DDoS Network Intrusion Detection and Classification

Karla Muller

Introduction

- What is a DDoS attack?
  - A distributed network of compromised systems aiming to exhaust a network resources
  - Meant to bring server offline, steal data, or/and as a distraction from other malware infections
- Why is it important?
  - With an increase in IoT devices and Cloud computing comes an increase in scale, strength and variety of DDoS attacks
  - Detecting “bad traffic” in time could help save not only the IT systems but also the business reputation of a company

Data

- CICDDos2019 was generated by a team of researchers at Canadian Institute of Cybersecurity in UNB
- It contains benign traffic as well as the most up-to-date common DDoS attacks:
  - MSSQL
  - LDAP
  - NetBIOS
  - Syn
  - UDP
  - And others…

Clean-up

- Clean-up steps:
  - Converted my Labels to binary: BENIGN: 0 , ATTACK: 1
  - Dropped non-numeric identifiers: Unnamed: 0','Flow ID', ' Source IP', ' Timestamp', Destination IP', 'SimillarHTTP'
  - Converted object columns 'Flow Bytes/s' and 'Flow Packets/s' to floats and their infinity values to max column value

- Used Lasso to shrink coefficients and decrease number of variables

	Start shape	End shape
MSSQL	(4524498, 88)	(4524498, 28)
LDAP	(2181542, 88)	(2181542, 19)
NetBIOS	(4094986, 88)	(4094986, 31)
Syn	(1582681, 88)	(1582681, 25)
UDP	(3136802, 88)	(3136802, 33)
all dfs	(620820, 82)	(599458, 82)

Preliminary Results

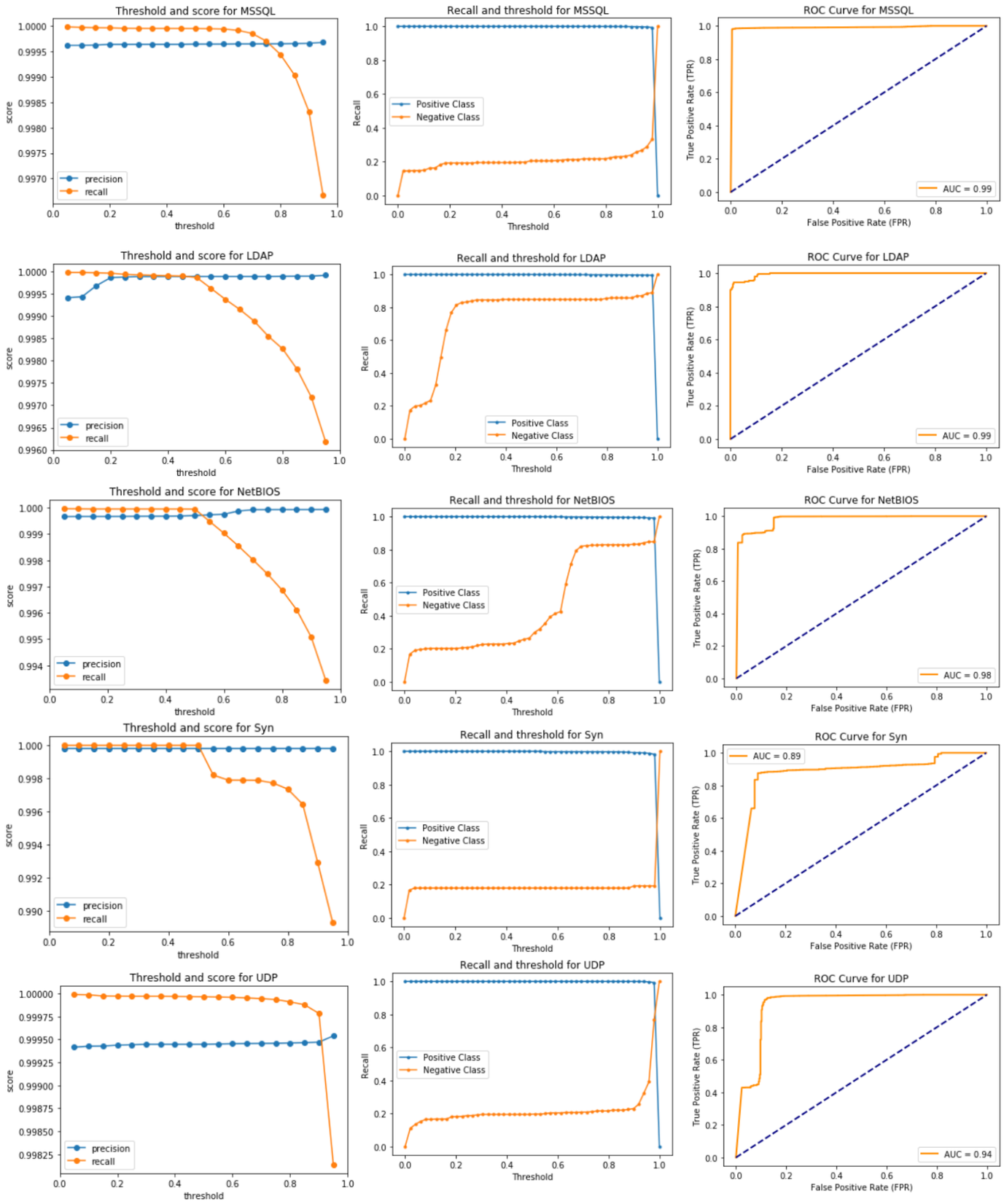
- MSSQL Logistic Regression with stratified split
  - Score on train: 0.99
  - Score on test: 0.99
  - Precision: 0.99
  - Recall: 0.99

	Predictec Class 0	Predicted Class 1
True 0	82	319
True 1	42	904457

- MSSQL Logistic Regression with SMOTE
  - Score on train: 0.94
  - Score on test: 0.90
  - Precision: 0.99
  - Recall: 0.89

	Predictec Class 0	Predicted Class 1
True 0	390	11
True 1	92565	811934

Logistic Regression Results

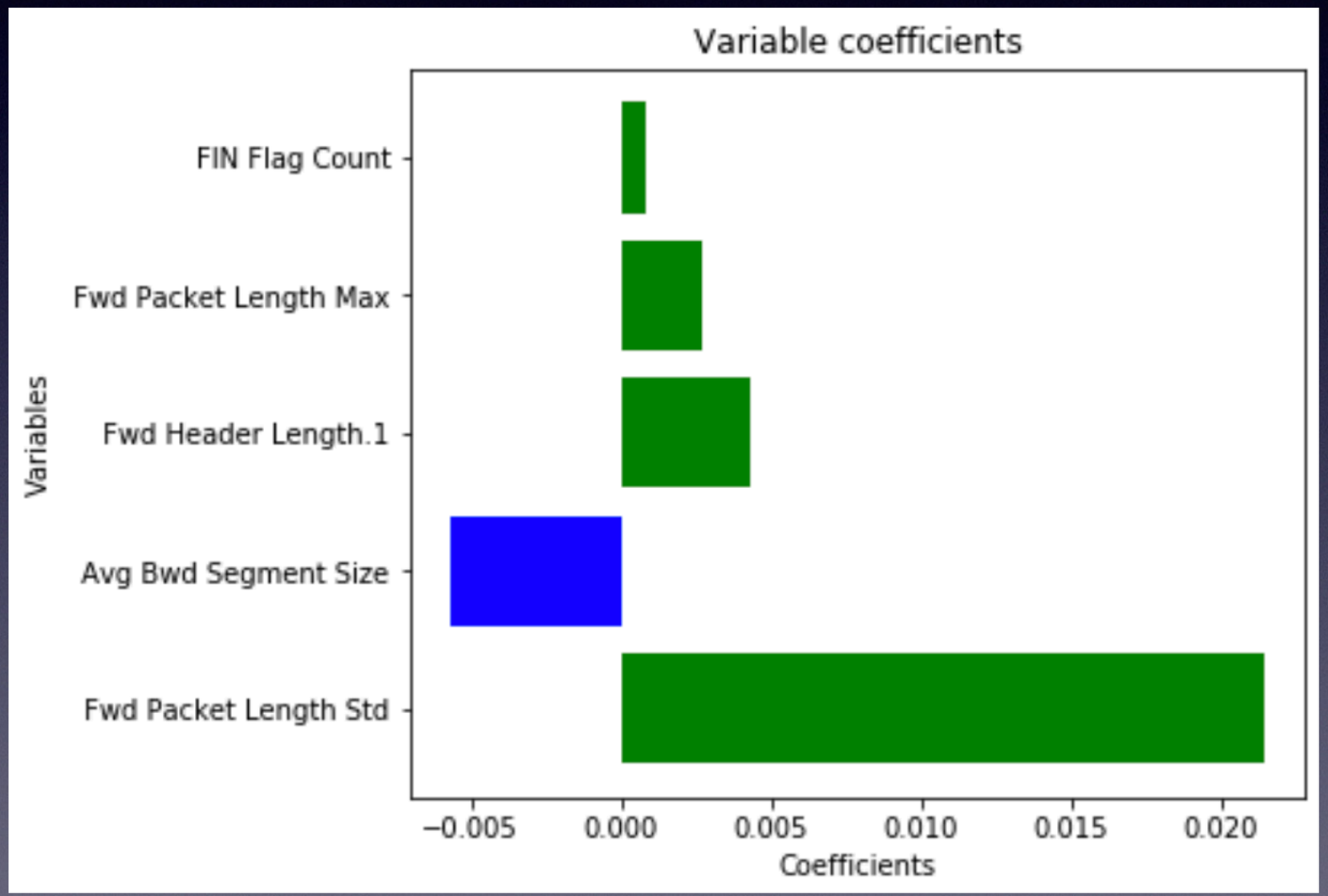


Decision Tree Classifier Results

- Score on train: 0.991579886814328
- Score on test: 0.991008574383611 9
- Confusion Matrix

	Predicted Class 0	Predicted Class 1	Predicted Class 2	Predicted Class 3	Predicted Class 4	Predicted Class 5
True 0	58	0	0	2	1	1
True 1	1	34816	221	7	0	122
True 2	0	9	17111	1	0	14
True 3	0	398	0	31300	0	7
True 4	0	0	0	0	11076	0
True 5	2	280	10	2	0	24453

My Top 5 Variables



Plan of Action

- What is your plan for the next two weeks?
  - Trying to improve models
    - Decrease overfitting
      - Using other SMOTEs
      - Feeding new data into my models
    - Comparing results to other models
- Investing time in model interpretation, feature importance, data visualization and time series of attacks

Interesting DDoS Stats

- Global estimates of the total number of DDoS attacks are anticipated to double to 14.5 million by 2022, according to Cisco's Visual Networking Index (VNI)
- Attacks can represent up to 25 percent of a country's total Internet traffic while they are occurring
- The largest application layer DDoS attack in history occurred in the spring of 2019 over a 13-day stretch. Imperva reported the attack, which targeted a streaming service client, and peaked at 292,000 requests per second (RPS).
- An increasing trend of what researchers refer to as strategic, "low-intensity incursions" that degrade the performance of servers over time uses lowball attacks that enable hackers to carry out longer attacks that fall below the level of intensity that would trigger DDoS defences.
- With a current value of $2.4 billion in 2019, one research firm estimates the DDoS protection and mitigation market will nearly double to $4.7 billion by 2024. That's a compound annual growth rate (CAGR) of 14 percent.

- Cybersecurity Ventures

References and additional resources

- Data:
  - DDoS Evaluation Dataset (CICDDoS2019): https://www.unb.ca/cic/datasets/ddos-2019.html
  - Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India, 2019
- Stats slide:
  - Cybersecurity Ventures, The-15-top-ddos-statistics-you-should-know-in-2020: https://cybersecurityventures.com/the-15-top-ddos-statistics-you-should-know-in-2020/
- Cool real time map visualizations and data of DDoS attacks
  - Kaspersky. Cyberthreat Realtime Map: https://cybermap.kaspersky.com/
  - Norse Corp Top 15 Live Cyber Attack Maps for Visualizing Digital Threat Incidents: https://norse-corp.com/map/