Institut Mines-Télécom

Deep Learning for Internet of Things (IoT) Network Security

Mustafizur R. SHAHID

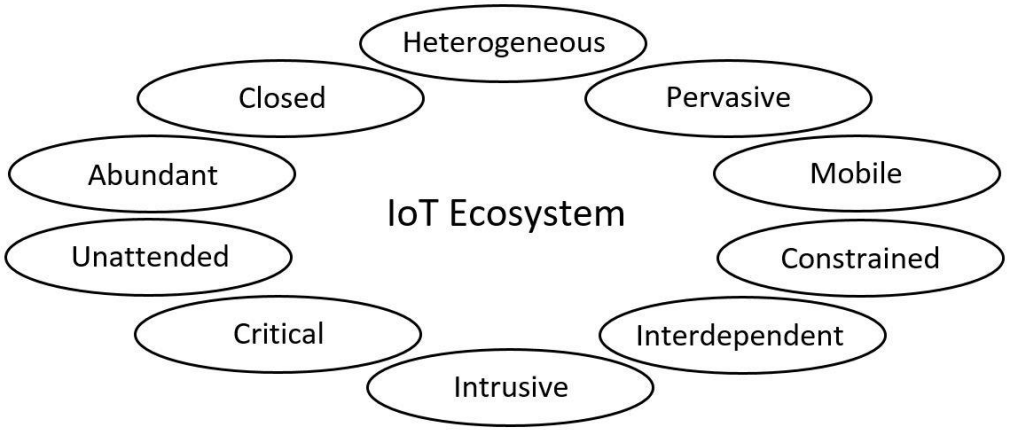
OUTLINE

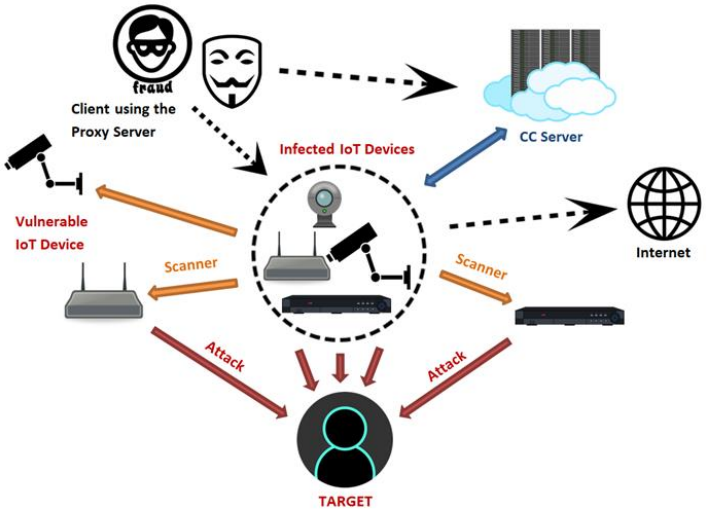
1. IoT Security Challenges
2. Thesis Objectives
3. IoT Device Type Recognition System
4. IoT Network Intrusion Detection System
5. IoT Network Traffic Generation
6. Conclusion

Institut Mines-Télécom

IoT Security Challenges

- 75 billion IoT devices connected by 2030
- Vulnerabilities in the IoT: weak credentials, backdoors, software vulnerabilities, poor software update policy, etc





- Constantly evolving IoT malware landscape: Mirai, Reaper, HideNSeek, etc
- IoT botnets are primarily used to perform large-scale DDoS attacks.

Thesis Objectives

- IoT devices perform very specific tasks. The networking behavior is therefore very stable and predictable. → well suited for machine/deep learning techniques.

- However, ML/DL algorithms require huge amount of data to be trained on.

This thesis attempts to answer the following question:

- How can deep learning help to monitor IoT networks?

  IoT device type recognition system

  IoT NIDS

- How can deep learning help to overcome the lack of IoT network traffic data?

  Synthetic IoT network traffic data generation

IoT Device Type Recognition System

Motivation:

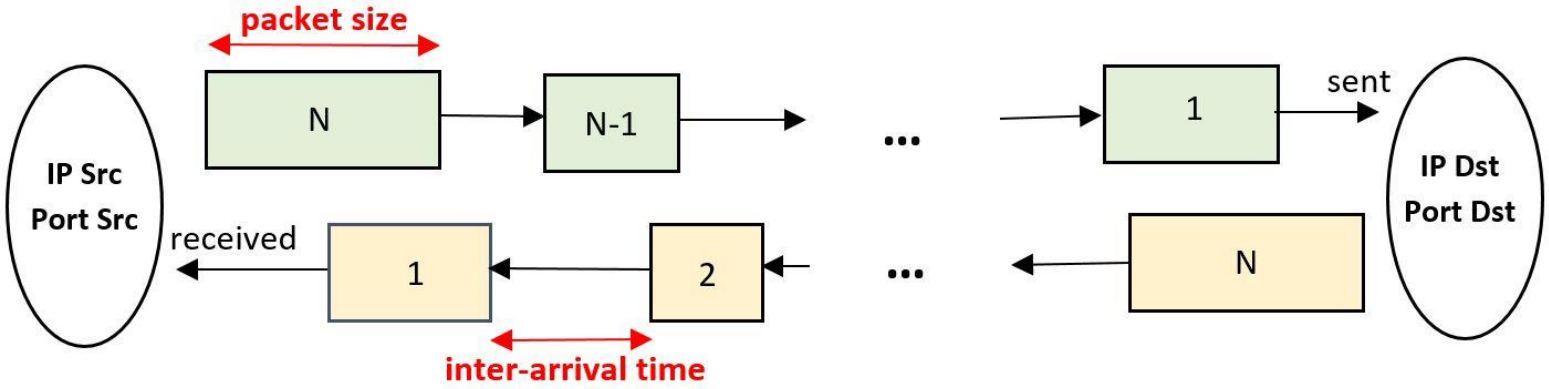
- Huge diversity of IoT devices makes it difficult to come up with a specific network signature for each device type*. ML algorithms can learn patterns from data.
- Device blacklisting/whitelisting.
- Application of device-specific filtering rules.
- Malicious use of device type recognition: passive network traffic analysis to discover vulnerable devices.

**Device type*: a specific model from a specific manufacturer.

IoT Device Type Recognition System

Network traffic data description:

- Bidirectional TCP flows identified by Src IP, Dest IP, Src Port, Dest Port
- Features used to describe a flow are the size of N packets sent and received, and the corresponding inter-arrival times:
- A timeout is used to split long TCP connection into multiple bidirectional flows.

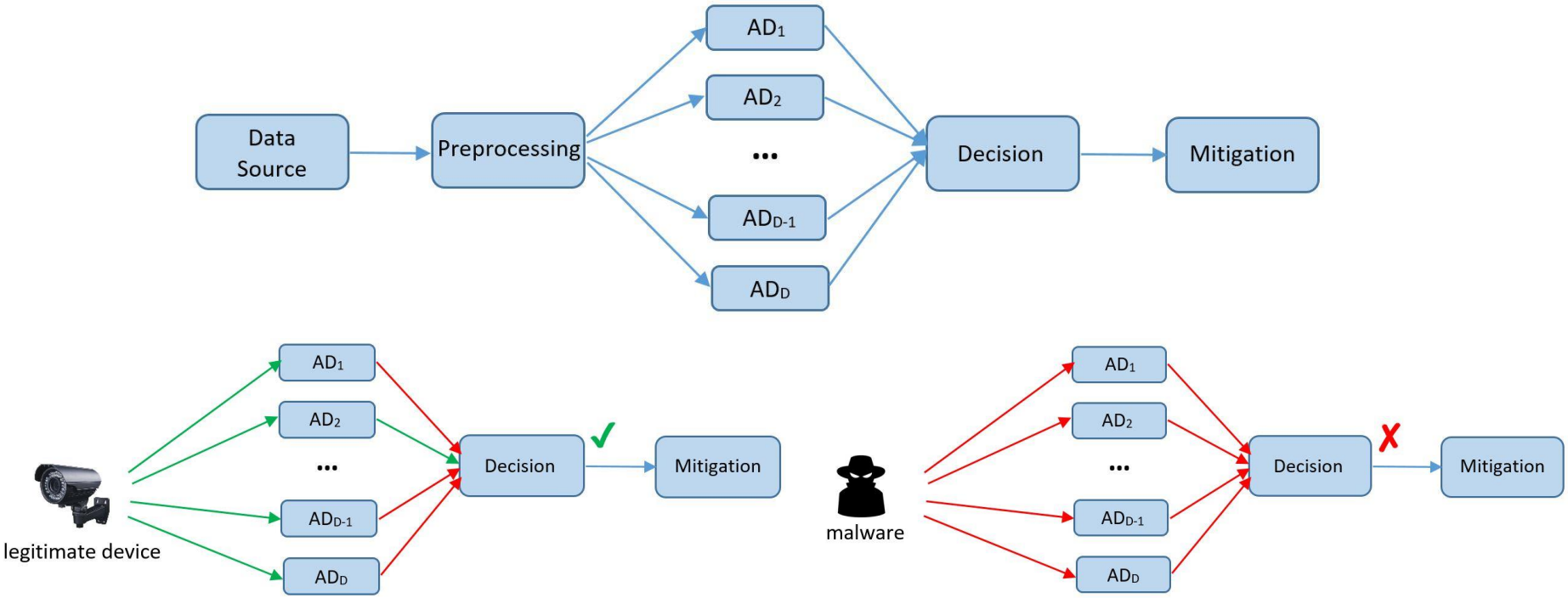


Experimental results:

- Traffic collected for 7 days from an experimental smarthome network. N = 10, timeout of 600 seconds.
- Six different supervised ML algorithms are tested to classify bidirectional flows: 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

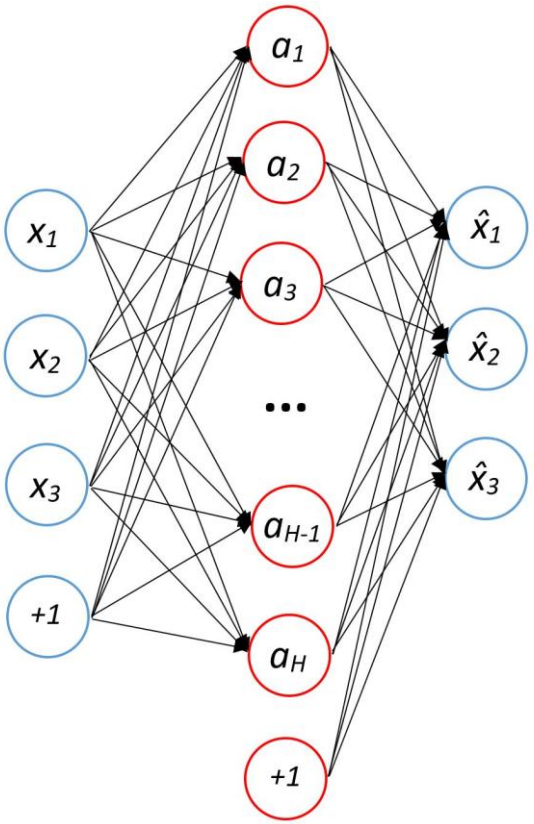
- Set of anomaly detectors(AD), each trained for a specific device type.



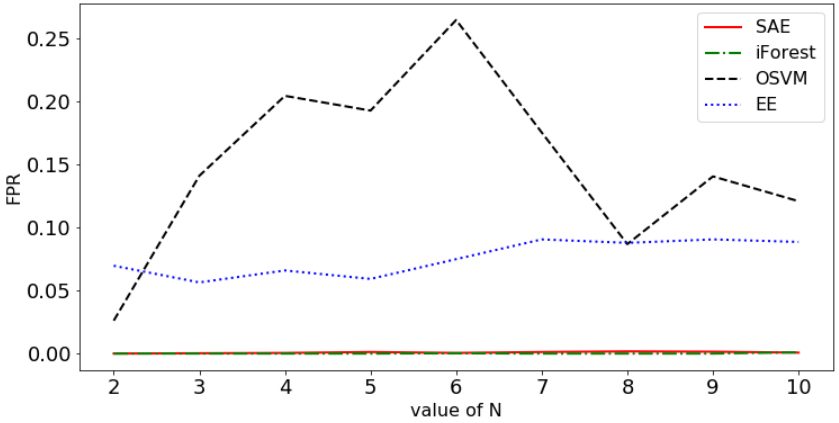
- Autoencoders learn to copy their inputs to their outputs under some constraints.
- An autoencoder is very bad at reconstructing outliers. Hence, the reconstruction error *RE* can be used to detect anomaly in IoT networks:

$$RE = \sum(\hat{x}_i - x_i)^2$$

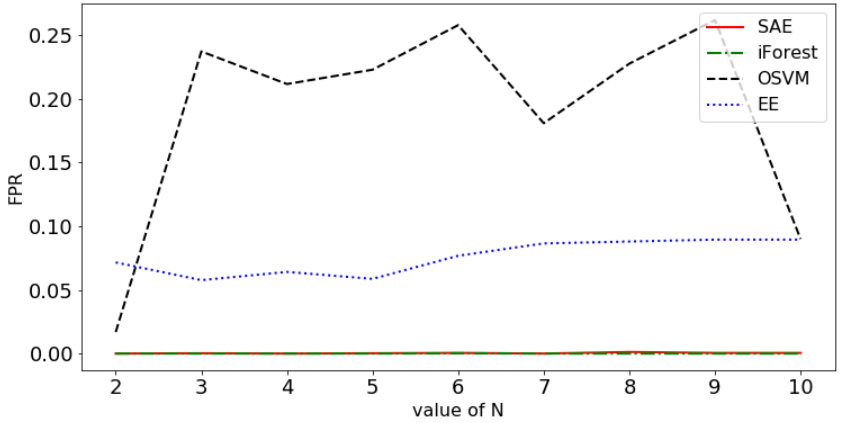
- The detection threshold is set so as to have a FPR on the validation set FPR_{Val} that is equal to $FPR_{desired}$.

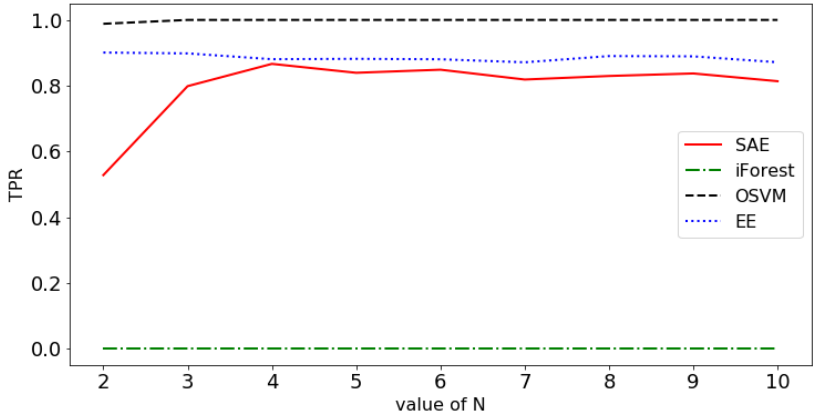


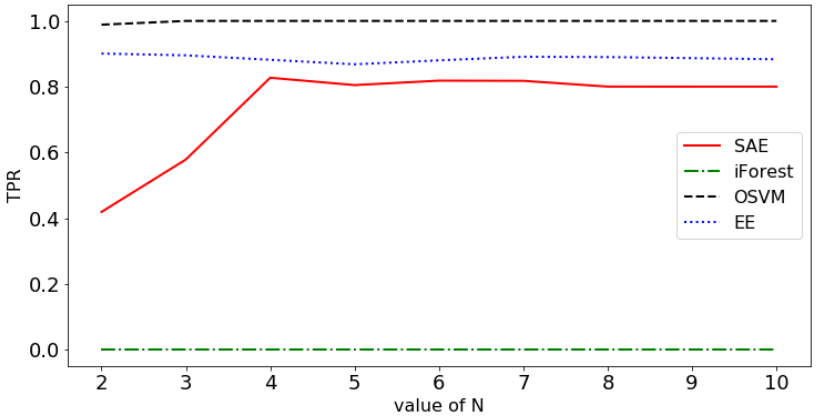
FPR_{Val} = 0.002



FPR_{Val} = 0.0005







- Difficulty to find publicly available IoT network traffic data. Privacy concerns. Physically deploying real IoT devices to produce real network traffic data can be very costly.

- We aim at generating bidirectional flows represented by a sequence of packet sizes and a duration. While generating packet-level features such as the size of individual packets, our generator implicitly comply with flow-level features such as the ordering of the packets, the total number of packets or bytes per flow, and the duration of the flow.

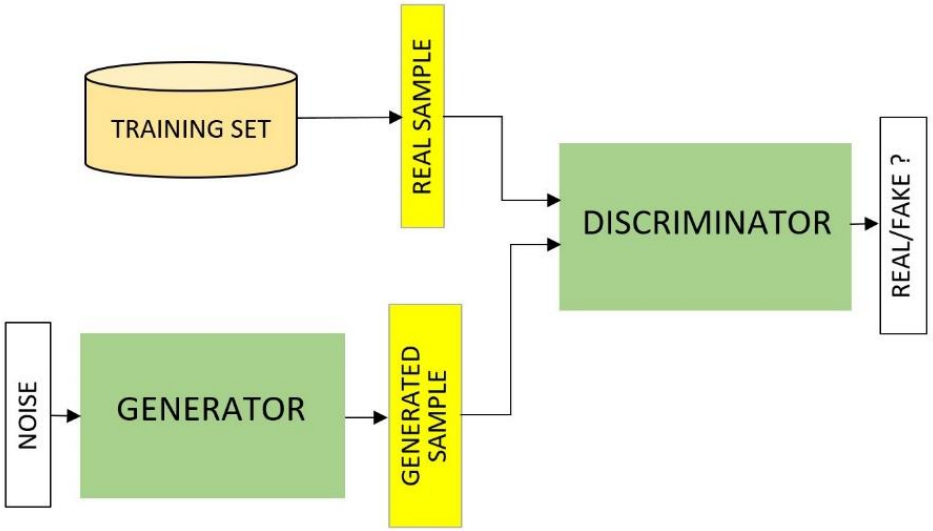
$$S = \{(size_1, direction_1), (size_2, direction_2), ..., (size_L, direction_L)\}$$

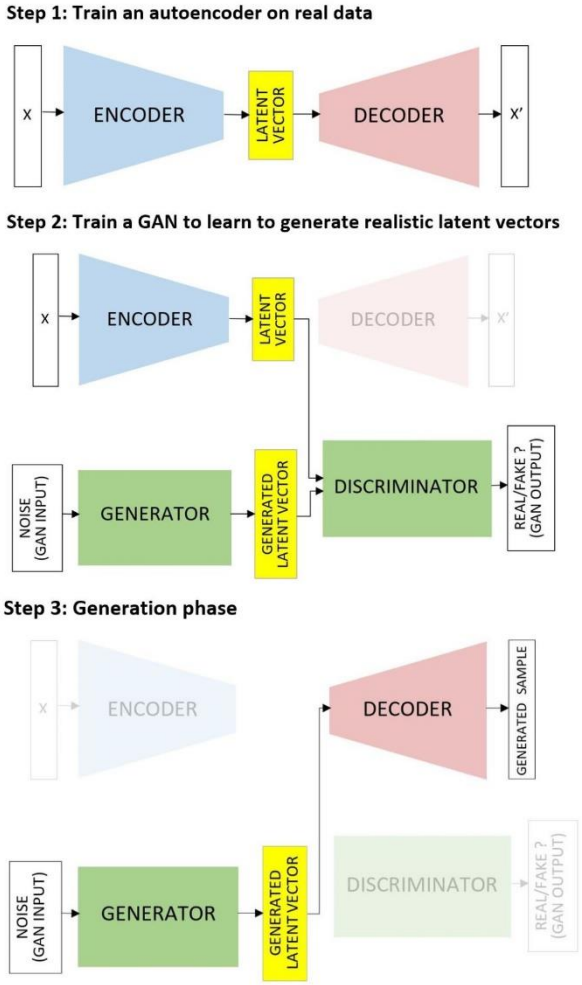
Example:

$$S = \{(60, sent), (60, received), (52, sent), (123, sent), (52, received), (135, received), (52, sent), (52, sent), (52, received), (52, sent), (0, PAD), ..., (0, PAD)\}$$

IoT Network Traffic Generation

- Generative Adversarial Networks (GAN) are special neural network architectures that learn to generate realistic looking data. A GAN consist of two components: a discriminator and a generator.

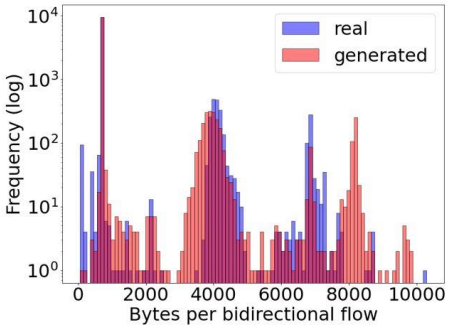


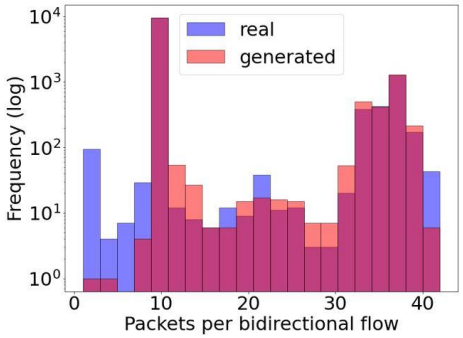


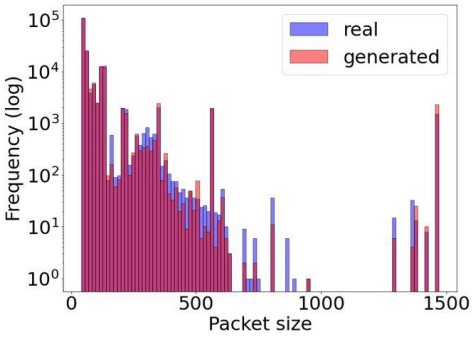
IoT Network Traffic Generation

- Experimental results obtained using network traffic data produced by a Google Home Mini.

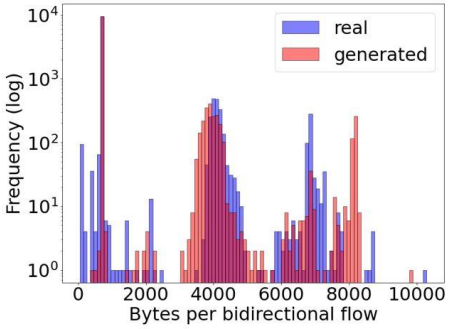
AE/WGAN-C

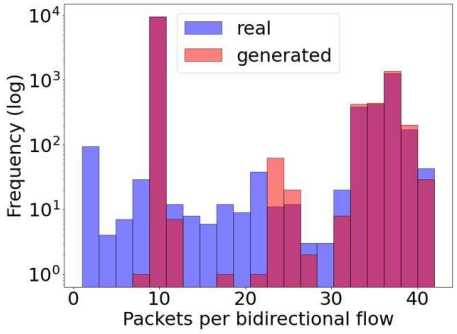


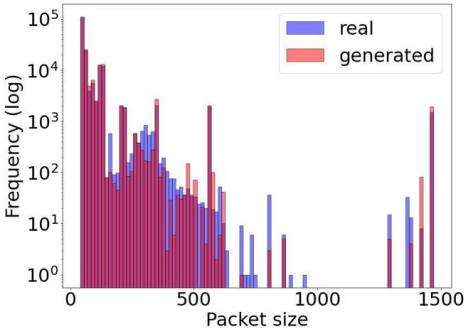




AE/WGAN-GP







Institut Mines-Télécom

Conclusion

Two ML based IoT network monitoring solutions were presented:

- IoT device type recognition system: supervised machine learning algorithms were trained to classify bidirectional flows based on the device type they belong to. An overall accuracy as high as 99.9% was achieved by the Random Forest classifier.

- IoT NIDS: autoencoders were trained to learn the legitimate networking behavior profile and to detect any deviation from it. Promising experimental results show that our method can achieve high TPR with a reasonable FPR.

- Synthetic IoT network traffic data generation: Generative Adversarial Networks (GANs) were trained to generate sequences of packet sizes and duration representing bidirectional flows.

List of Publications

M. R. Shahid, G. Blanc, Z. Zhang and H. Debar, "IoT Devices Recognition Through Network Traffic Analysis," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 5187-5192, doi: 10.1109/BigData.2018.8622243.

M. R. Shahid, G. Blanc, Z. Zhang and H. Debar, "Anomalous Communications Detection in IoT Networks Using Sparse Autoencoders," 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 2019, pp. 1-5, doi: 10.1109/NCA.2019.8935007.

M. R. Shahid, G. Blanc, H. Jmila, Z. Zhang and H. Debar, "Generative Deep Learning for Internet of Things Network Traffic Generation," 2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC), Perth, Australia, 2020, pp. 70-79, doi: 10.1109/PRDC50213.2020.00018.

Questions?