
- Centralized control management,
- Global view of the network,
- Dynamic updating of forwarding rules,
- Separation of the control plane from the data plane,
- Programmability of the network by external application

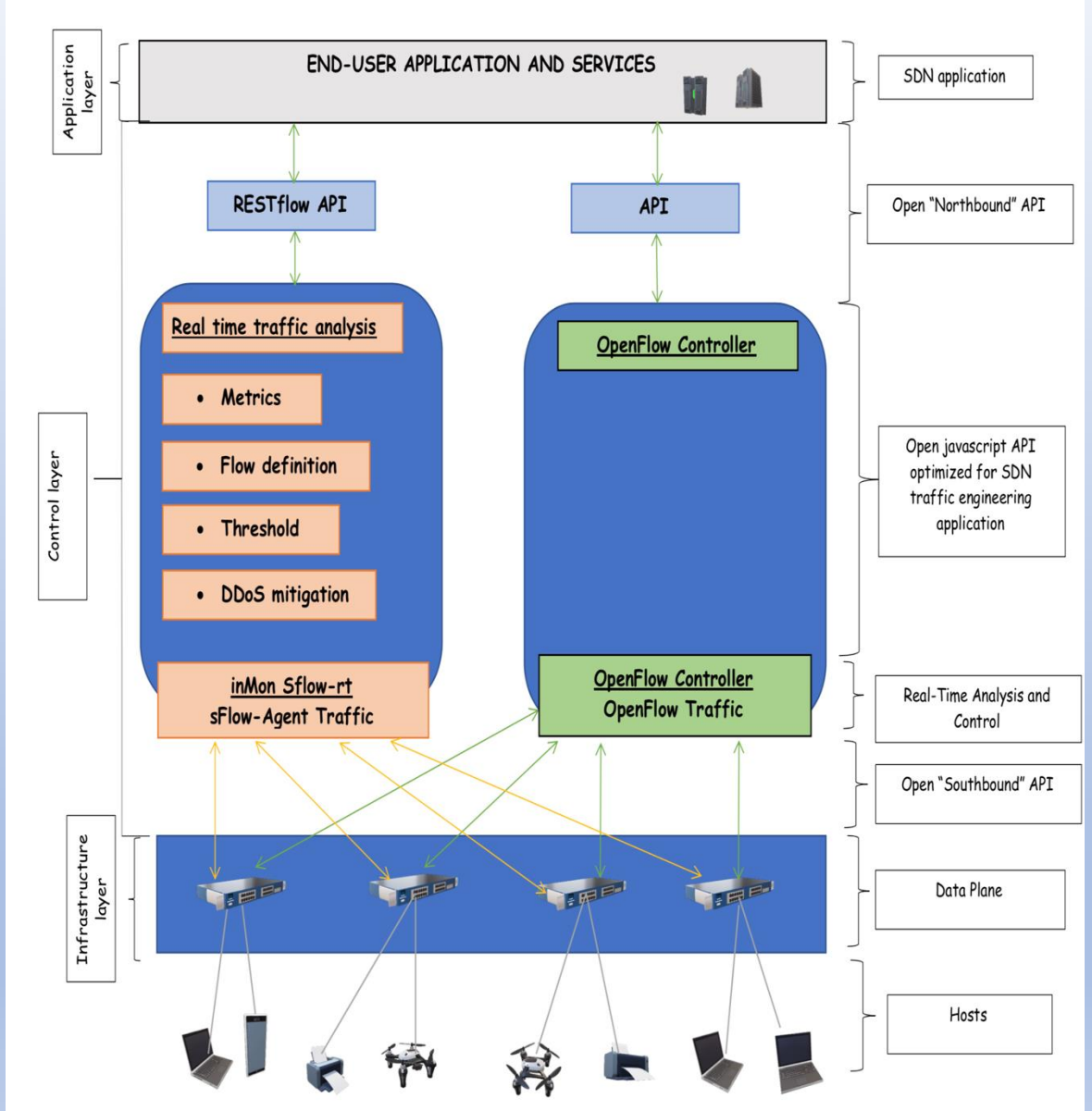

Figure 3. SDN Architecture

SDN-based DDoS attack Detection techniques

- Entropy, : network feature distribution to detect anomalous network activities.
- Machine learning: use algorithms like Bayesian networks, SOM, and fuzzy logic to identify the presence of anomalies.
- Traffic pattern analysis,: work on the assumptions that the infected IoT hosts exhibit similar behavioral patterns which are different from normal IoT hosts
- Connection rate: number of connections instantiated within a certain window of time
- SNORT :use combination of the intrusion detection system (such as SNORT)
- Open-flow integrated: OpenFlow to detect attacks and reconfigure the network dynamically.

Mitigation techniques

- Drop packet,
- Block port,
- Redirection of legitimate traffic to a new IP address,
- Control bandwidth,
- Deep packet inspection,
- network reconfiguration and topology change,
- Quarantine or Traffic isolation,
- MAC address change and/or IP address change.

to mitigate DDoS attack.

PROPOSED SYSTEM SETUP

- The host PC CPU is 2.3Ghz Intel Core i5 and 8 GB 2133 MHz LPDDR3 memory.
- The virtual machine has one processor core CPU and 2GB memory.
- The Mininet is a network simulator that runs on a virtual machine with Ubuntu 14.0 operating system.
- The Mininet is used to create the SDN network topology with OpenFlow switch and host PCs and it is connected to SDN controller.
- The floodlight is the Java-based OpenFlow controller and it runs on the virtual machine with Ubuntu 14.0 operating system.
- The inMon sFlow-RT is used for real-time traffic analysis and it runs on the virtual machine with Ubuntu 14.0 operating system.
- The Nodejs is an open-source, cross-platform JavaScript run-time environment that executes JavaScript code outside of a browser and it runs on the virtual machine with Ubuntu 14.0 operating system.
- The browser is used to access graphical user interface (GUI) of the floodlight and inMon sFlow-RT.

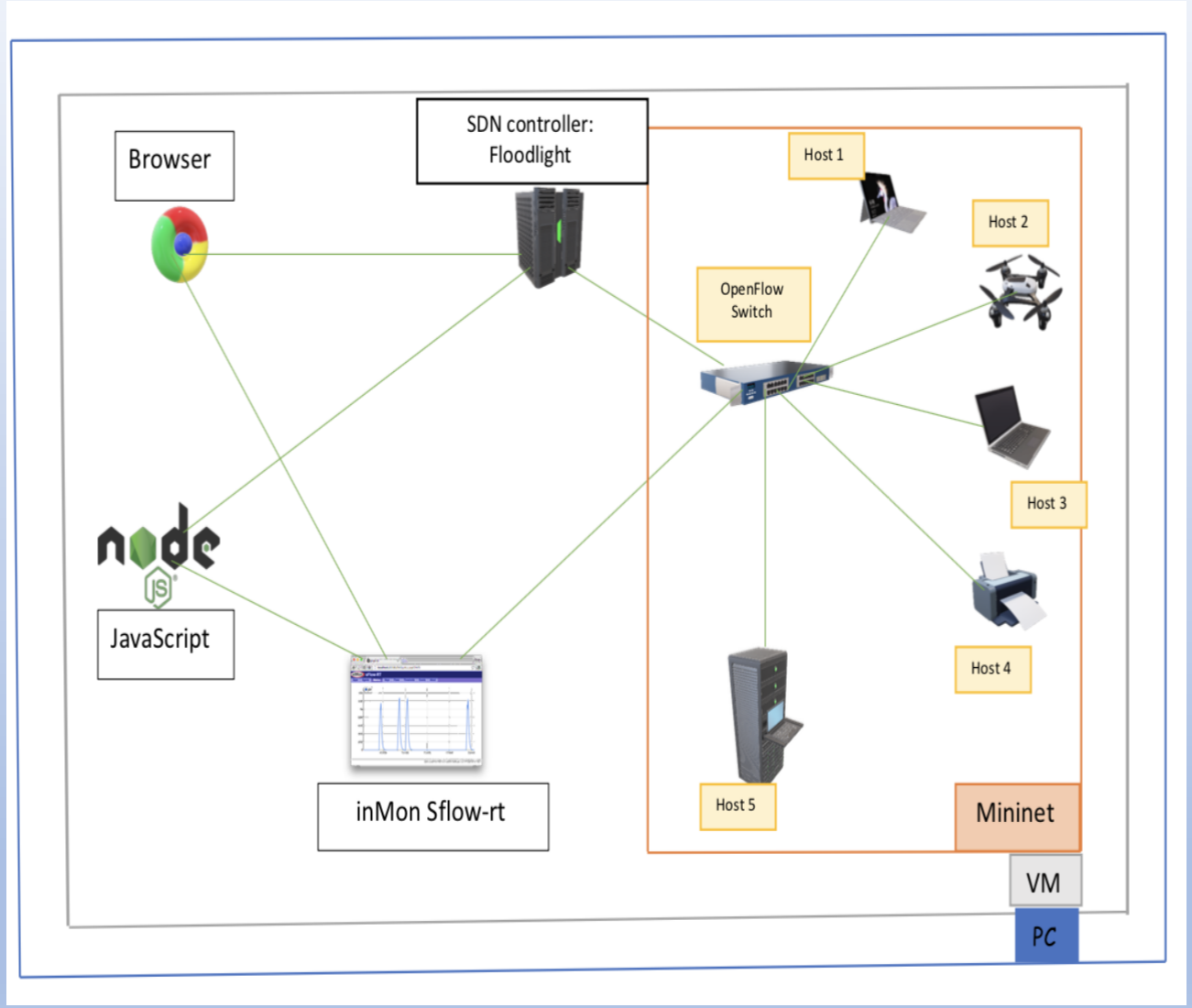

Figure 4. Proposed system setup.

IMPLEMENTATION AND RESULTS

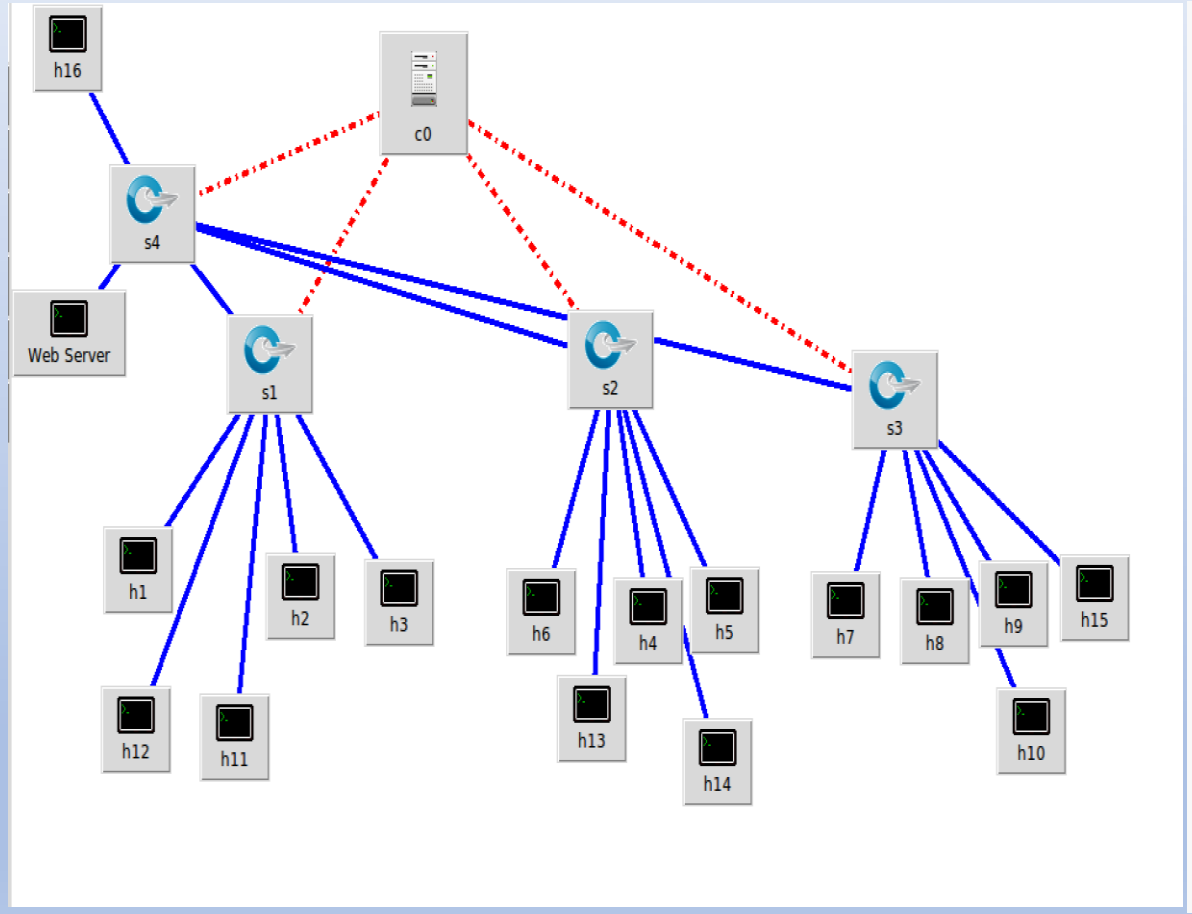

Figure 5. Topology of proposed system

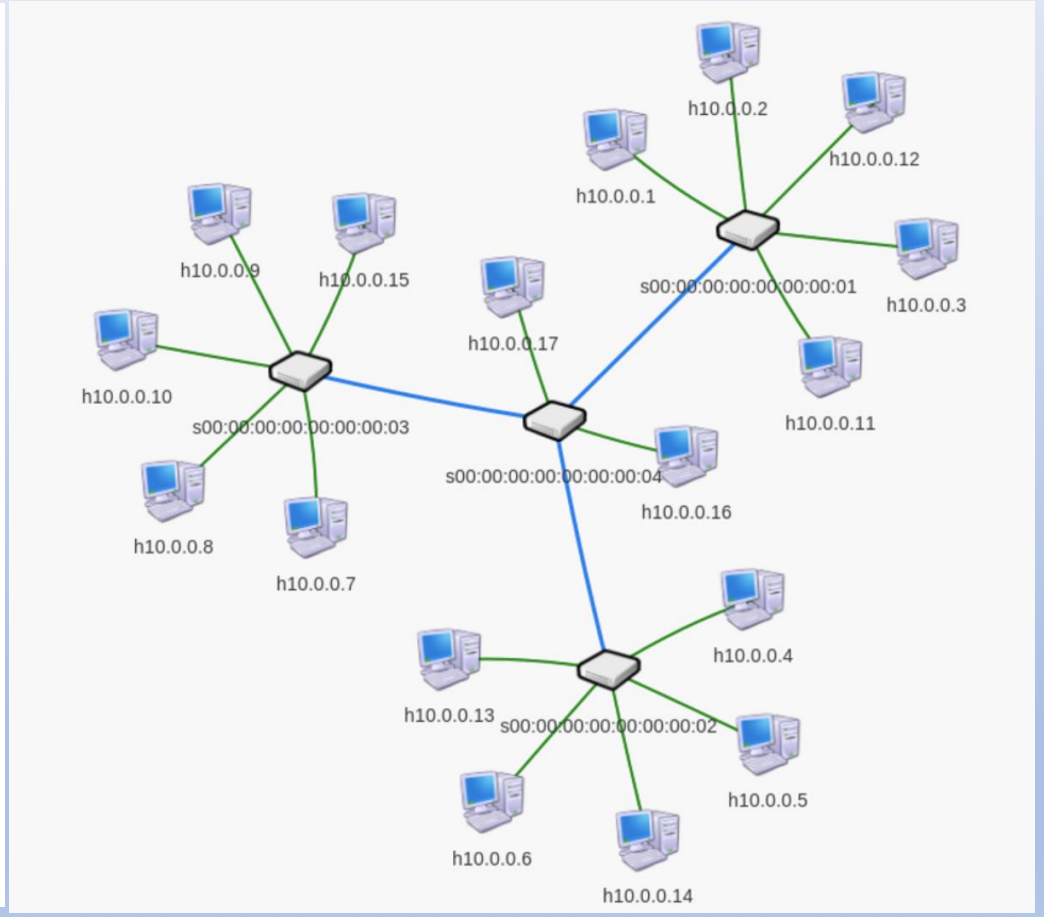

Figure 6. Topology of proposed system in SDN controller

Results before DDoS Attack

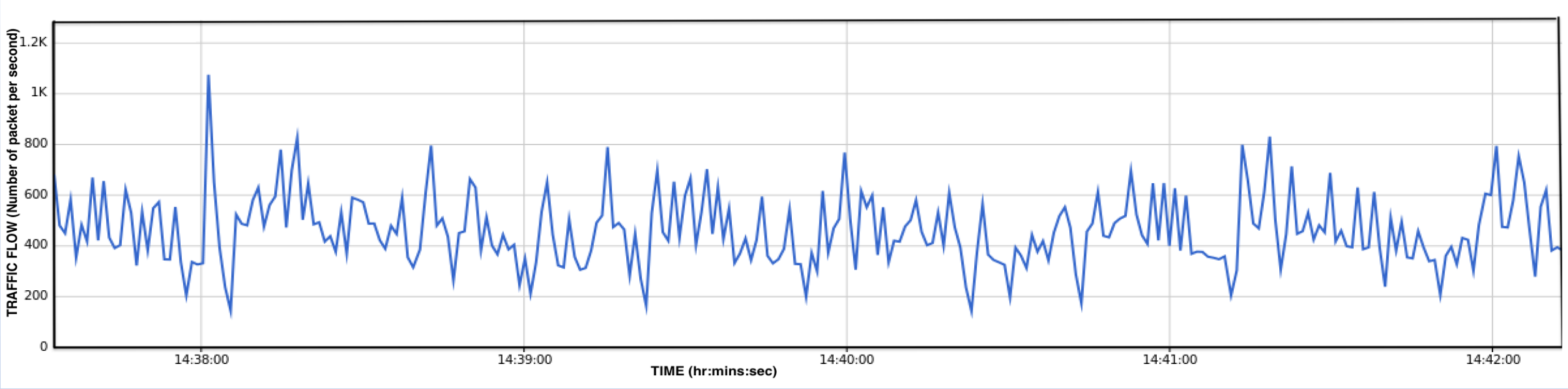

Figure 7. Traffic flow (number of packets per second) in the network

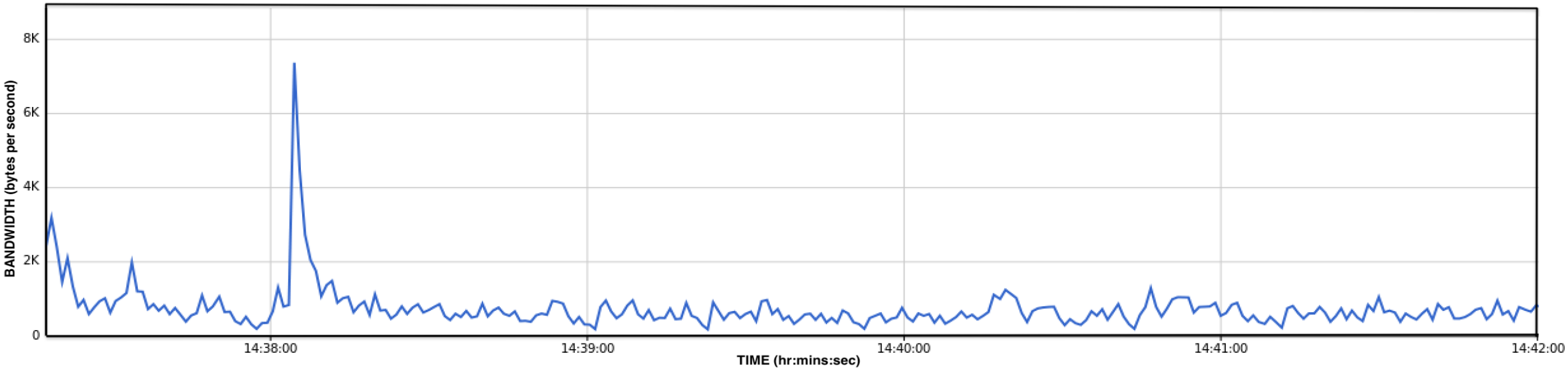

Figure 8. Network bandwidth (bytes per second)

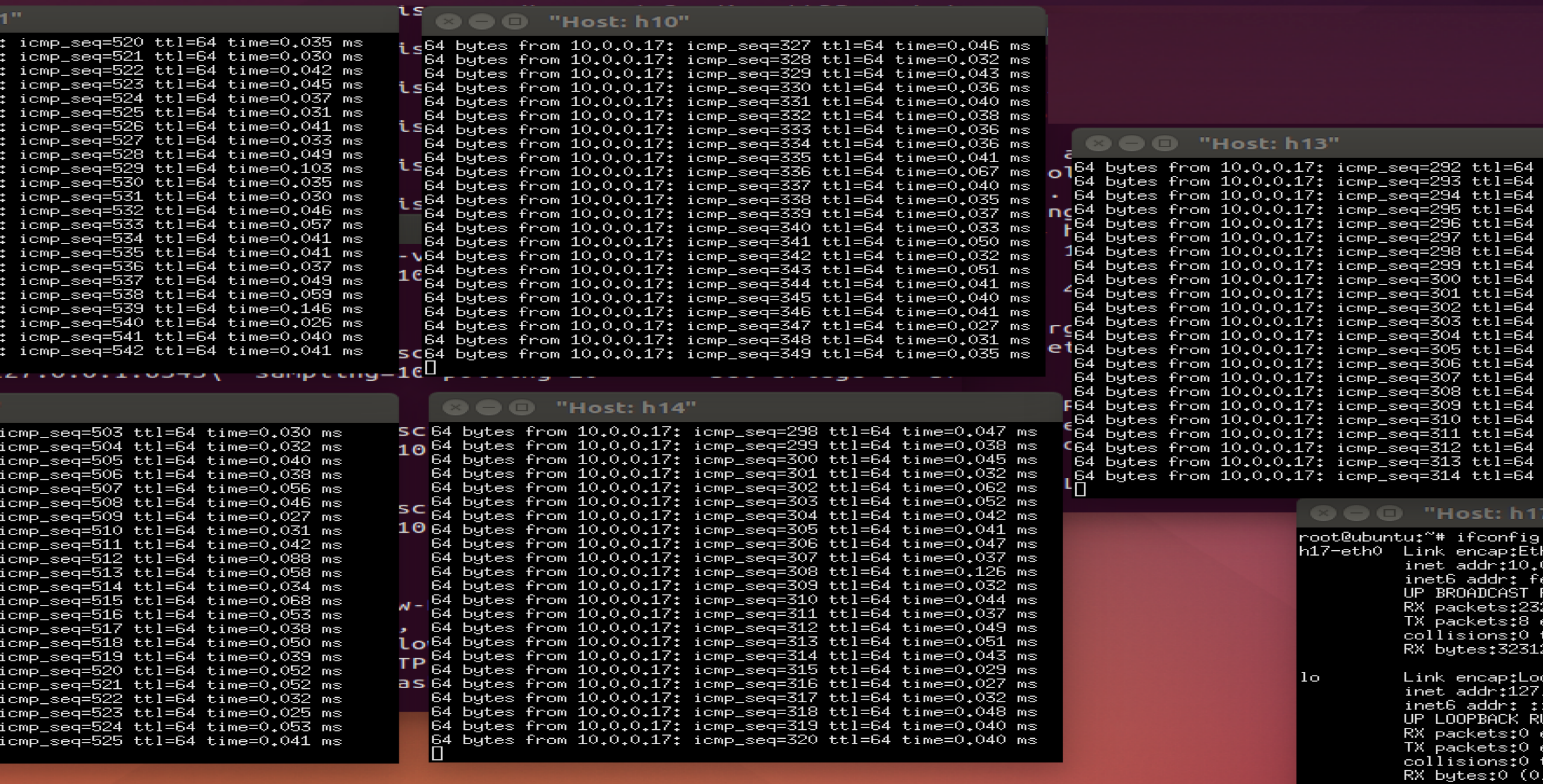

Figure 9. Time delay for ping command from normal host users.

Results after DDoS attack

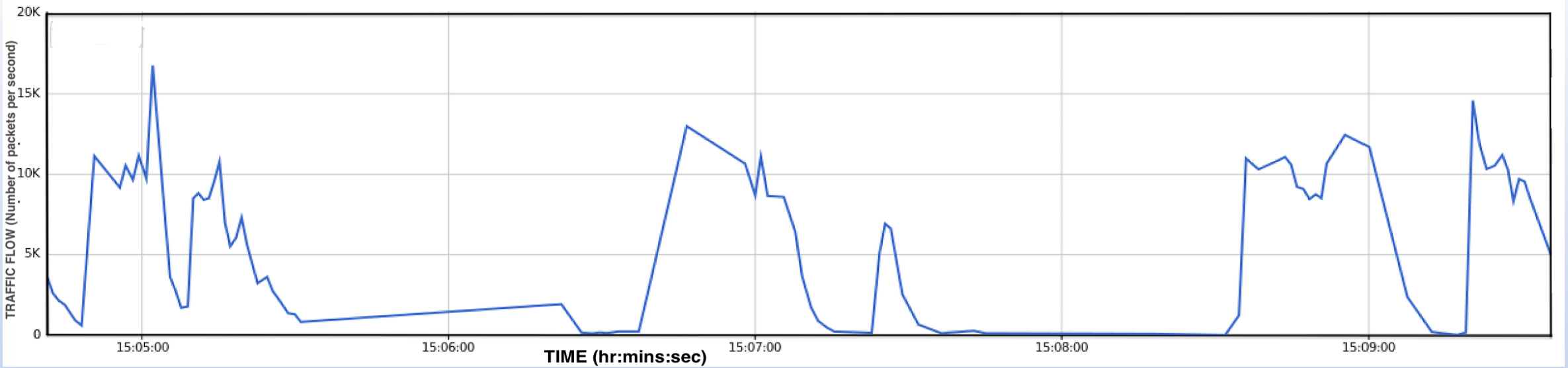

Figure 10. Traffic Flow (number of packets per second) in the network under attack

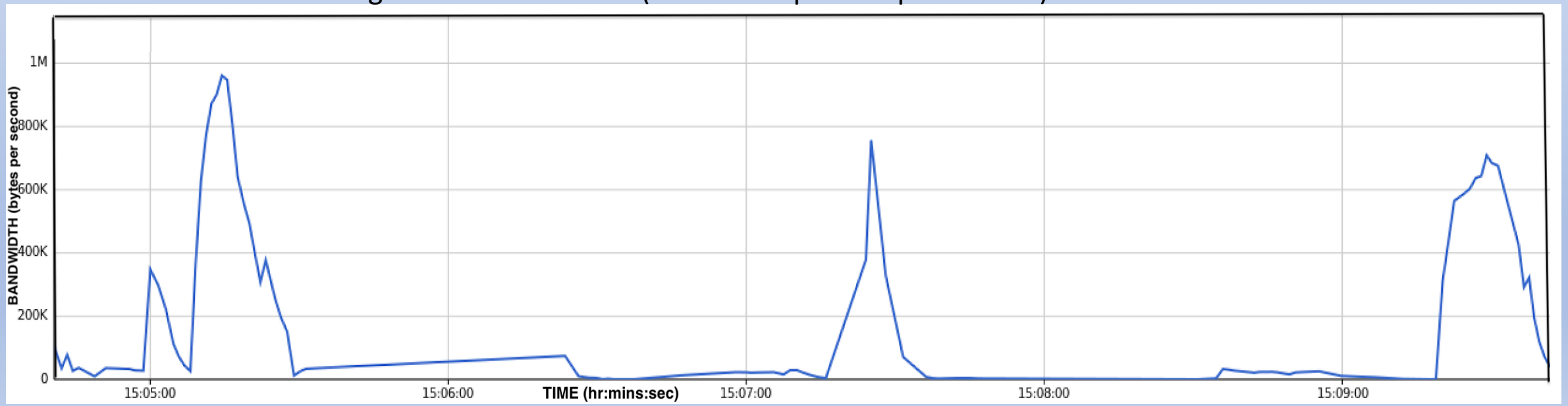

Figure 11. Network Bandwidth under attack

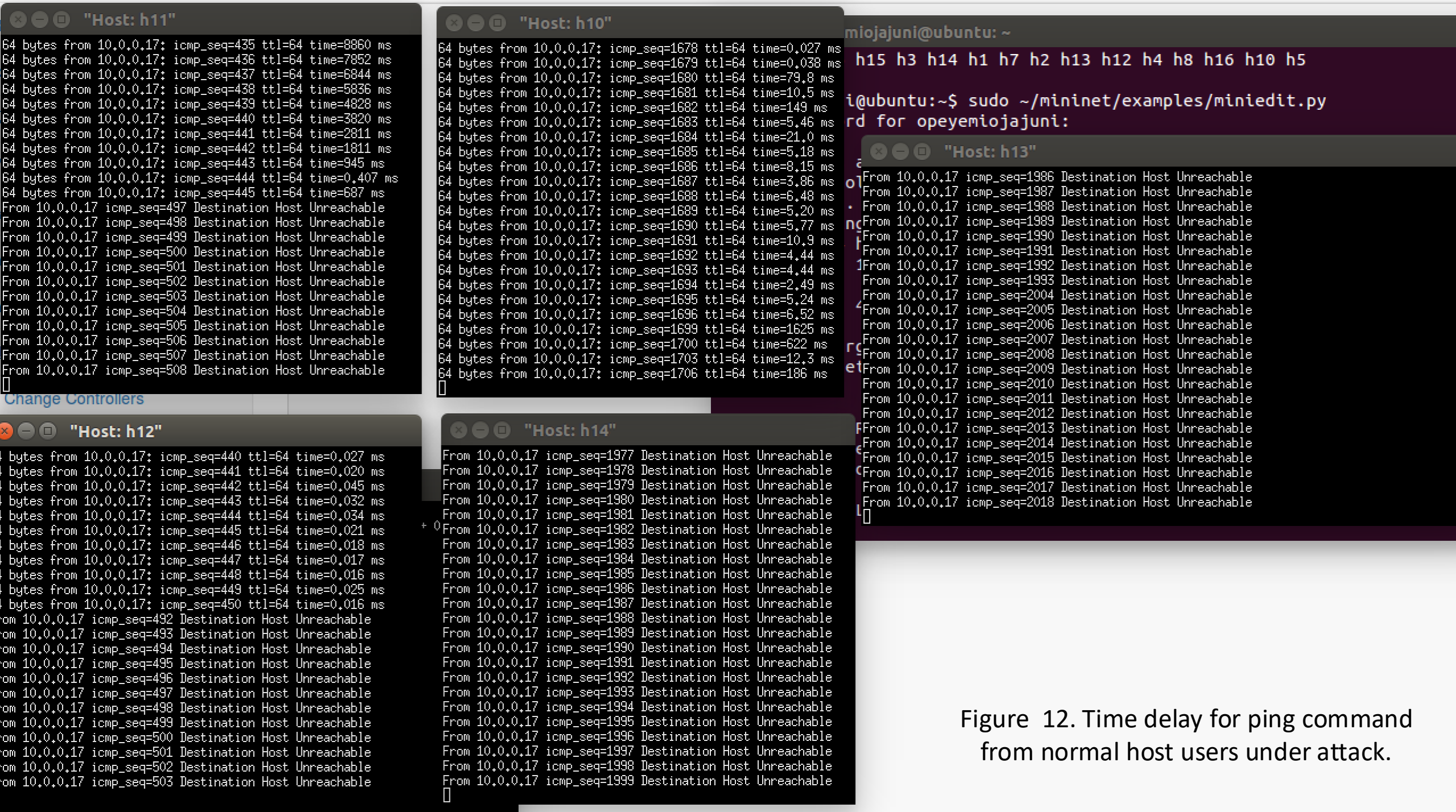

Figure 12. Time delay for ping command from normal host users under attack.

After Nodejs execute detection and mitigation Javascript

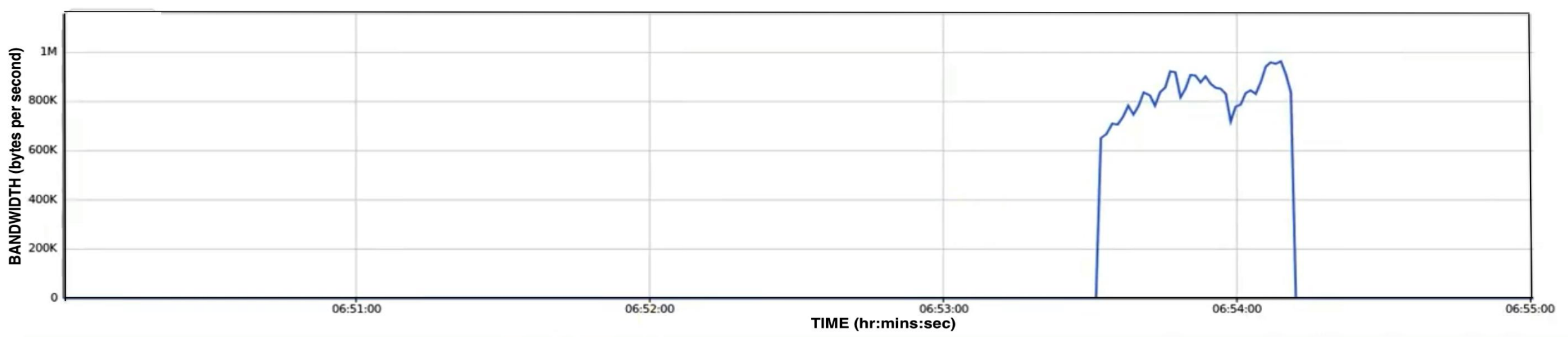

Figure 13. Network Bandwidth after Nodejs in SDN executes the detection and mitigation JavaScript.

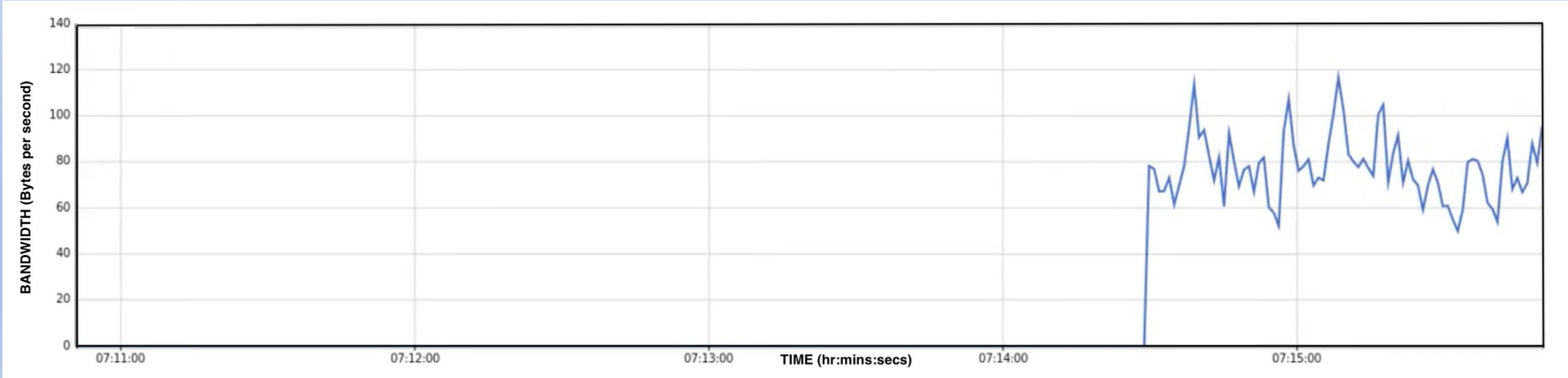

Figure 14. Network bandwidth Threshold

Limitation ,Conclusion and Future work

- Results show the efficacy of SDN in detecting and mitigating DDoS attack.

The limitation of the proposed framework are

- Detection of malicious traffic below the control bandwidth limit and the detection of the attacker.
- System considered only static threshold for bandwidth limit.

Future work will consider dynamic threshold for bandwidth limit.

Reference

- [1] Y. Lu and L. Da Xu, “Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics,” IEEE Internet of Things Journal, pp. 1–1, 2018.
- [2] L. D. Xu, W. He, and S. Li, “Internet of Things in Industries: A Survey,” IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.
- [3] “Cisco Visual Networking Index: Forecast and Trends, 2017–2022,” Cisco. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html. [Accessed: 09-Feb-2019].
- [4] “Internet of Things at a glance Cisco,” *Cisco*. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf. [Accessed: 08-Feb-2019].
- [5] M. Mukherjee et al., “Security and Privacy in Fog Computing: Challenges,” IEEE Access, vol. 5, pp. 19293–19304, 2017.
- [6] R. K. L. Ko et al., “TrustCloud: A Framework for Accountability and Trust in Cloud Computing,” in 2011 IEEE World Congress on Services, Washington, DC, USA, 2011, pp. 584–588.
- [7] S. T. Zargar, J. Joshi, and D. Tipper, “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks,” IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013.
- [8] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, “A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things,” IEEE Communications Magazine, vol. 56, no. 2, pp. 30–36, Feb. 2018.
- [9] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona, “IoDDoS — The Internet of Distributed Denial of Sevice Attacks - A Case Study of the Mirai Malware and IoT-Based Botnets:,” in Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, Porto, Portugal, 2017, pp. 47–58.

- [10] Q. Yan, F. R. Yu, Q. Gong, and J. Li, “Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges,” IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 602–622, 2016.
- [11] M. E. Ahmed and H. Kim, “DDoS Attack Mitigation in Internet of Things Using Software Defined Networking,” in 2017 IEEE Third International Conference on Big Data Computing Service and Applications (BigDataService), Redwood City, CA, USA, 2017, pp. 271–276.
- [12] N. Z. Bawany, J. A. Shamsi, and K. Salah, “DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions,” Arabian Journal for Science and Engineering, vol. 42, no. 2, pp. 425–441.
- [13] S. M. Mousavi and M. St-Hilaire, “Early detection of DDoS attacks against SDN controllers,” in 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 2015, pp. 77–81.
- [14] D. Yin, L. Zhang, and K. Yang, “A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework,” IEEE Access, vol. 6, pp. 24694–24705, 2018.
- [15] N. Dayal, P. Maity, S. Srivastava, and R. Khondoker, “Research Trends in Security and DDoS in SDN,” Security and Communication Networks, vol. 9, no. 18, pp. 6386–6411, 2016.
- [16] N. Z. Bawany, J. A. Shamsi, and K. Salah, “DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions,” Arabian Journal for Science and Engineering, vol. 42, no. 2, pp. 425–441.
- [17] “sFlow-RT.” sFlow-RT 2019, [Online]. Available: https://sflow-rt.com /. [Accessed: 14-Feb-2019].

QUESTIONS ?

THANK YOU