

Internet of Things: Spy Your Mate

Giovanni Baccichet

👤 10851745

Politecnico di Milano — June 29, 2022

1 Introduction

In this project, you are requested to analyze the traffic generated by a webcam call and, from such traffic, identify whether a person or only the background is recorded in the video. You have to approach this problem from a *Machine Learning* (ML) perspective.

It is important to point out the hardware and software (specific versions) used to fulfill the requirements, in order to replicate the achieved results. For this project I used:

- Apple MacMini8,1 w/ Intel Core i5 and 32 GB RAM, running macOS 12.4;
- Wireshark 3.6.6;
- Jupyter Notebook w/ Python 3.9.12, using Anaconda-Navigator;
- NodeRED 2.2.2 running on Docker 4.9.1;
- Zoom.us 5.10.7.

Everything disclosed in this report (except for the network dumps, due to privacy reasons) can be found in this repository: github.com/GiovanniBaccichet/IoT-human-detection.

2 Network Setup

Figure 1 represents a simplified version of the network topology used is displayed. Briefly: two computers connected to the same network, the red one using a 5 GHz WiFi connection, the other one using a Gigabit Ethernet connection. In the following section the *Internet* portion of the diagram will be addressed, along with the network traffic generation process followed for the experiment.

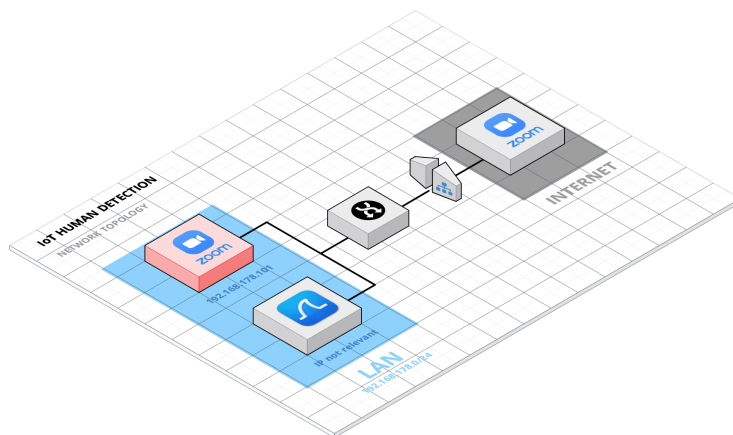


Figure 1: Network Topology: a simplified version of the LAN, target in red.

2.1 Traffic Generation

Traffic generation was performed using the PC dumping the network traffic as a participant of a Zoom call, in which the target PC was the administrator and had the webcam turned on. The IP address of the eavesdropper was 192.168.178.69. Since Zoom is not a *Peer-To-Peer* application, an IP was needed in order to clean out the traffic from other unwanted destinations (sources). For this purpose an application firewall (Little Snitch 5.4.1) was used: it allowed to visualize a list of addresses used by Zoom to relay the traffic, see figure 2. This allowed to get an idea of the range of IP addresses that the service provider used to perform the operation.

The time period in which someone was framed by the webcam was about 20 minutes, the same for the background only, for a total of 40 minutes.

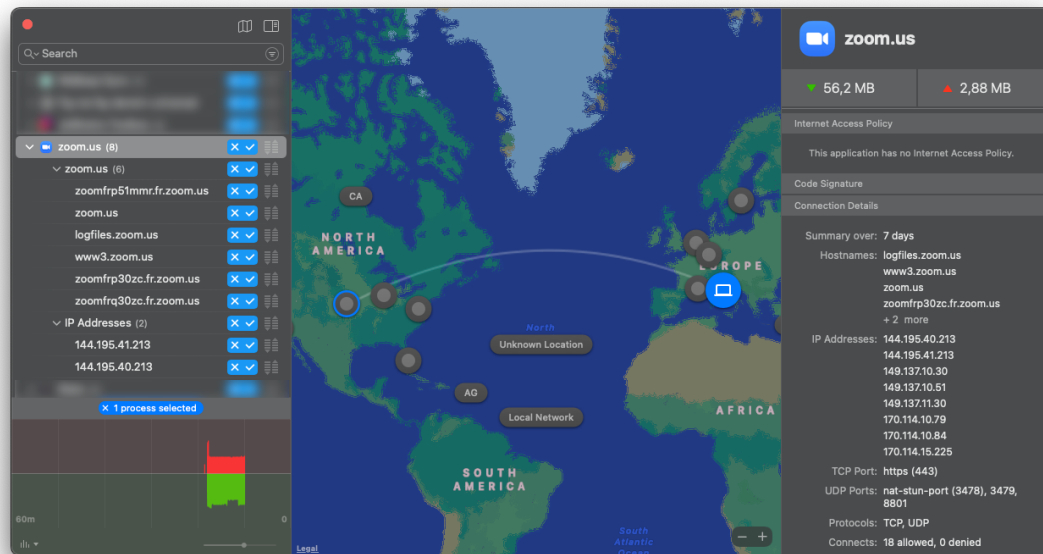


Figure 2: Little Snitch instance, visualizing Zoom.US traffic (*IP addresses don't correspond to the Jupiter Notebook's ones because this screenshot was taken in a second moment*)

2.2 Traffic Acquisition

Traffic acquisition was performed using Wireshark to acquire a *Packet CAPture* (PCAP) file, from which some interesting information was extracted and exported in *Comma Separated Value* (CSV) format, using tshark. The latter is presented in a terminal fashion, and the command used was:

Command Line

```
$ tshark -r "dataset-zoom-us-20+20_min.pcapng" -T fields -e  
frame.time -e ip.src -e ip.dst -e ip.proto -e frame.len -E header=y  
-E separator=, > "zoom_dataset.csv" -Y 'ip.addr == 149.137.12.48'
```

Said command allowed to export a CSV with the following characteristics (columns):

- Timestamp;
- Source IP address;
- Destination IP address;
- Protocol;

- Frame Length.

From an initial network dump of 8.43 GB, this allowed to narrow down to only 10.8 MB.

3 Node-RED Setup

In order to acquire a *Ground Truth*, and represent it, a *Node-RED* dashboard was used. In the figures below it is possible to see the *flow* used (Figure 3), and the dashboard itself (Figure 4).

Node-RED was running in a Docker container: so the CSV generated and (at the end) parsed were inputted using a remote shell connection.

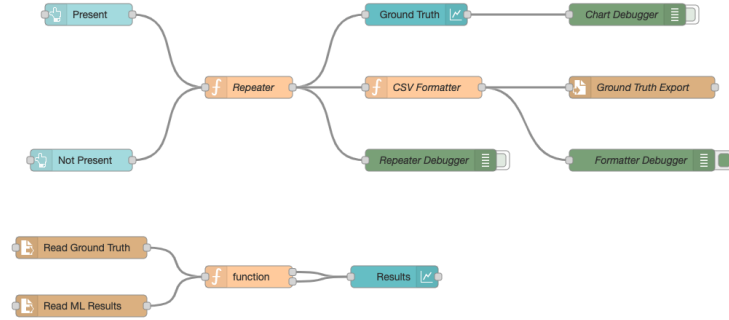


Figure 3: Node-RED Flow

The ground truth consisted, as mentioned above, in a CSV reporting the timestamp and the value 1 if someone was framed, otherwise 0.

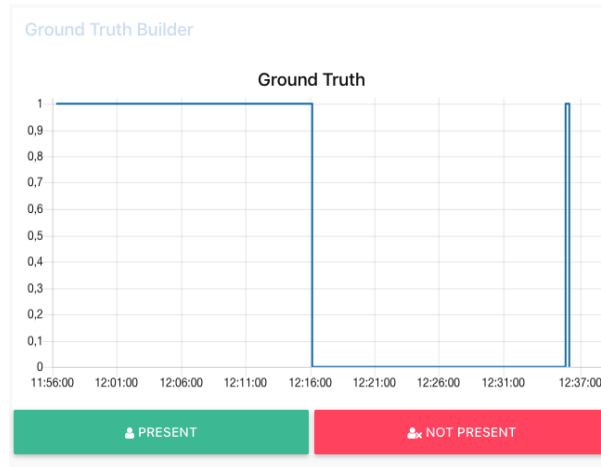


Figure 4: Node-RED Ground Truth Builder

4 Features and Data Visualization

Everything disclosed in the previous section was used as an input for the Jupyter Notebook (which can be found in the repository mentioned in the introduction). The most technical details won't be addressed in this report, since every step is commented in the code itself.

On the other hand, in this section some remarks about the data acquired (before the model training) will be given.

The approach used to select the features was incremental: starting with few features, visualizing them graphically and trying to train the model. The features used were: PacketNumber (*number of packets within*

a time interval of 450 ms), PacketIntervalAvg (average amount of time between packets within 450 ms - figure 6), PacketSizeAvg (average packet size - figure 8), PacketSizeStd, PacketSizeMed, PacketSizeMin, PacketSizeMax, InboundCount (number of packets received by the eavesdropper - figure 9), OutboundCount (number of packets sent by the eavesdropper).

The correlation matrix between said features can be seen in figure 5.

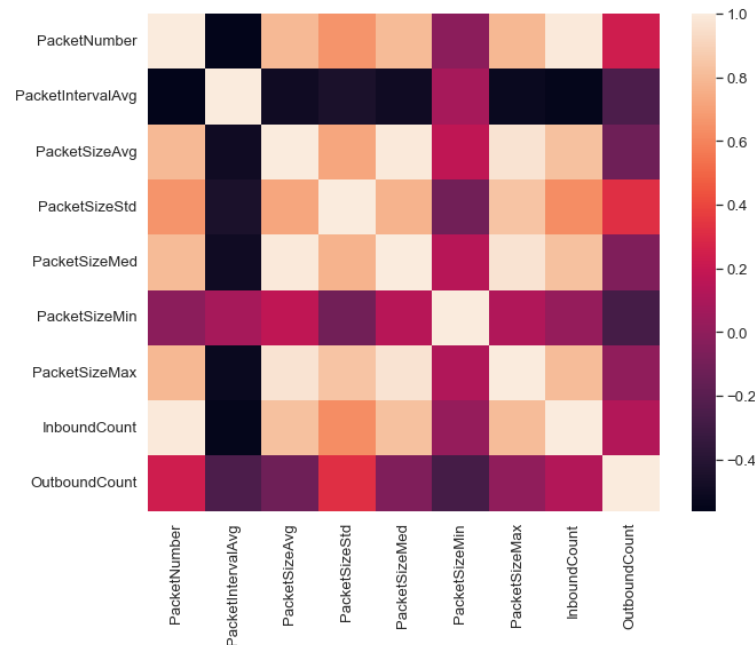


Figure 5: Selected features correlation matrix

Plotting some of those features, with respect to the ground truth, it is evident when someone is framed and when not, despite the fact that some features are correlated (not completely) with some others.

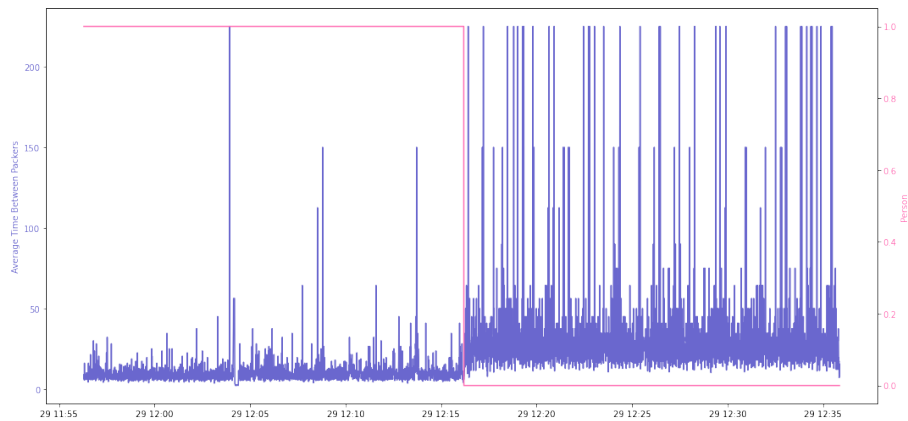


Figure 6: Average Time Between Packets

In the Jupyter Notebook are attached some other diagrams aimed at visualizing the data frame we are dealing with and also the selected features.

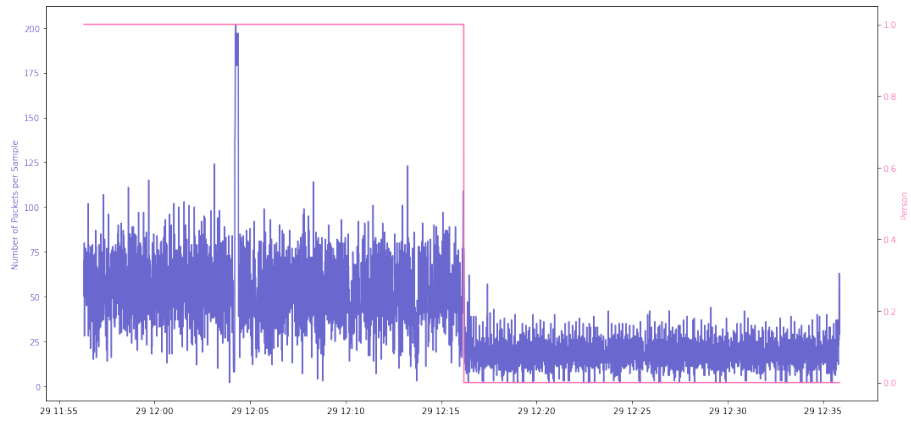


Figure 7: Packets per Sample of 450 ms

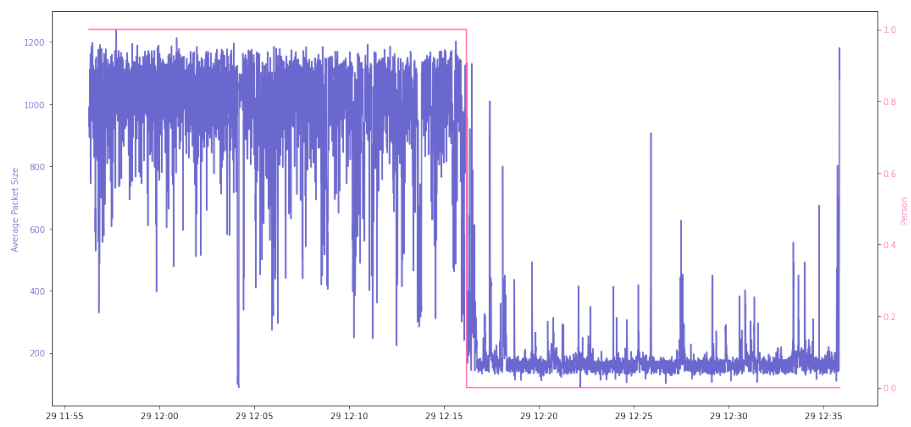


Figure 8: Average Packet Size within a Sample (450 ms)

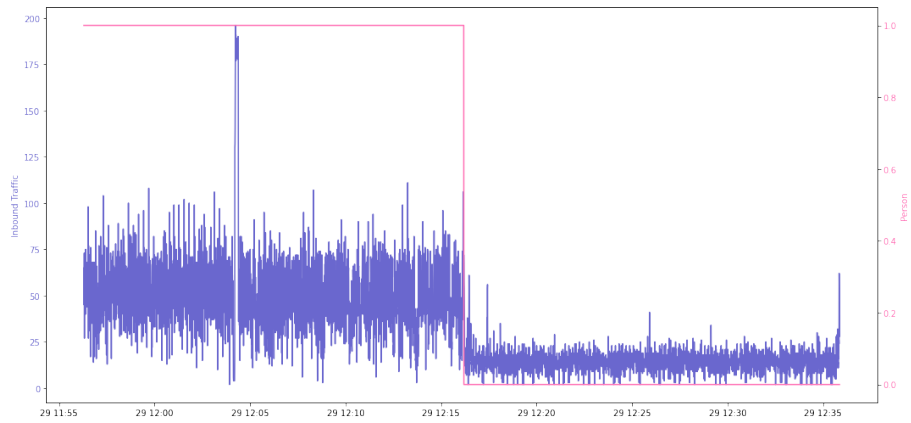


Figure 9: Inbound Traffic

5 Results

As anticipated by the data visualization, the results were very accurate. The ML algorithms tested were:

- Random Forest;
- K-Nearest Neighbor;
- Support Vector Machine;
- Logistic Regression.

Every algorithm tested presented very similar results, with the lowest accuracy reported of around 97%, and the highest one of 99%. Everything is reported in the Jupyter Notebook, however in this report will be included some more information about the best and the worst performing ones.

5.1 Random Forest

5.2 Support Vector Machine