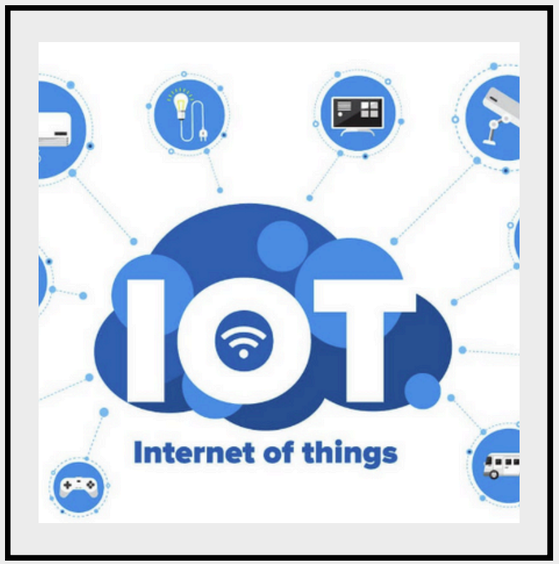
SEATWORK 10.1 CASE STUDY: IMPROVING RT-IOT2022 ANALYSIS

Presented by Sanchez and Silang

Technological Institute of the Philippines

INTRODUTION OF THE DATA SET



The RT-IoT2022 dataset contains normal and attack traffic from IoT devices like ThingSpeak-LED, Wipro-Bulb, and MQTT-Temp. It includes 9 types of attacks (like SSH brute-force and DDoS) and 3 normal scenarios.

Data was collected using Zeek, Flowmeter, and Wireshark from a setup with 50 attacker machines and 420 victim machines. It also includes system logs and 80 traffic features, making it useful for IoT security research.

EXTRACT – TRANSFORM – LOAD

Extract

```
import pandas as pd

df = pd.read_csv('/RT_IOT2022.csv')
```

Transform

Created a copy of data and renaming of data

```
[31] data = df[['Attack_type',
                'proto',
                'service',
                'flow_SYN_flag_count',
                'flow_RST_flag_count',
                'fwd_PSH_flag_count',
               ]]

     data.rename(columns={
                'proto': 'Protocol',
                'service': 'Service',
                'flow_SYN_flag_count': 'SYN_flag_count',
                'flow_RST_flag_count': 'RST_flag_count',
                'fwd_PSH_flag_count': 'PSH_flag_count'
                 }, inplace=True)
```

Only display top 3 common attack types in rows

```
[45] common = data[(df['Attack_type'].isin(['DOS_SYN_Hping','Thing_Speak','ARP_poisioning']))]
     common
```

	Attack_type	Protocol	Service	SYN_flag_count	RST_flag_count	PSH_flag_count
4146	Thing_Speak	tcp	http	2	0	2
4147	Thing_Speak	udp	dns	0	0	0
4148	Thing_Speak	tcp	http	2	0	2
4149	Thing_Speak	udp	dns	0	0	0
4150	Thing_Speak	tcp	http	2	0	2
...	...	...	...	...	...	...
115445	DOS_SYN_Hping	tcp	-	1	0	0
115446	DOS_SYN_Hping	tcp	-	1	0	0
115447	DOS_SYN_Hping	tcp	-	1	0	0
115448	DOS_SYN_Hping	tcp	-	1	0	0
115449	DOS_SYN_Hping	tcp	-	1	0	0

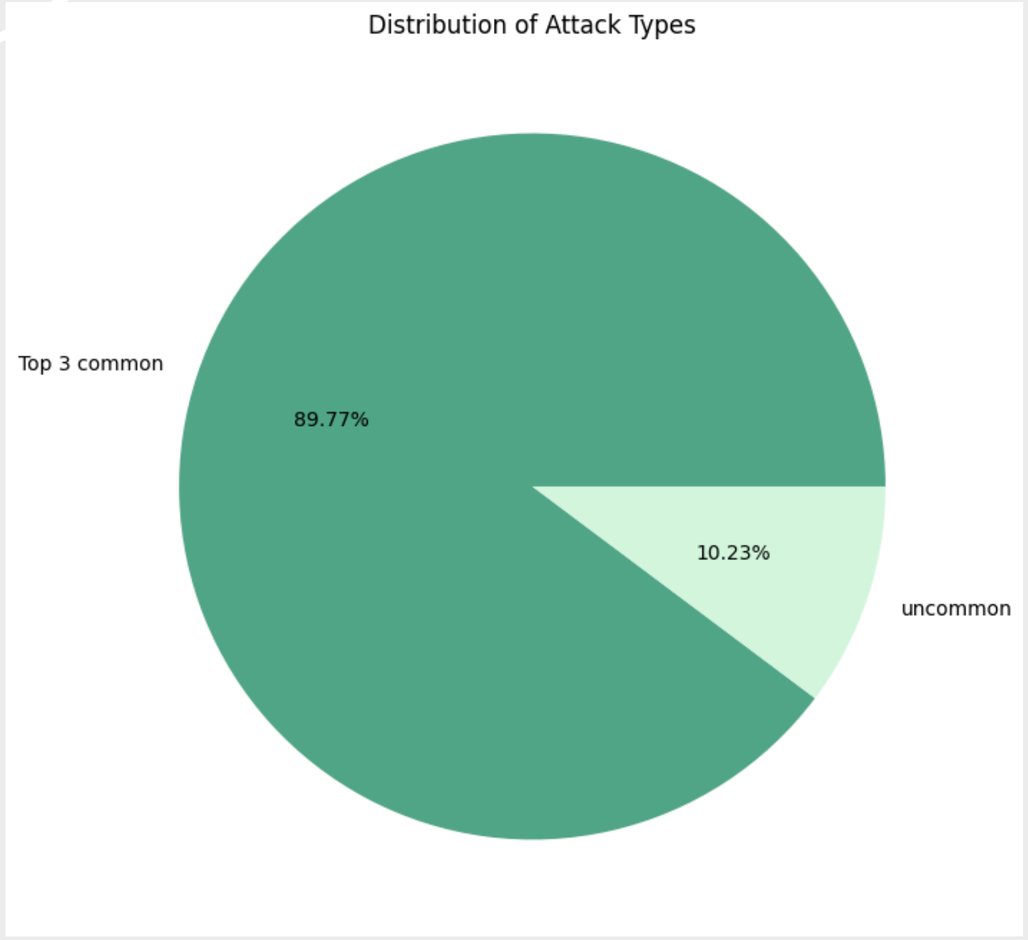
110517 rows × 6 columns

Only display top 3 common attack types in rows

```
ps_counts = common.groupby(
    ['Attack_type', 'Protocol', 'Service']
    ).size().reset_index(name='count')
ps_counts
```

	Attack_type	Protocol	Service	count
0	ARP_poisioning	icmp	-	8
1	ARP_poisioning	tcp	-	214
2	ARP_poisioning	tcp	dns	125
3	ARP_poisioning	tcp	http	129
4	ARP_poisioning	tcp	ssl	1459
5	ARP_poisioning	udp	-	324
6	ARP_poisioning	udp	dhcp	26
7	ARP_poisioning	udp	dns	5458
8	ARP_poisioning	udp	ntp	7
9	DOS_SYN_Hping	tcp	-	94659
10	Thing_Speak	icmp	-	45

INSIGHTS

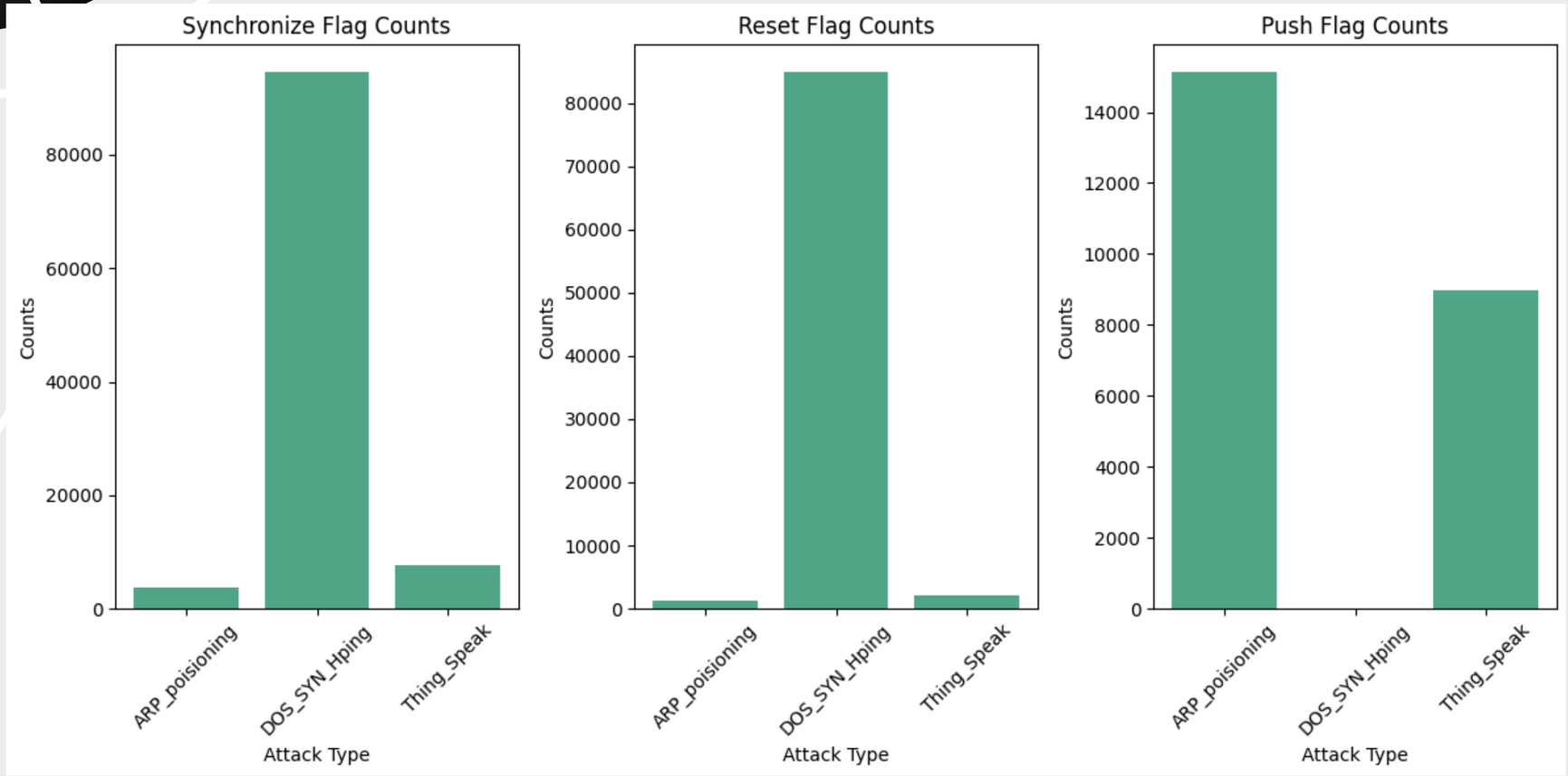


ANALYZSIS

This shows top 3 common attack types that occur in the data set which also includes the others.

The top 3 common attacks amount to 89.77% while the uncommon amounts to 10.23%

INSIGHTS



ANALYSIS

DOS SYN Hping has a high count for Synchronize and Reset flag counts.

while on the other hand, the ARP poisoning and Thing Speak does it all but more on PUSH flag counts, demanding a data transfer immediately

OVERALL ANALYSIS

To sum it up, DOS has the highest Synchronize and Reset flags since its job is only to disrupt services while no need to push since it does not need to manipulate data and to avoid wasting time, while ARP-poisoning and Thing-Speak only has high counts of Push flag since the goal of it is to manipulate data, hence it’s pushing to transfer data immediately.

RECCOMENDATIONS

USE A FIREWALL

Set up a firewall to block suspicious traffic and limit the number of incoming requests to prevent synchronized flood attacks.

UPDATE IOT DEVICES REGULARLY

Make sure your IoT devices, like ThingSpeak, are always updated with the latest security patches to avoid vulnerabilities.

ENABLE ARP SPOOFING PROTECTION

Use tools or settings that can detect or prevent ARP poisoning, such as enabling ARP monitoring on your network.