Machine Learning Approaches for Detection of DDoS Attacks in IoT Networks

Adrian Gruszczynski

Institute of Computer Science
Freie Universität Berlin

Seminar IoT & Security, July 2022

Table of Contents

Table of Contents

Introduction

- Internet of Things is constantly developing
  - Estimated 20.4 billion connected devices worldwide in 2022 [9]
  - 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
  - Low security standards, devices use default credentials [2]
- Fertile ground for privacy and security attacks

Introduction

- Insecure IoT devices may threaten critical Internet infrastructure [6]
  - 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 [12]
  - Prediction of future attacks by learning from existing examples
  - Malware recognition

Table of Contents

Botnets

- Group of devices infected by malware
- The size varies from hundreds to hundreds of thousands of devices [2]
- Can be controlled remotely by an attacker to execute malicious activities
  - Phishing
  - Spamming
  - DDoS
- IoT provides an ideal foundation for botnets and carrying out DDoS attacks
  - Easy target due to low security measures in IoT
  - High number of hackable devices
  - Massive pool of legitimate IP addresses and sources of traffic

DDoS

- Cyberattack that targets a host, network or infrastructure [2]
- The goal is to render the target unavailable for others by exhausting its resources (Bandwidth, Memory, CPU, etc.)
- Attacks on critical internet infrastructure (DNS) have an enormous impact
- Thanks to the broad availability of botnets DDoS is a simple yet powerful weapon
- DDoS attacks happen on two levels:
  - Network-level: exploits network layer protocols e.g. TCP, UDP, IP, etc.
  - Application-level: exploits application layer protocols e.g. HTTP, DNS, etc.
- There is a number of DDoS techniques including:
  - Amplification: generate most traffic with least amount of bandwidth
  - Reflection: used in combination with IP-spoofing to hide the origin IP

- DDoS capable malware that first appeared in 2016
- Responsible for the biggest scale DDoS attack ever recorded peaking at 1.2Tbps [2]
  - Rendered popular internet services unavailable (Github, Netflix, Amazon, etc.)
  - Impacted United States and Europe
- Botnet of approximately 500k compromised devices
- Source code was published causing a number of similar attacks to follow

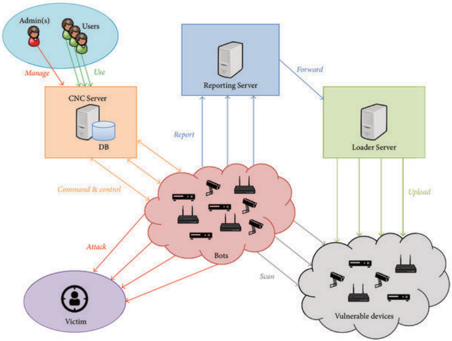

Figure: Mirai logical infrastructure [2]

Machine learning 101 - Basics

- Allows for solving of complex problems without a predefined set of rules [4]
- Tasks include classification, anomaly detection and translation
- Classification based on training approach:
  - Supervised: requires pairs of input x and output y, want to learn mapping from x to y (classification, regression)
  - Unsupervised: uses unlabelled data to extract latent patterns (clustering, denoising, compression)

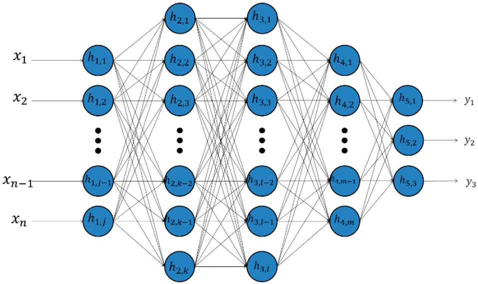

Figure: Visual representation of a feed forward neural network [1].

Machine learning 101 - Optimisation

- Dataset divided into training and test part
- Model sees the entire training data example by example and tries to predict the output given an input
- It learns the dependencies by adjusting its internal parameters to minimise the prediction error
- The learning takes place using stochastic gradient descent and backpropagation
- After training models gets evaluated with the test data to assess real performance on unseen data

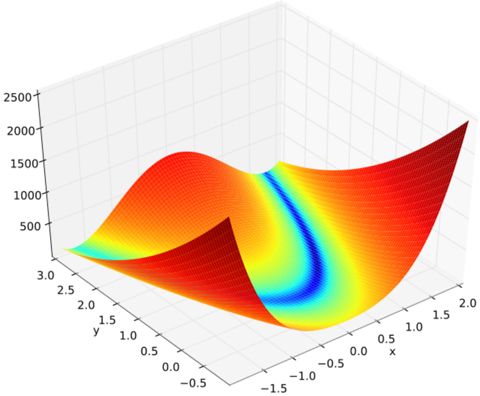

Figure: Visual representation of a 2D loss landscape [4].

Machine learning 101 - Performance Measures

- Performance of a model depends on a problem
- Accuracy for classification: ratio of correctly predicted examples to all predicted
- Mean Squared Error (MSE) for regression tasks
- For unsupervised tasks performance metrics are problem dependent

		y Positive	Negative
$\hat{y}$	Positvive	a	b
	Negative	c	d
	Total	$a + c$	

Table: Confusion matrix.

Table of Contents

Convolutional Neural Network

- Ability to learn complex spatial dependencies in image data [4]
- Builds its own understanding of images by extracting high level feature representations
- Architecture is a combination of convolutional and pooling layers
  - Convolution works by shifting a filter through the input and computing a dot product
  - Pooling is a nonlinear down sampling of the input to reduce amount of information
- Broad range of application in image recognition, image segmentation, speech recognition, anomaly detection, etc.

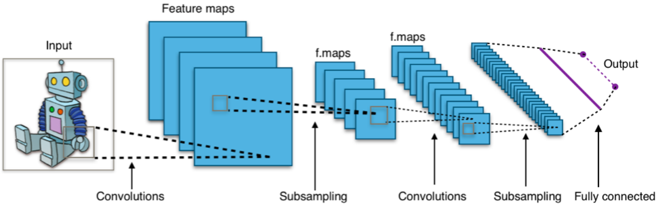

Figure: Convolutional neural network: visual representation [9].

Malware Detection Using Image Recognition

- Researchers visualised malware binaries as grayscale images [10]
- They used the images in combination with image recognition techniques for malware detection
- One study uses a convolutional neural network to classify images a malware or goodware based
- They use IoTPOT [11] data that has examples of malware binaries from two families: Mirai and Gafgyt
- The authors propose a 2-tier architecture
  - Lightweight convolutional neural network that runs on the IoT device
  - The device can detect suspicious software with roughly 94% accuracy
  - Software classified as malware gets sent to the cloud for further examination

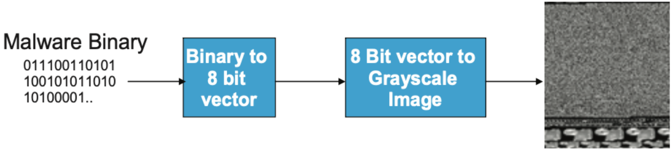

Figure: Visualising malware as 8-bit grayscale images [8].

Table of Contents

Discussion

- Authors show that on-device deep learning is a feasible approach
- The proposed method is vulnerable to obfuscation and encryption
- It is questionable how well this generalizes to new malware families
- Models have to be re-trained and re-distributed
- In contrast to network-based DDoS detection this method requires tampering with devices

Conclusion

- Machine and deep learning show great potential for anomaly and malware detection [4]
- Deep learning methods enable learning complex patterns without manual feature engineering [4]
- The researchers use data of DDoS traffic simulated in a lab environment [7], [3]
  - Difficult to compare results
  - Questionable real life performance
- Low availability of public datasets for DDoS and DDoS malware detection
- Methods that detect unknown attacks show high potential [7]
- On-device anomaly and malware detection is not well researched yet
- Regulatory approaches seem promising in long term [5]
- Ease of integration into existing systems plays key role [3]
- Future research should focus on transfer learning, autoencoders and unsupervised learning

References

Daniel Berman et al. "A Survey of Deep Learning Methods for Cyber Security". In: *Information* 10 (Apr. 2019), p. 122. DOI: 10.3390/info10040122.

Michele De Donno et al. "DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation". In: *Security and Communication Networks* 2018 (Feb. 2018), pp. 1–30. DOI: 10.1155/2018/7178164.

Rohan Doshi, Noah Apthorpe, and Nick Feamster. "Machine Learning DDoS Detection for Consumer Internet of Things Devices". In: May 2018, pp. 29–35. DOI: 10.1109/SPW.2018.00013.

Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep Learning*. MIT Press, 2016. URL: http://www.deeplearningbook.org.

James Jerkins. "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code". In: Jan. 2017, pp. 1–5. DOI: 10.1109/CCWC.2017.7868464.

Constantinos Kolias et al. "DDoS in the IoT: Mirai and other botnets". In: *Computer* 50 (Jan. 2017), pp. 80–84. DOI: 10.1109/MC.2017.201.

Yair Meidan et al. "N-BaIoT—Network-Based Detection of IoT Botnet