Detection and Mitigation Mechanisms for Attacks in Programmable Data Planes

1. Background

- Growing rate and size of attacks on networks (DDoS and others) [1]
- Fixed black-box implementation in modern routers, switches and modems
- Emerging of programmable devices due to SDN and since 2014 also P4 [2]
- New technologies, new areas of attack

2. Research Question

Which detection and mitigation mechanisms can be implemented to prevent DDoS and SYN-flood attacks?

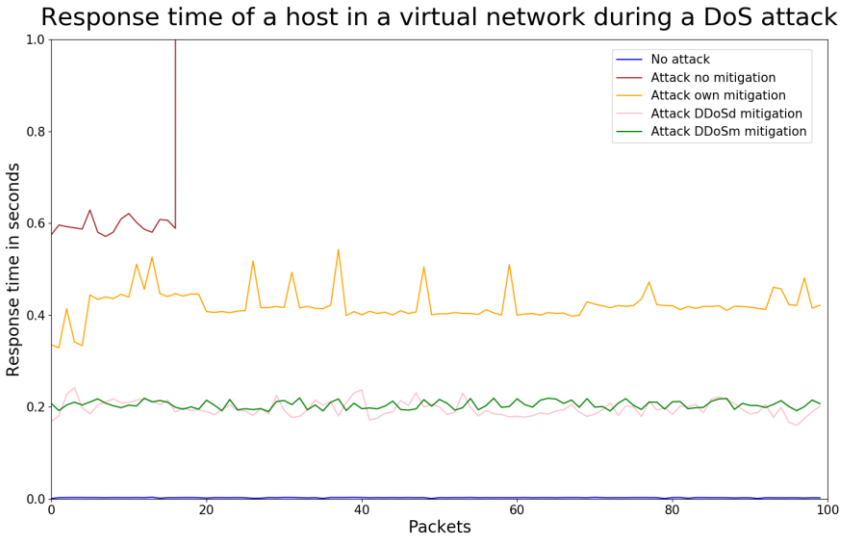
More information

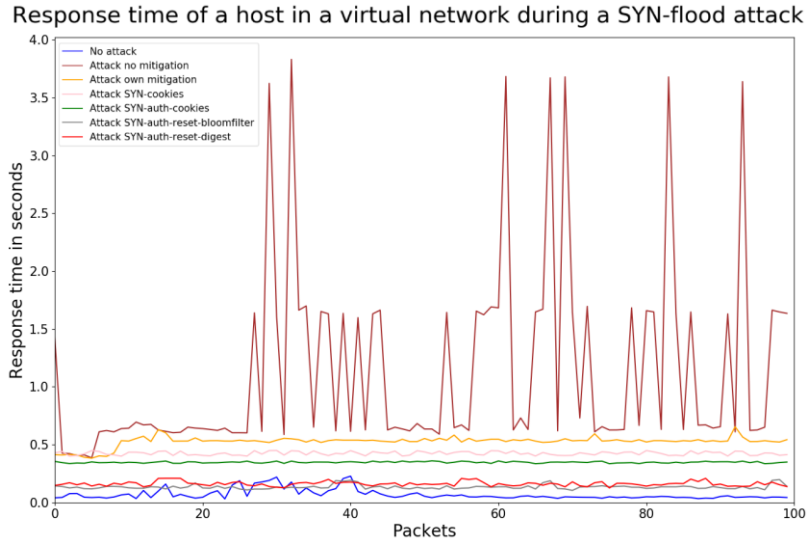
- Author: Frank Broy
  Email: f.r.f.broy@student.tudelft.nl
- Supervisor: Chenxing Ji
- Professor: Fernando Kuipers

3. Method

- Create a virtual network using Mininet and simulate different kinds of attacks
- Implement detection mechanisms in P4 and document which attacks are detected
- Implement mitigation mechanisms in P4 and see if there is an improvement in network performance during an attack
- Compare the different results and find the best practices

4. Results





5. Conclusion

- Many new methods, such as machine learning and Blockchain, are coming up
- Occurrence counting proves very effective
- P4 allows for very flexible packet treatment and analysis

6. References

- [1]https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/
- [2] https://p4.org

TU Delft