Machine Learning Approaches for Detection of DoS Attacks in IoT Networks

Adrian Gruszczynski

Institute of Computer Science
Freie Universität Berlin

Seminar IoT & Security, May 2022

Table of Contents

Motivation

- Internet of Things is constantly developing
  - Estimated 20.4 billion connected devices worldwide in 2022 [1]
  - Applications in various domains e.g. smart cities, smart healthcare, autonomous vehicles, industry 4.0, smart grids, etc.
- Security and privacy are crucial
  - Challenging constrains due to hardware and networking limitations
  - Heterogeneous networks producing large amounts of data
- Fertile ground for privacy and security attacks

Motivation

- Insecure IoT devices may threaten critical Internet infrastructure
  - Using vulnerable consumer IoT devices becomes a common technique for orchestrating DDoS attacks
  - Mirai botnet disrupted DNS service of Dyn and significantly limited accessibility of popular services such as Github, Netflix and Amazon
- Intelligent system monitoring leveraging ML/DL methods provides a solution for threat detection
  - Anomaly detection can facilitate detection of malicious traffic
  - Prediction of future attacks by learning from existing examples

Preliminary report structure

- Introduction
  - What is the domain?
  - What are the challenges?
  - Why is it important?
- Background and related work
  - Network anomaly detection
  - ML/DL for IoT security
  - DDos attacks in IoT networks
- Theoretical framework and architectural design
  - System architecture and performance measures
  - k-nearest neighbours
  - Boosting
  - Artificial neural network
- Discussion
- Conclusion

Related work

- A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security (IEE Communications Surveys & Tutorials, cited by 425)
- Real-time anomaly detection systems for Denial-of-Service attacks by weighted k-nearest-neighbor classifiers (Expert Systems with Applications, cited by 151)
- Machine Learning DDoS Detection for Consumer Internet of Things Devices (2018 IEEE Security and Privacy Workshops (SPW), cited by 425)
- Boosting-Based DDoS Detection in Internet of Things Systems (IEEE Internet of Things Journal 2022, cited by 20)
- Detection of known and unknown DDoS attacks using Artificial Neural Networks (Neurocomputing, cited by 307)

Report schedule

- 10th May 2022: Presentation
- Report outline, finish draft introduction and related work, start working on methods
- 8th June 2022: Preliminary version of the report
- Finish methods, discussion and conclusion, correct spelling, create slides for presentation
- 3rd July 2022: Deadline for report submission
- 6th July 2022: Final presentation

References

David Furlonger Rajesh Kandaswamy. *Blockchain-Based Transformation*. https://www.gartner.com/en/doc/3869696-blockchain-based-transformation-a-gartner-trend-insight-report. Accessed on 2022-05-08.