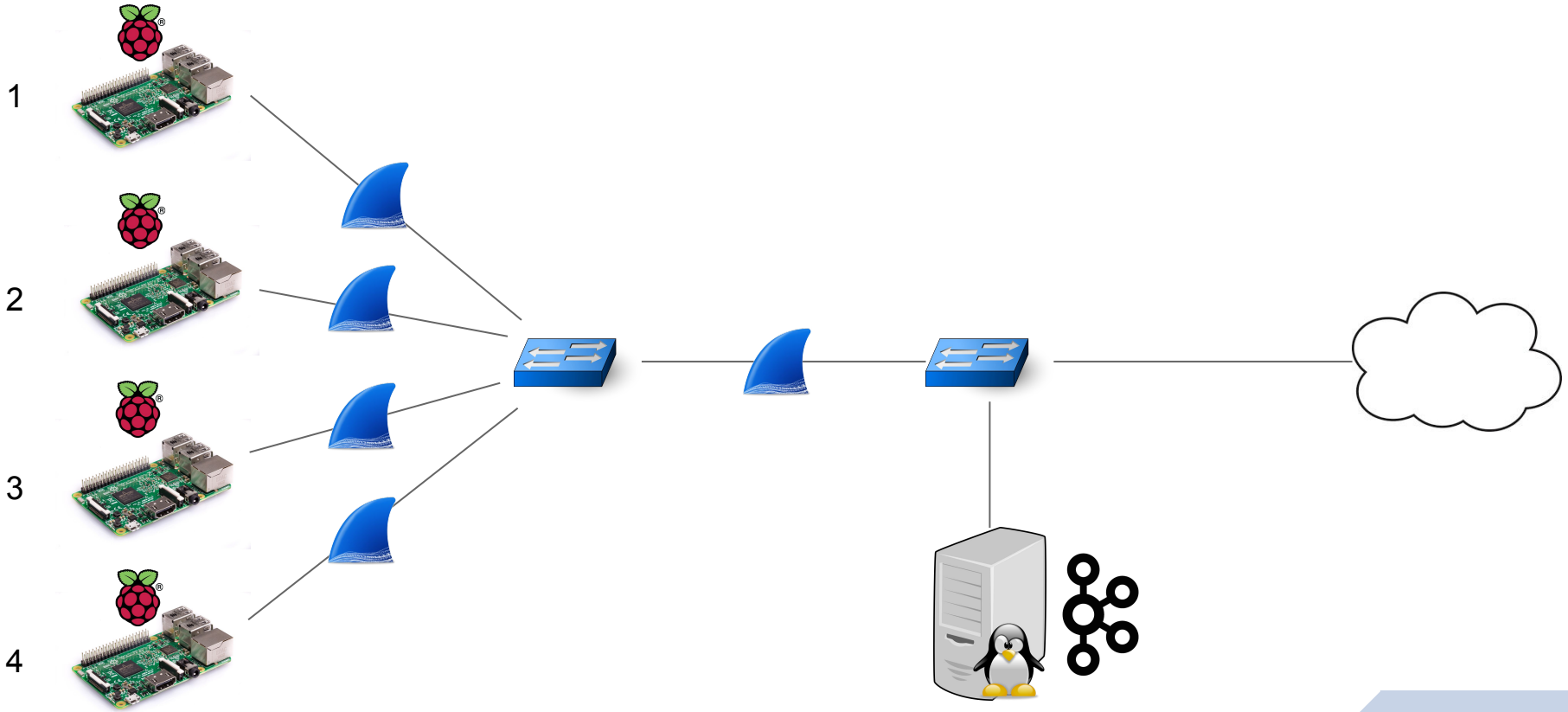
IoT network monitoring in a vulnerable environment

Técnicas de Perceção de Redes

Diogo Ferreira *76504*
Luís Leira *76514*

IoT network architecture



Regular Traffic - Sensors to Server

- Sensor 1 sends data to server every 30 seconds
- Sensor 2 sends data to host every minute
- Sensor 3 sends data to host every 3 minutes
- Sensor 4 sends data to host at a random interval from 30 to 180 seconds

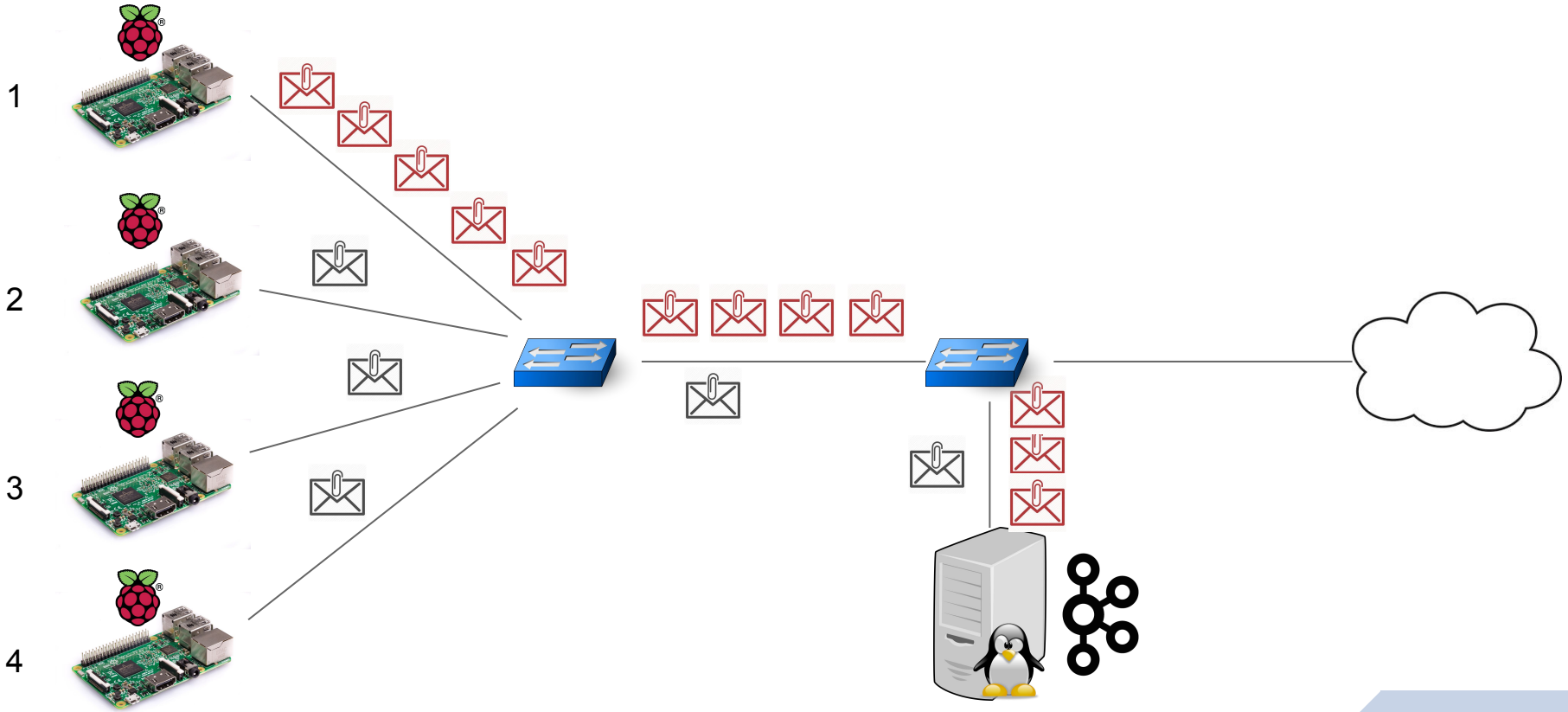
Regular Traffic - Commands

- Sensor 1, sensor 2, sensor 3, sensor 4 and server send commands between each other at a random interval from 5 to 15 minutes

Scenario 1 - DoS Attack

- Sensor 1 tries to disrupt the network, sending data every second

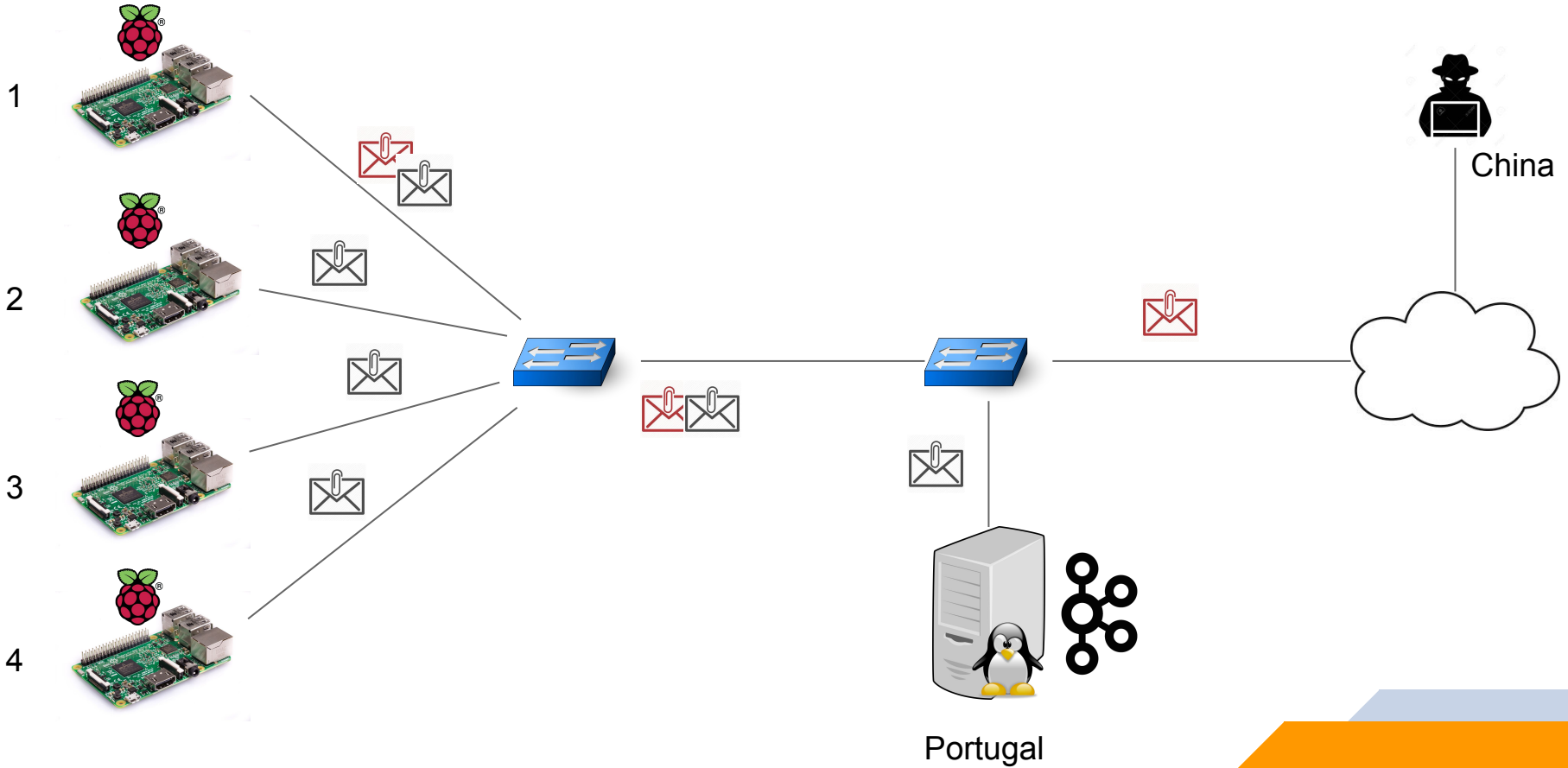
Scenario 1



Scenario 2 - Sensor sends data to attacker

- Sensor 1 sends data to server and also to IP geographically away from the server

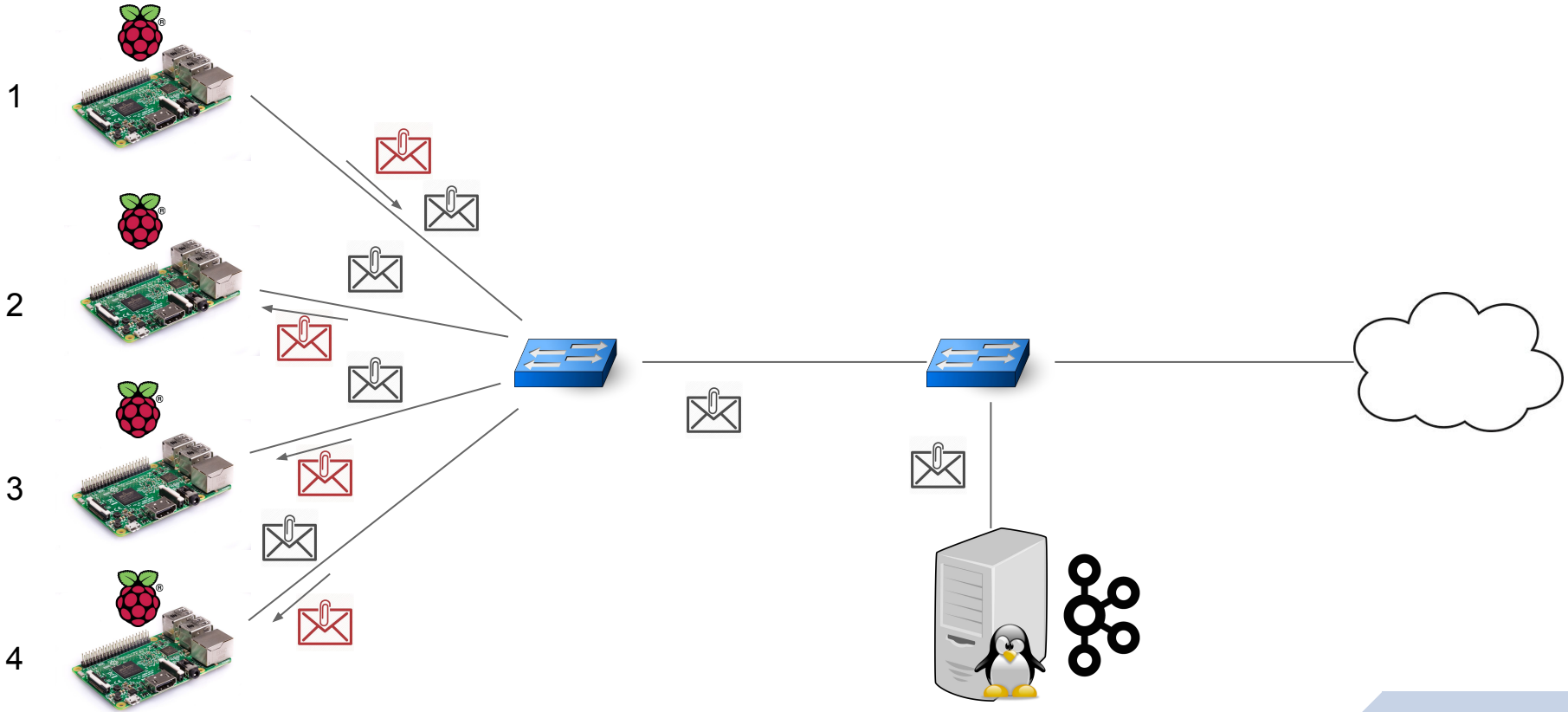
Scenario 2



Scenario 3 - Sensor collects data from other sensors

- Sensor 1 polls all other sensors for data every 30 seconds

Scenario 3




After the data
gathering...

Some metrics extracted from the captures

- IPv4 packet length (between sensors, between sensor and server, between sensor and external IP)
- Geographical distance from the server location to the external IP location
- Number of DNS, ICMP, ARP, TCP, UDP and other packets
- Number of packets with each TCP flag (SYN, ACK, FIN, URG, PUSH, RST)
- Number of external IP’s contacted
- ...

Training the models

- 1 second sampling interval
- Observation window of 6 minutes (double the time of sensor that sends data at a lower frequency, 3 minutes)
- Sliding window of 60 seconds
- K-fold cross-validation test *(K = 5)*
- 5 machine-learning algorithms: *SVC*, *Linear SVC*, *Poly SVC*, *RBF SVC* and *neural networks*

Analysis on the stub network

Best results with the *neural network* algorithm

Confusion Matrix

	Regular Scenario	Scenario 1	Scenario 2	Scenario 3
Regular Scenario	894	0	0	0
Scenario 1	0	953	0	0
Scenario 2	0	0	1129	0
Scenario 3	0	0	0	1146

Analysis on the attacking sensor network

Best results with the *neural network*, *SVC* or *linear SVC* algorithms

Confusion Matrix

	Regular Scenario	**Scenario 1**	**Scenario 2**	**Scenario 3**
Regular Scenario	894	0	0	0
Scenario 1	0	953	0	0
Scenario 2	0	0	1129	0
Scenario 3	0	0	0	1146

Analysis on the attacked sensor network

Best results with the *neural network* algorithm

Confusion Matrix

	Regular Scenario	**Scenario 3**
Regular Scenario	874	19
Scenario 3	16	1129

Average: 0.983
Standard Deviation: 0.001

Future work

- Develop a version with only layer 2 metrics (for monitoring sensors using a layer 2 protocol like LoRa instead of WiFi)
- Train with new data, using traffic more similar between regular traffic and anomalies:
  - Reduce the burst time in scenario 1
  - Send data to closer IP in scenario 2
  - Increase the polling time in scenario 3

IoT network monitorization in an vulnerable environment

Técnicas de Perceção de Redes

Diogo Ferreira *76504*
Luís Leira *76514*