Cyber Attack analysis on IoT devices (CICIoT2023)

David Dai*[1,2]

[1]*Student ID: 235821890*
[1]*daix1890@mylaurier.ca*

Abstract

This project attempts to determine the effectiveness and efficiency of different machine learning techniques in identifying the benign and malicious network package and categorize the the type of security attack targeting Internet of Things(IoT) devices in the network. Logistic Regression, Random Forests and Deep Neural Network techniques will be used for prediction.

1 Description of Applied Problem

Nowadays, the Internet of Things(IoT) plays important roles in everyday life and has enabled many industries to be more intelligent. In the last decade, IoT connections surged[Cis20] and is predicted to keep growing rapidly[SKS+20]. This new paradigm relies on an extensively connected sensors and actuators network with multiple devices producing network traffic[MNG+17][DMD+22].

Conversely, several challenges still need to be faced to ensure the efficiency and security of the systems.[NDG22][SKS+20] The development of new applications may also bring new requirements to the systems [SK19]. For example, mission-critical applications, such as self-drive vehicles or smart medical devices requires more restrictive response times than common IoT applications.

The goal of this project to measure the effectiveness and efficiency of common machine learning techniques in identifying malicious attacks on connected IoT devices and differentiating their category using CICIoT2023 IoT security dataset[NDF+23].

2 Description of Available Data

2.1 Lab environment and Network Topology

The production of CICIot2023 IoT security dataset was conducted in Canadian Institute for Cybersecurity (CIC) IoT Lab. The experiment comprised 105 IoT devices 4 : A total of 67 IoT devices were directly involved in the attacks and other 38 Zigbee and Z-Wave devices were connected to five hubs. 33 type of attacks were executed on these devices. The attacks can be classified into seven categories, namely DDoS, DoS, Recon, Web-based, brute force, spoofing, and Mirai.

This topology is divided into two parts. In the first part, an ASUS router connects the network to the Internet and a Windows 10 Desktop computer shares this connectivity. In addition, a Cisco switch is placed between this computer and a VeraPlus access point connecting 7 Raspberry Pi devices, acting as malicious attackers in the experiments. Then, the Cisco switch is connected to the second part through a Gigamon Network Tap. This network device collects all the IoT traffic and sends it to two network monitors, which are responsible for storing the traffic

*Project Proposal for CP-640: Machine Learning. Wilfrid Laurier University, Fall 2024

using wireshark. In the second part, a Netgear Unmanaged Switch is connected to five gateways and base stations to enable communication with IoT devices with protocols such as Zigbee and Z-Wave.

2.2 Benign and Malicious Scenarios

As depicted4, a network tap and two traffic monitors are dedicated to monitoring the network traffic and the network traffic is monitored using Wireshark. These two data streams are combined using mergecap[Bax14].

For each attack, a different experiment is performed targeting all applicable devices. In all scenarios, the attacks are performed by malicious IoT devices targeting vulnerable IoT devices. For example, DDoS attacks are executed against all devices, whereas web-based attacks target devices that support web aplications. Table 1 depicts the category and subcategory of attacks together and the tools used in each attack alongside the number of rows generated and captured.

2.3 Feature Extraction and Data Description

Figure 1 illustrates how the data generation, extraction, and labeling are conducted for each attack scenario (and benign scenario). The first phase relies on the use of different tools presented in Table 1 to execute attacks against IoT devices in the network. After that, the network traffic is captured in pcap format using Wireshark. Finally, for each attack executed, the entire traffic captured is labeled as belonging to that particular attack.

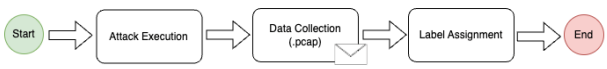

Figure 1: how to produce the dataset

Regarding the data processing step 2, the network traffic data is composed of captures of all attacks alongside benign traffic. Such huge chunk of data (about 548GB) is splited into 10MB by TCPDUMP in parallel, the feature of which is extracted using DPKT package and stored in seperate csv files. These features2 are extracted based on proposals present in the literature regarding IoT security. Furthere, the extracted features are group in window sizes of 10 or 100 based on different characteristics of attack category/subcategory to mitigate data size discrepancy (e.g., DDoS and CommandInjection) and basic statistics are calculated using Pandas and Numpy. Finally, subfiles are grouped into a processed csv dataset using Pandas. Thereupon, the resulting csv datasets represent the combination of features of each data chunk.

3 Analysis and Visualization Techniques

3.1 Pre-proccesing

As introduced in Feature Extraction, primitive feature extraction and data grouping as well as data cleaning has already been conducted before the dataset is release. However, the dataset is still as large as 13GB and with 47 features 2. Therefore, more shrinking/sampling of dataset should be done prior to further analysis. Fortunately, random sampling [kaga] on rows and feature importance study on columns/features[kagb] has already been worked out by community contributors to enable efficient analysis on the data.

Another challenge is that important features, such as IP address are missing for some IoT devices because these devices relies on protocols other than TCP/IP. I have to rely on other related features specific to that particular protocol, e.g. Zigbee or Z-Wave, to identify the device.

3.2 Analysis

In the original paper[NDF+23], Four Metrics, Accuracy, Recall, Precision and F1-Score, were used to measure the effectiveness of the machine learning models. This project will continue to use these criteria to measure the performance of machine learning algorithms3. and Logistic Regression and Random Forest will be reused to classify the attack categories and compare with the result gained in the original paper.

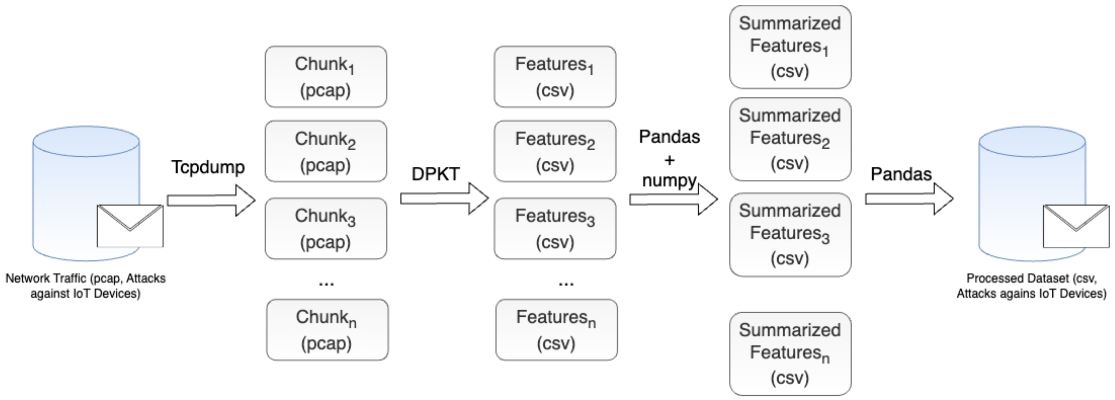

Figure 2: data processing steps

One possible improvement on original paper is to category 8 class or 34 class of attack categories with better precision and F1-score. Some ensemble techniques similar to Random Forest, e.g. XGBoost are worth trying to obtain a better performance.

Another surprising yet interesting result from original paper is that Random Forest outperformed Deep Neural Network (DNN). The paper didn't disclose the specific architecture of the DNN in use. So different architecture will be worth trying, e.g. LSTM/RNN is supposed to be able to obtain high-level information if the sequence of network packages were inter-related.

3.3 Visualization

In prepossessing phase, visualization provides an intuitive way to get a quick and overall understanding of data. For example[tab], heat map can be used to show the correlations of features while box or violin plots will be used to show the distribution of the different features and area chart will be useful to display the change of different traffic volume along the time.

After analysis, common visualization techniques, including confusion matrix and bar chart similar to the original paper, will be leveraged to illustrate the effectiveness of these machine learning models. Besides, curve diagram will be depicted to display learning rate of different machine learning techniques to show how efficient each algorithm is

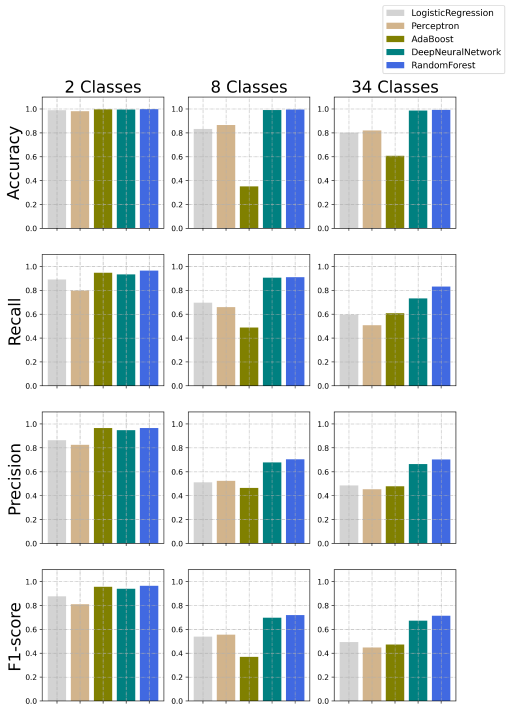

Figure 3: evaluation of machine learning models

References

[Bax14] James H Baxter. *Wireshark essentials*. Packt Publishing Ltd, 2014.

[Cis20] U Cisco. Cisco annual internet report (2018–2023) white paper. *Cisco: San Jose, CA, USA*, 10(1):1–35, 2020.

[DMD+22] Sajjad Dadkhah, Hassan Mahdikhani, Priscilla Kyei Danso, Alireza Zohourian, Kevin Anh Truong, and Ali A Ghorbani. Towards the development of a realistic multidimensional iot profiling dataset. In *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*, pages 1–11. IEEE, 2022.

[kaga] Creating a Smaller Dataset for CICIoT2023 — kaggle.com. `https://www.kaggle.com/code/madhavmalhotra/creating-a-smaller-dataset-for-ciciot2023`. [Accessed 24-09-2024].

[kagb] Feature Importance Study on the CICIoT2023 — kaggle.com. `https://www.kaggle.com/code/shreyaan10/feature-importance-study-on-the-ciciot2023`. [Accessed 24-09-2024].

[MNG+17] Mohsen Marjani, Fariza Nasaruddin, Abdullah Gani, Ahmad Karim, Ibrahim Abaker Targio Hashem, Aisha Siddiqa, and Ibrar Yaqoob. Big iot data analytics: architecture, opportunities, and open research challenges. *ieee access*, 5:5247–5261, 2017.

[NDF+23] Euclides Carlos Pinto Neto, Sajjad Dadkhah, Raphael Ferreira, Alireza Zohourian, Rongxing Lu, and Ali A Ghorbani. CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment. *Sensors (Basel)*, 23(13), June 2023.

[NDG22] Euclides Carlos Pinto Neto, Sajjad Dadkhah, and Ali A Ghorbani. Collaborative ddos detection in distributed multi-tenant iot using federated learning. In *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*, pages 1–10. IEEE, 2022.

[SK19] Surbhi Sharma and Baijnath Kaushik. A survey on internet of vehicles: Applications, security issues & solutions. *Vehicular Communications*, 20:100182, 2019.

[SKS+20] Kinza Shafique, Bilal A Khawaja, Farah Sabir, Sameer Qazi, and Muhammad Mustaqim. Internet of things (iot) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5g-iot scenarios. *Ieee Access*, 8:23022–23040, 2020.

[tab] Visualize your Data — tableau.com. `https://www.tableau.com/trial/visualize-your-data`. [Accessed 25-09-2024].

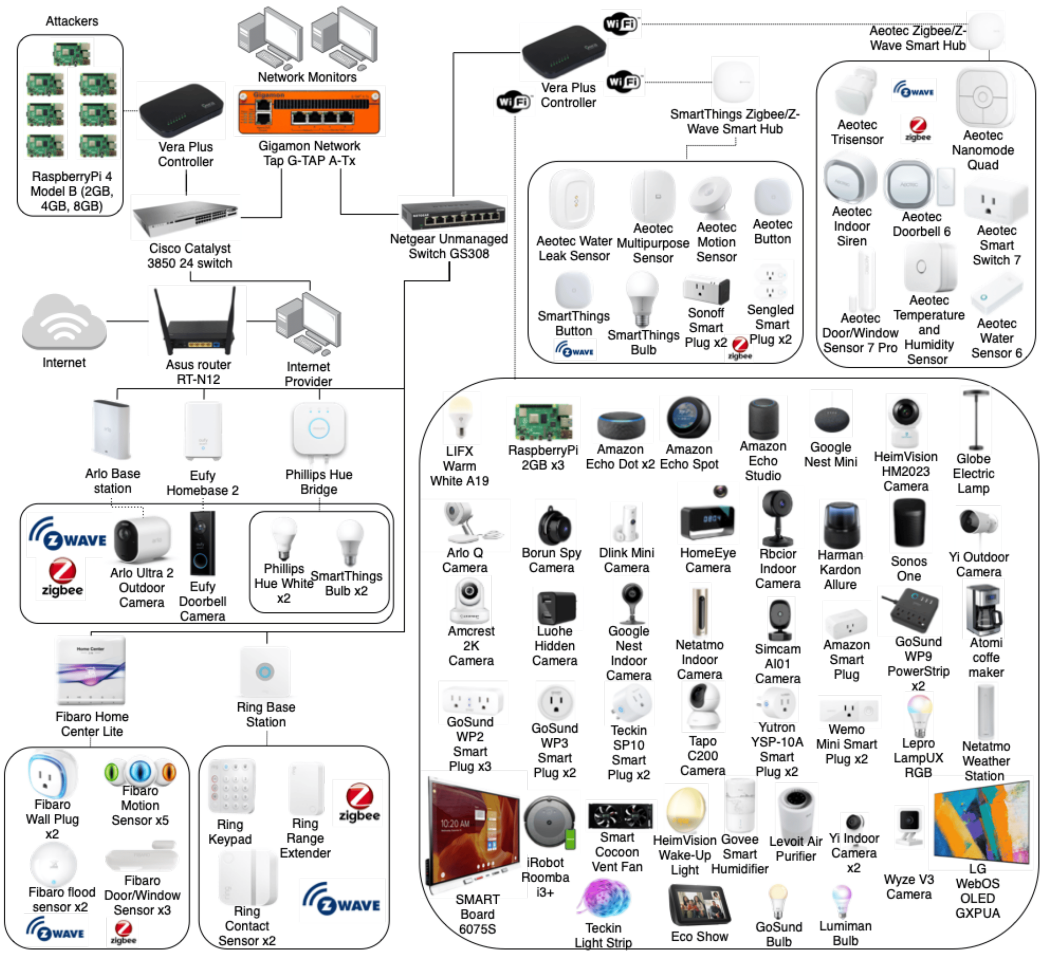

Figure 4: Topology of CICIot2023

Category	Subcategory	Rows	Toos
DDos	ACK Fragmentation	285,104	hping3
DDos	UDP Flood	5,412,287	udp-flood
DDos	SlowLoris	23,426	slowloris
DDos	ICMP Flood	7,200,504	hping3
DDos	RSTFIN Flood	4,045,285	hping3
DDos	PSHACK Flood	4,094,755	hping3
DDoS	HTTP Flood	28,790	golang-httpflood
DDos	UDP Fragmentation	286,925	udp-flood
DDos	ICMP Fragmentation	452,489	hping3
DDos	TCP Flood	4,497,667	hping3
DDos	SYN Flood	4,059,190	hping3
DDos	SynonymousIP Flood	3,598,138	hping3
Dos	TCP Flood	2,671,445	hping3
Dos	HTTP Flood	71,864	golang-httpflood
DoS	SYN Flood	2,028,834	hping3
Dos	UDP Flood	3,318,595	hping3 and udp-flood
Recon	Ping Sweep	2262	nmap and fping
Recon	OS Scan	98,259	nmap
Recon	Vulnerability Scan	37,382	nmap and vulscan
Recon	Port Scan	82,284	nmap
Recon	Host Discovery	134,378	nmap
Web-Based	Sql Injection	5245	DVWA
Web-Based	Command Injection	5409	DVWA
Web-Based	Backdoor Malware	3218	DVWA and Remot3d
Web-Based	Uploading Attack	1252	DVWA
Web-Based	XSS	3846	DVWA
Web-Based	Browser Hijacking	5859	Beef
Brute Force	Dictionary Brute Force	13,064	nmap and hydra
Spoofing	Arp Spoofing	307,593	ettercap
Spoofing	DNS Spoofing	178,911	ettercap
Mirai	GREIP Flood	751,682	Adapted Mirai Source Code
Mirai	Greeth Flood	991,866	Adapted Mirai Source Code
Mirai	UDPPlain	890,576	Adapted Mirai Source Code

Table 1: Attack category and tools

ID	Feature	Description
1	ts	Timestamp
2	flow duration	Duration of the packet's flow
3	Header Length	Header Length
4	Protocol Type	IP, UDP, TCP, IGMP, ICMP, Unknown (Integers)
5	Duration	Time-to-Live (ttl)
6	Rate	Rate of packet transmission in a flow
7	Srate	Rate of outbound packets transmission in a flow
8	Drate,	Rate of inbound packets transmission in a flow
9	fin flag number	Fin flag value
10	syn flag number	Syn flag value
11	rst flag number	Rst flag value
12	psh flag numbe	Psh flag value
13	ack flag number	Ack flag value
14	ece flag numbe	Ece flag value
15	cwr flag number	Cwr flag value
16	ack count	Number of packets with ack flag set in the same flow
17	syn count	Number of packets with syn flag set in the same flow
18	fin count	Number of packets with fin flag set in the same flow
19	urg coun	Number of packets with urg flag set in the same flow
20	rst count	Number of packets with rst flag set in the same flow
21	HTTP	Indicates if the application layer protocol is HTTP
22	HTTPS	Indicates if the application layer protocol is HTTPS
23	DNS	Indicates if the application layer protocol is DNS
24	Telnet	Indicates if the application layer protocol is Telnet
25	SMTP	Indicates if the application layer protocol is SMTP
26	SSH	Indicates if the application layer protocol is SSH
27	IRC	Indicates if the application layer protocol is IRC
28	TCP	Indicates if the transport layer protocol is TCP
29	UDP	Indicates if the transport layer protocol is UDP
30	DHCP	Indicates if the application layer protocol is DHCP
31	ARP	Indicates if the link layer protocol is ARP
32	ICMP	Indicates if the network layer protocol is ICMP
33	IPv	Indicates if the network layer protocol is IP
34	LLC	Indicates if the link layer protocol is LLC
35	Tot sum	Summation of packets lengths in flow
36	Min	Minimum packet length in the flow
37	Max	Maximumpacket length in the flow
38	AVG	Average packet length in the flow
39	Std	Standard deviation of packet length in the flow
40	Tot size	Packet's length
41	IAT	The time difference with the previous packet
42	Number	The number of packets in the flow
43	Magnitude	(Average of the lengths of incoming packets in the flow + average of the lengths of outgo
44	Radius	(Variance of the lengths of incoming packets in the flow + variance of the lengths of outg
45	Covariance	Covariance of the lengths of incoming and outgoing packets
46	Variance	Variance of the lengths of incoming packets in the flow/ variance of the lengths of outgoi
47	Weight	Number of incoming packets $\times$ Number of outgoing packets

Table 2: Feature Descriptions