Institut Mines-Télécom

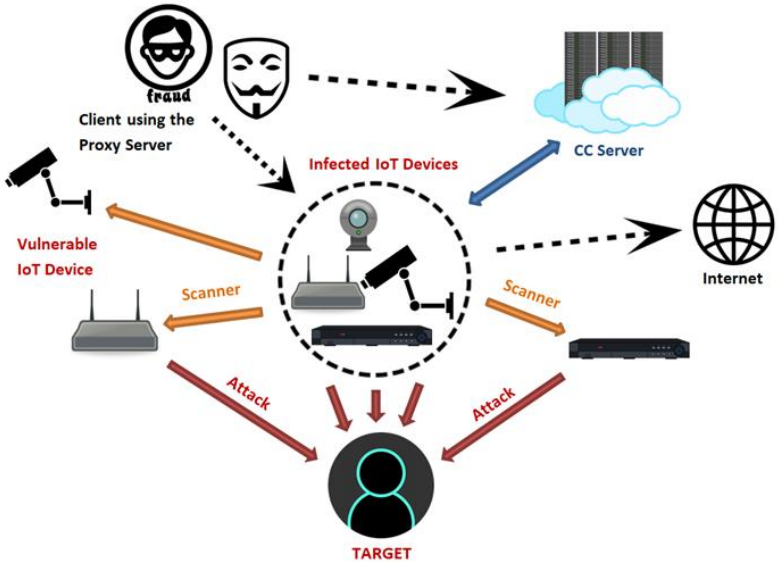
Machine Learning for IoT Network Monitoring

Mustafizur SHAHID

SOMMAIRE

Institut Mines-Télécom

- 75 billions connected devices by 2030
- Diversity of IoT devices: security camera, smart bulb, smart plug, smart thermostat, smart car, …
- Security related issues: Mirai botnet (600,000 infected devices at its peak)
- 600% increase in IoT attacks from 2016 to 2017 (ISTR Symantec 2018)



IoT Botnet
Source: www.fortinet.com

- IoT devices perform very specific tasks making their networking behavior very stable and predictable.

- Data analysis methods well suited to detect the type of IoT devices connected to the network or to perform intrusion detection.

- Proposed approach:
  - step 1: Determine the type of IoT device connected to the network.
  - step 2: Use the legitimate behavior profile that corresponds to the detected IoT device to detect anomalous network activities.

- Legitimate behavior profile of different IoT devices are learned beforehand.

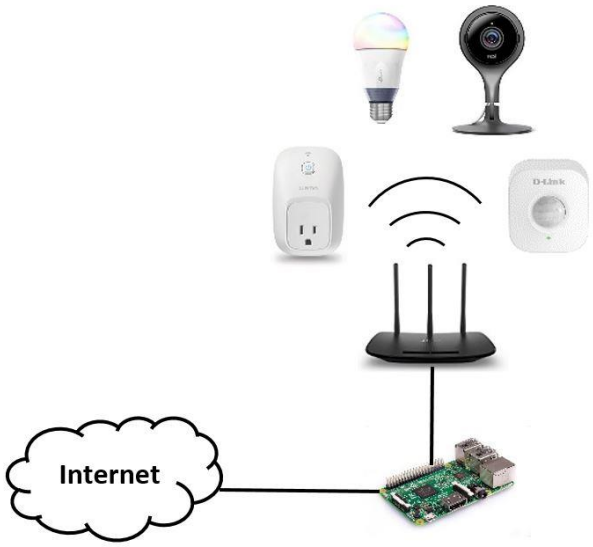
- Network traffic described by bidirectional TCP flows identified by Src IP, Dest IP, Src Port, Dest Port.

- A timeout is used to split long TCP connection into multiple bidirectional flows.

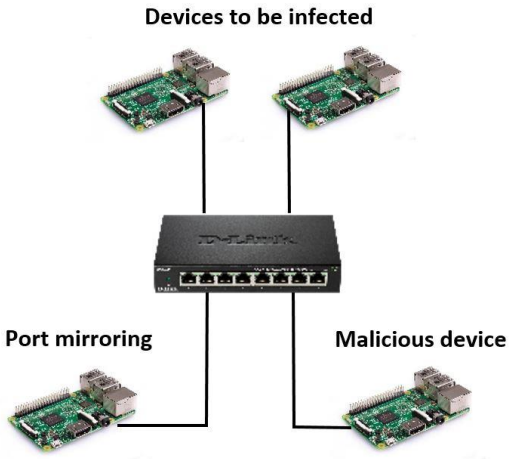
- Bidirectional flows are described by the following features:
  - Size of the first N packets sent
  - Size of the first N packets received
  - The N - 1 packet inter-arrival times between the first N packets sent
  - The N - 1 packet inter-arrival times between the first N packets received

- Experimental smart home network composed of Nest security camera, D-Link motion sensor, TP-Link smart bulb and smart plug.
- Traffic collected for 7 days
- N = 10, timeout = 600 seconds

	train	test
Motion sensor	867	207
Security camera	839	216
Smart Bulb	821	219
Smart Plug	695	163
Total	**3222**	**805**

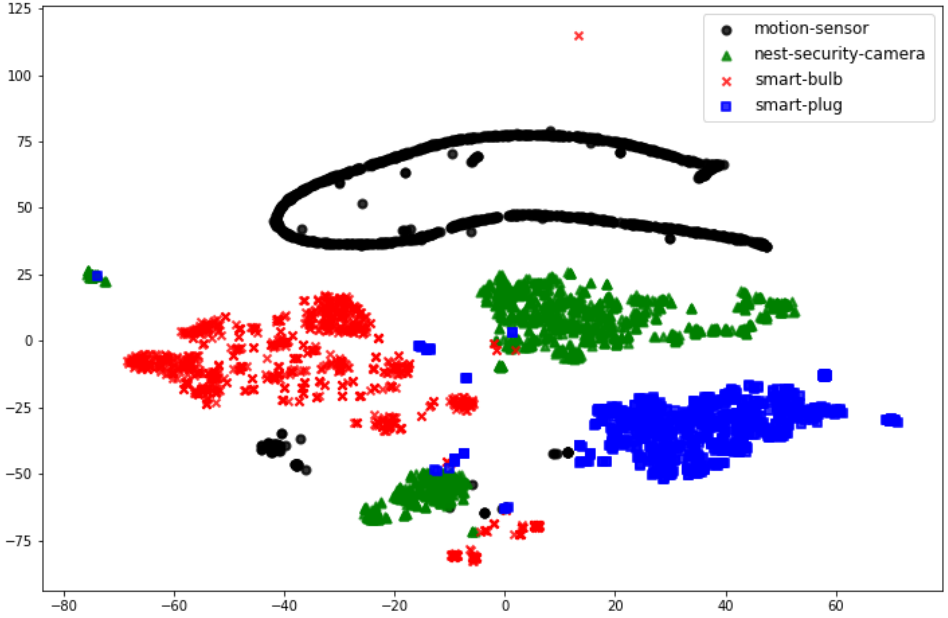


- Malicious network traffic generation in a contained environment



- Use malicious network data collected by IoTPOT (an IoT honeypot from the university of Yokohama, Japan)

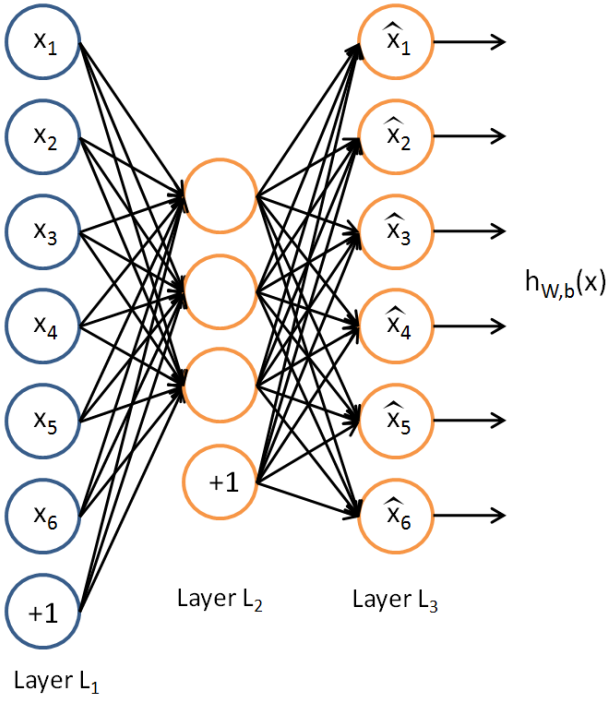
- t-Distributed Stochastic Neighbor Embedding (t-SNE)
- Non-linear dimensionality reduction technique
- The selected set of features are discriminative enough to distinguish between the different IoT devices.



- IoT Device Recognition through network traffic classification
- Six different classification algorithms are tested: Random Forest, Decision Tree, SVM, k-Nearest Neighbors, Artificial Neural Network and Gaussian Naïve Bayes.

	accuracy	micro-av. precision	micro-av. recall	micro-av. F1 score
RF	.999	.999	.999	.999
DT	.995	.995	.995	.995
SVM	.993	.993	.993	.993
KNN	.989	.989	.989	.989
ANN	.986	.986	.986	.986
GNB	.919	.919	.919	.919

- Autoencoders are unsupervised artificial neural networks that can learn an efficient representation of the input data.
- Autoencoders learn to copy their inputs to their outputs under some constraints. For example, limiting the size of the internal representation will force the autoencoder to learn efficient representation of the data.
- An autoencoder is very bad in reconstructing outliers. Hence, the reconstruction error can be used to detect anomaly in IoT networks.
- For each IoT device type, a different autoencoder can be trained. The autoencoder will learn the expected behavior of the device. If the reconstruction error is too high that indicates a possible attack.



- Results for the motion sensor only
- Sparse autoencoder setup: 500 neurons in the hidden unit, learning rate of 0.01, sparsity target of 0.1, sparsity weight of 0.2.
- Dataset composition:

	Legitimate data	Malicicous data (IoTPOT)
Training set	667	0
Validation set	200	200
Test set	207	200

- The threshold is tuned by maximizing the f1-score on the validation set. The smallest threshold that maximizes the f1-score is selected (false negative is more harmful than false positive).

►Performance achieved:

100% of the attacks are detected with a false positive rate of 1%.

F1-score: 0.995
Accuracy: 0.995
Precision: 0.990
Recall: 1.
False positive rate: 0.0097
AUC: 0.995

- The purpose of the work is to propose a method to recognize IoT devices by analyzing network traffic data, and then to perform network intrusion detection.
- Features used were the size of the first N packets sent and received, along with the corresponding inter-arrival times.
- Small experimental smart home network was built to generate network traffic data.
- Promising results were achieved for IoT device recognition with an overall accuracy as high as 99.9% for the Random Forest Classifier.
- Sparse autoencoders are used to perform anomaly detection. Preliminary results for the motion sensor, show an attack detection rates of 100% with a false positive rate of 1%.