Network Security CS G513
Final Project Evaluation

Characterizing and Classifying IoT Traffic in Smart Cities and Campuses

Team 24
Aashita Dutta (2020H1030130H)
Pavan Prabhu (2020H1030108H)

Introduction

1. Problem:
- Lack of visibility in IoT devices
- consolidating network traffic may be troublesome
- Erroneous handling of smart system from different departments
- Vulnerability to critical cyber security attacks
2. How to resolve?
- Nature of IoT Traffic and why it is important?
- Data Traces Collection and Smart Environment setup
- Characterization and profiling of IoT Devices
- classification of IoT Devices

Category	Device	Mac Address	Wireless / Wired
Hubs	Smart Things	d0:52:a8:00:67:5e	Wired
	Amazon Echo	44:65:0d:56:cc:d3	Wireless
Cameras	Netatmo Welcome	70:ee:50:18:34:43	Wireless
	TP-Link Day Night Cloud camera	f4:f2:6d:93:51:f1	Wireless
	Samsung SmartCam	00:16:6c:ab:6b:88	Wireless
	Dropcam	30:8c:fb:2f:e4:b2	Wireless
	Insteon Camera	00:62:6e:51:27:2e / e8:ab:fa:19:de:4f	Wired / Wireless
	Withings Smart Baby Monitor	00:24:e4:11:18:a8	Wired
Switches & Triggers	Belkin Wemo switch	ec:1a:59:79:f4:89	Wireless
	TP-Link Smart plug	50:c7:bf:00:56:39	Wireless
	iHome	74:c6:3b:29:d7:1d	Wireless
	Belkin wemo motion sensor	ec:1a:59:83:28:11	Wireless
Air quality sensors	NEST Protect smoke alarm	18:b4:30:25:be:e4	Wireless
	Netatmo weather station	70:ee:50:03:b8:ac	Wireless
Healthcare devices	Withings Smart scale	00:24:e4:1b:6f:96	Wireless
	Blipcare Blood Pressure meter	74:6a:89:00:2e:25	Wireless
	Withings Aura smart sleep sensor	00:24:e4:20:28:c6	Wireless
Light Bulbs	LiFX Smart Bulb	d0:73:d5:01:83:08	Wireless
Electronics	Triby Speaker	18:b7:9e:02:20:44	Wireless
	PIX-STAR Photo-frame	e0:76:d0:33:bb:85	Wireless
	HP Printer	70:5a:0f:e4:9b:c0	Wireless

(b) List of IoT devices in the smart environment.

Workflow

- Extract the feature vectors from the available .pcap files.
- Extracting the device specific (LiFX light bulb and Macbook) attributes to analyze the load, burstiness, protocols, DNS- NTP Requests etc.
- Importing selecting packet's attributes to SQLite with scapy.
- Plotting graphs based on selected features in SQLite table.
- Overall graphical representation of the features.
- Some Assumptions: Each session is 30 mins

Libraries Used

Note: Earlier we were using pyshark to analyse pcap files and csv to export data. But now we are using scapy and SQLite.

- Scapy - To parse the .pcap files and extract the necessary data/features into the SQLite tables.
- SQLite - To store data in sqlite database.
- Pandas - To clean and preprocess data.
- Numpy - To work with arrays.
- Matplotlib - To plot graphs, histograms to represent the results visually.

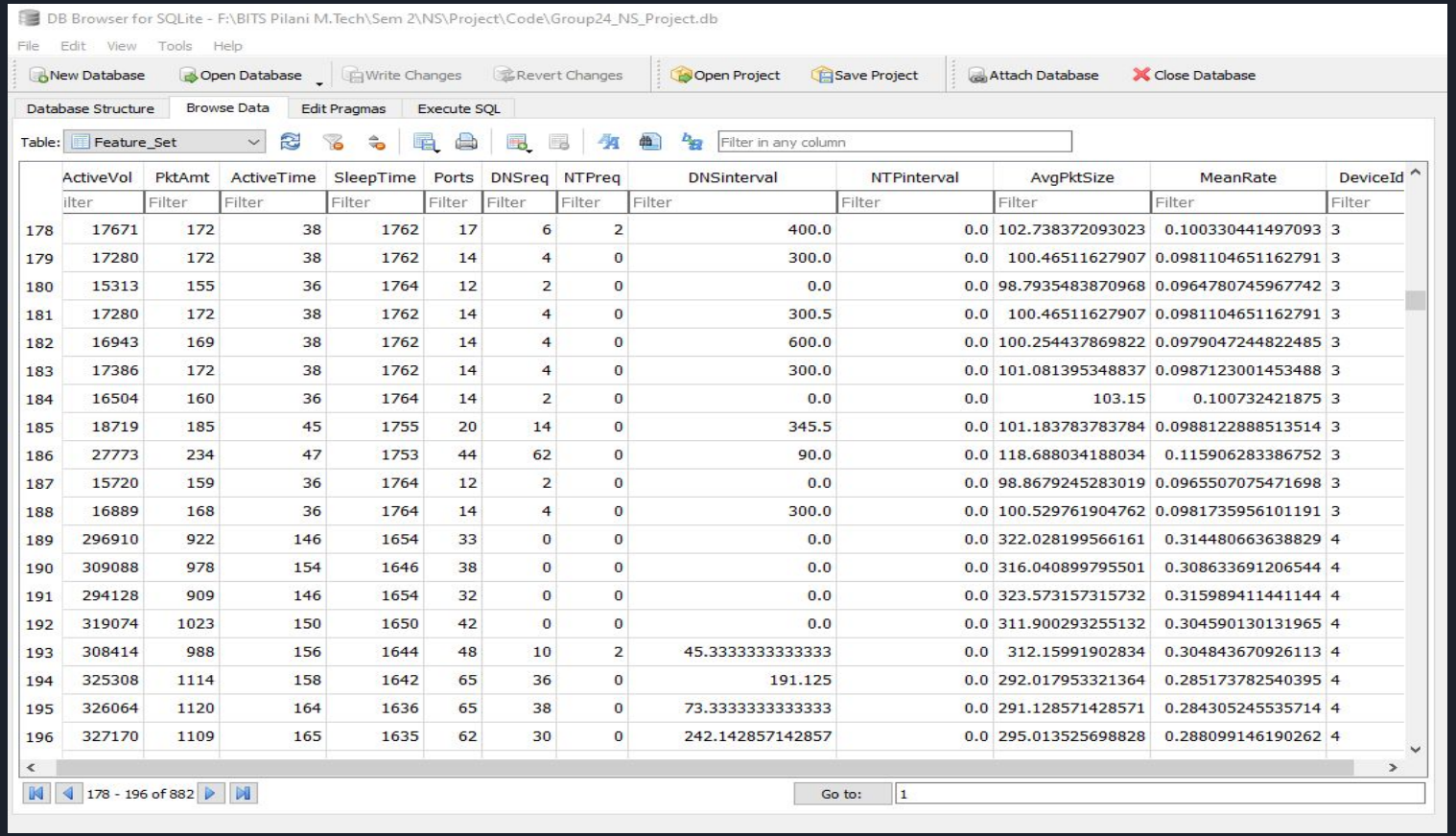
Dataset Source

- This paper provides the trace data openly available for download at: http://149.171.189.1/.
- The size of the data captured varies between 100 MB and 4 GB, with an average of 356 MB.
- Traces, collected over a period of 2 weeks stored as pcap files.
- Over 20 IoT devices deployed to trace data.
- Pcap files helped fetching attributes like sleep time, burst rate, packet size, volume, ports, protocols etc.

Data Visualization

1. With the extracted attributes, we are plotting the following histogram/bar graphs using matplotlib for specific devices like LiFx Light Bulb and Macbook:
   - Load(kBps) vs Time (Hrs)
   - Active Time vs Daily Time
   - Sleep Time vs Hours
   - Average Packet Size vs Time
   - Port vs Frequency
   - Probability of Port Numbers vs Destination Port Number
2. Attributes List fetched in Table:
   - Active Volume,
   - Packets Count
   - Active time,
   - Sleep Time,
   - Ports,
   - DNS Requests,
   - NTP Requests,
   - DNS Interval,
   - NTP Interval,
   - Average Packet Size,
   - Mean Rate of traffic load,
   - Device Id

Tabular Results - Features Extracted


DB Browser for SQLite - F:\BITS Pilani M.Tech\Sem 2\NS\Project\Code\Group24_NS_Project.db

File Edit View Tools Help

New Database | Open Database | Write Changes | Revert Changes | Open Project | Save Project | Attach Database | Close Database

Database Structure | Browse Data | Edit Pragmas | Execute SQL

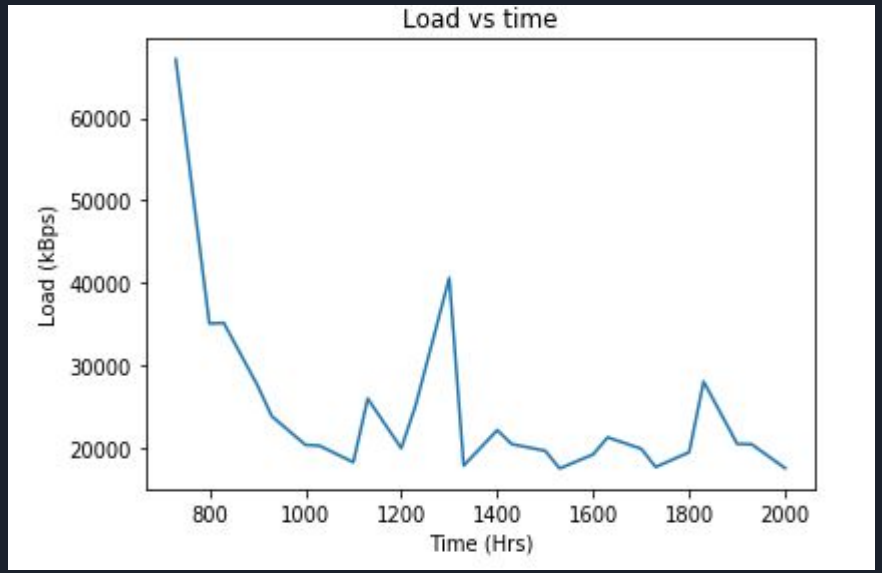
Table: Feature_Set | Filter in any column

	ActiveVol	PktAmt	ActiveTime	SleepTime	Ports	DNSreq	NTPreq	DNSinterval	NTPinterval	AvgPktSize	MeanRate	DeviceId
	ilter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
178	17671	172	38	1762	17	6	2	400.0	0.0	102.738372093023	0.100330441497093	3
179	17280	172	38	1762	14	4	0	300.0	0.0	100.46511627907	0.0981104651162791	3
180	15313	155	36	1764	12	2	0	0.0	0.0	98.7935483870968	0.0964780745967742	3
181	17280	172	38	1762	14	4	0	300.5	0.0	100.46511627907	0.0981104651162791	3
182	16943	169	38	1762	14	4	0	600.0	0.0	100.254437869822	0.0979047244822485	3
183	17386	172	38	1762	14	4	0	300.0	0.0	101.081395348837	0.0987123001453488	3
184	16504	160	36	1764	14	2	0	0.0	0.0	103.15	0.100732421875	3
185	18719	185	45	1755	20	14	0	345.5	0.0	101.183783783784	0.0988122888513514	3
186	27773	234	47	1753	44	62	0	90.0	0.0	118.688034188034	0.115906283386752	3
187	15720	159	36	1764	12	2	0	0.0	0.0	98.8679245283019	0.0965507075471698	3
188	16889	168	36	1764	14	4	0	300.0	0.0	100.529761904762	0.0981735956101191	3
189	296910	922	146	1654	33	0	0	0.0	0.0	322.028199566161	0.314480663638829	4
190	309088	978	154	1646	38	0	0	0.0	0.0	316.040899795501	0.308633691206544	4
191	294128	909	146	1654	32	0	0	0.0	0.0	323.573157315732	0.315989411441144	4
192	319074	1023	150	1650	42	0	0	0.0	0.0	311.900293255132	0.304590130131965	4
193	308414	988	156	1644	48	10	2	45.3333333333333	0.0	312.15991902834	0.304843670926113	4
194	325308	1114	158	1642	65	36	0	191.125	0.0	292.017953321364	0.285173782540395	4
195	326064	1120	164	1636	65	38	0	73.3333333333333	0.0	291.128571428571	0.284305245535714	4
196	327170	1109	165	1635	62	30	0	242.142857142857	0.0	295.013525698828	0.288099146190262	4

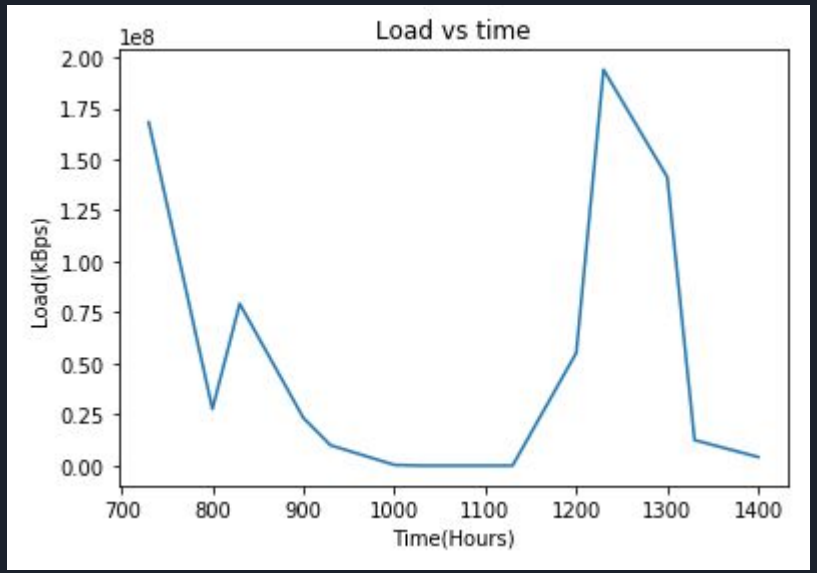
178 - 196 of 882 | Go to: 1

Graphical Results
Load vs Time

Light Bulb

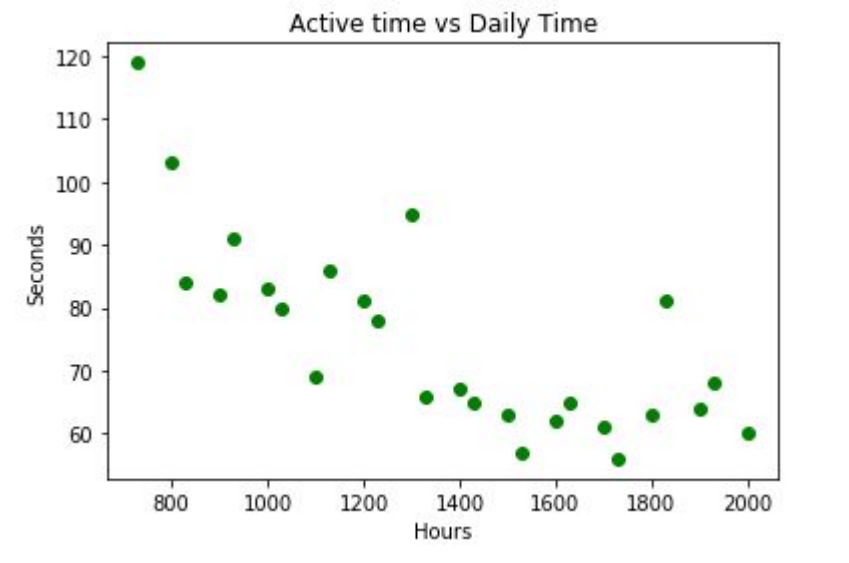


Macbook

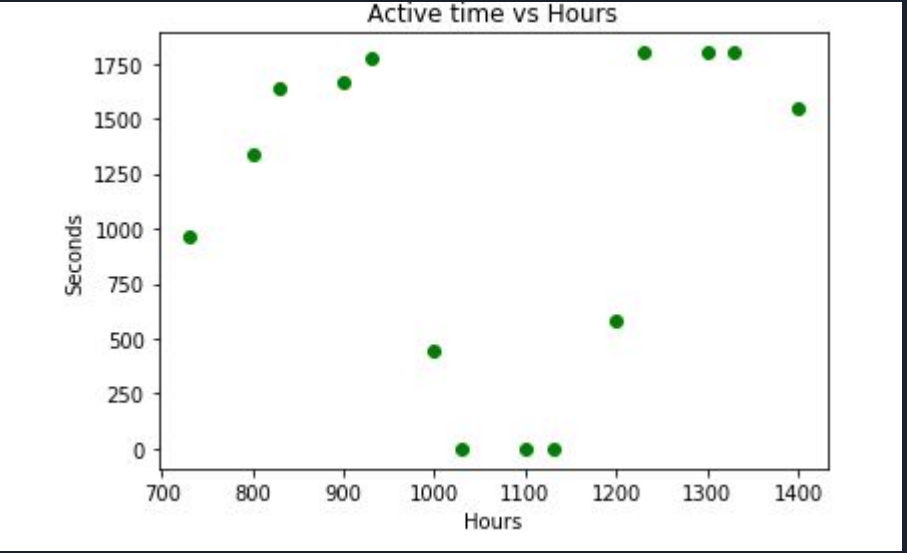


Active time vs Daily Time

Light Bulb

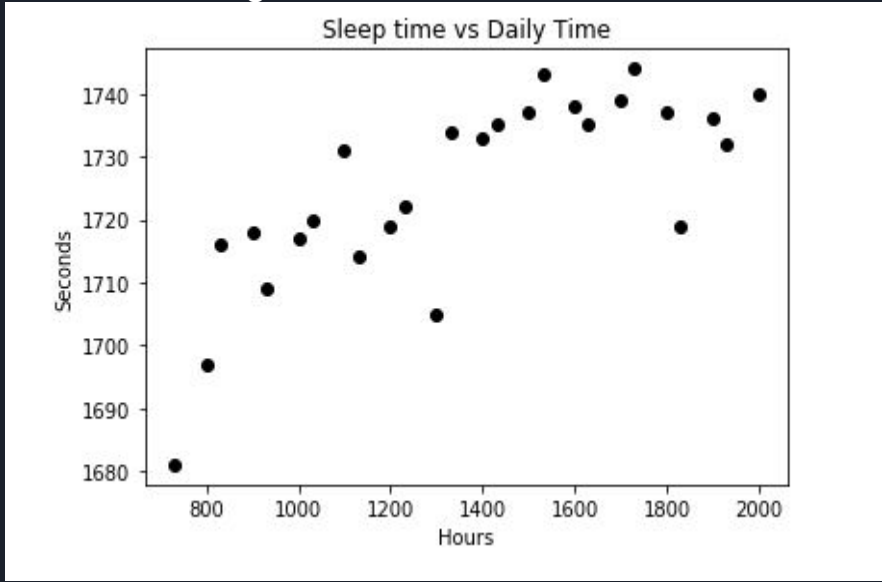


Macbook

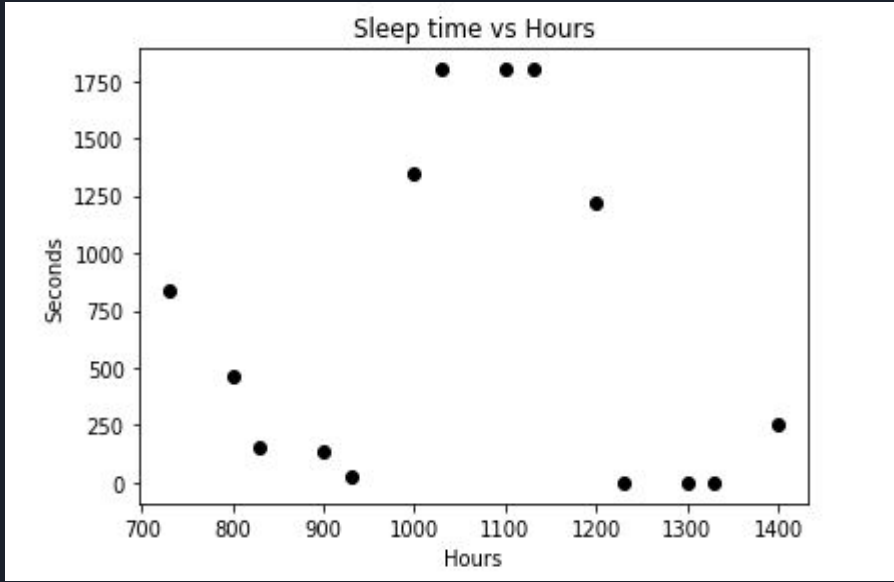


Sleep time vs Hours

Light Bulb

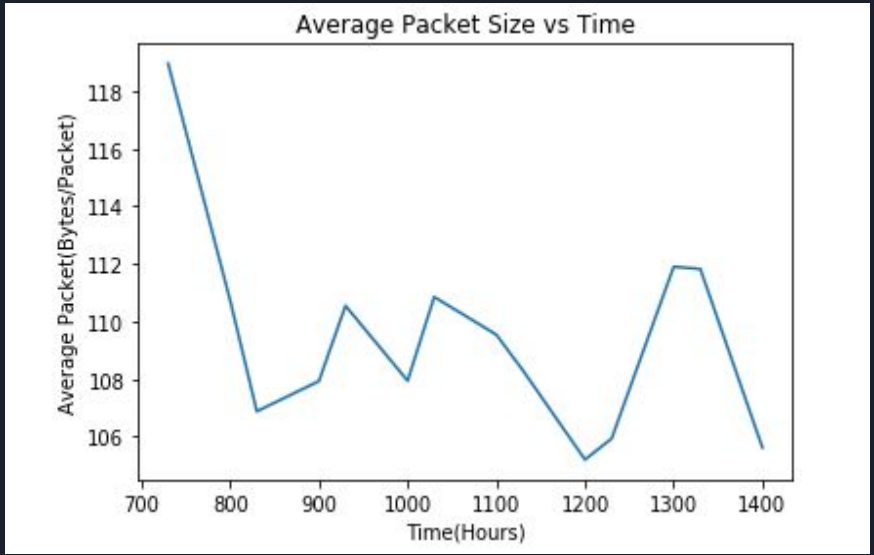


Macbook

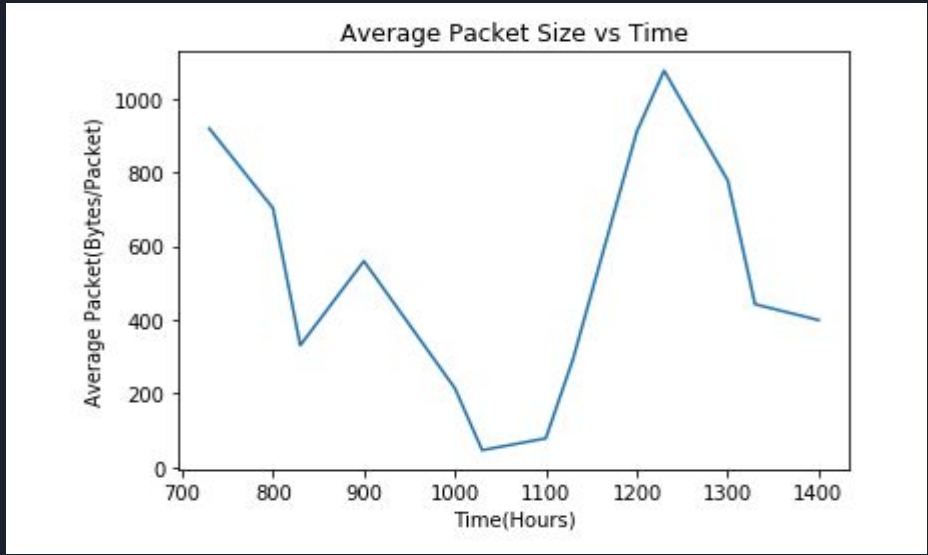


Average Packet Size vs Time

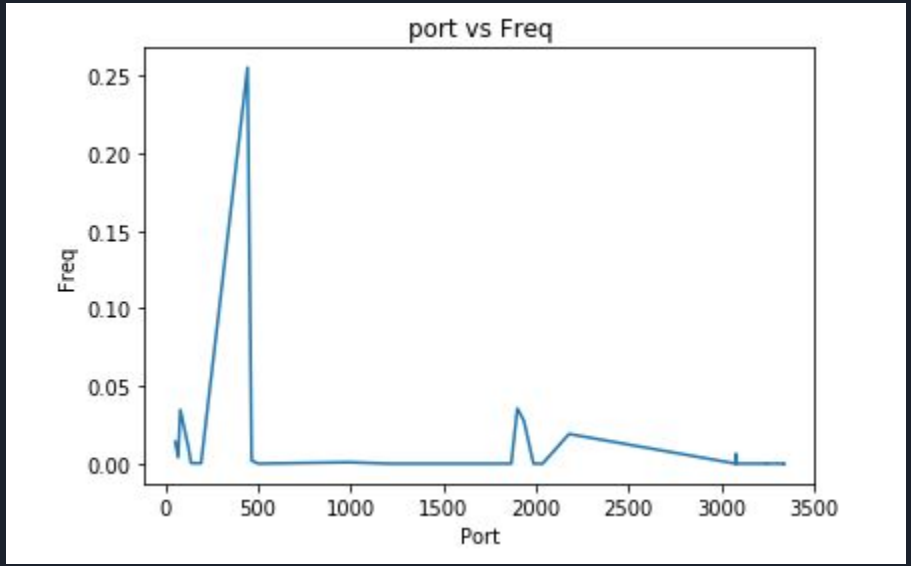
Light Bulb



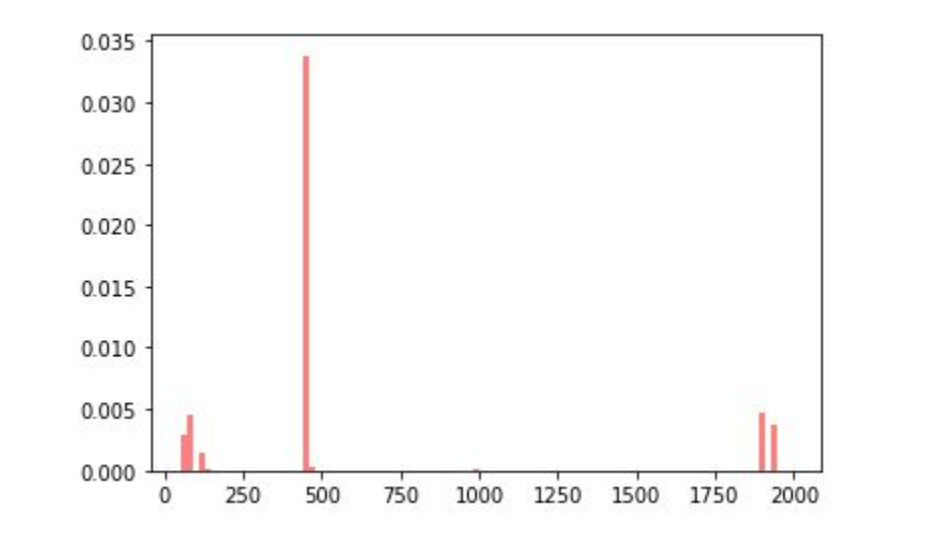
Macbook



Port vs Frequency



Probability of Port number vs Destination Port Number



Future Prospects

- This paper sets the stage for future performance in IoT devices characterization and classification with open-source data availability.
- Since the actual behaviour or actual graph about devices is not described, so its difficult to track how the devices are compromised for cyber attacks without knowing what “normal” IoT traffic profile looks like.
- Since about 45% of IoT traffic is not being transferred over HTTPS that shows its prone to various attacks but rest 55% comprises the traffic that we are not sure of.

THANK YOU