ANR PROJECT: GRIFIN

COGNITIVE AND PROGRAMMABLE SECURITY FOR RESILIENT NEXT-GENERATION NETWORKS

Authors

Gregory Blanc
IMT/Télécom SudParis
Institut Polytechnique de Paris

Thomas Silverston
LORIA, Université de Lorraine

Sébastien Tixeuil
LIP6, Sorbonne Université

Partners

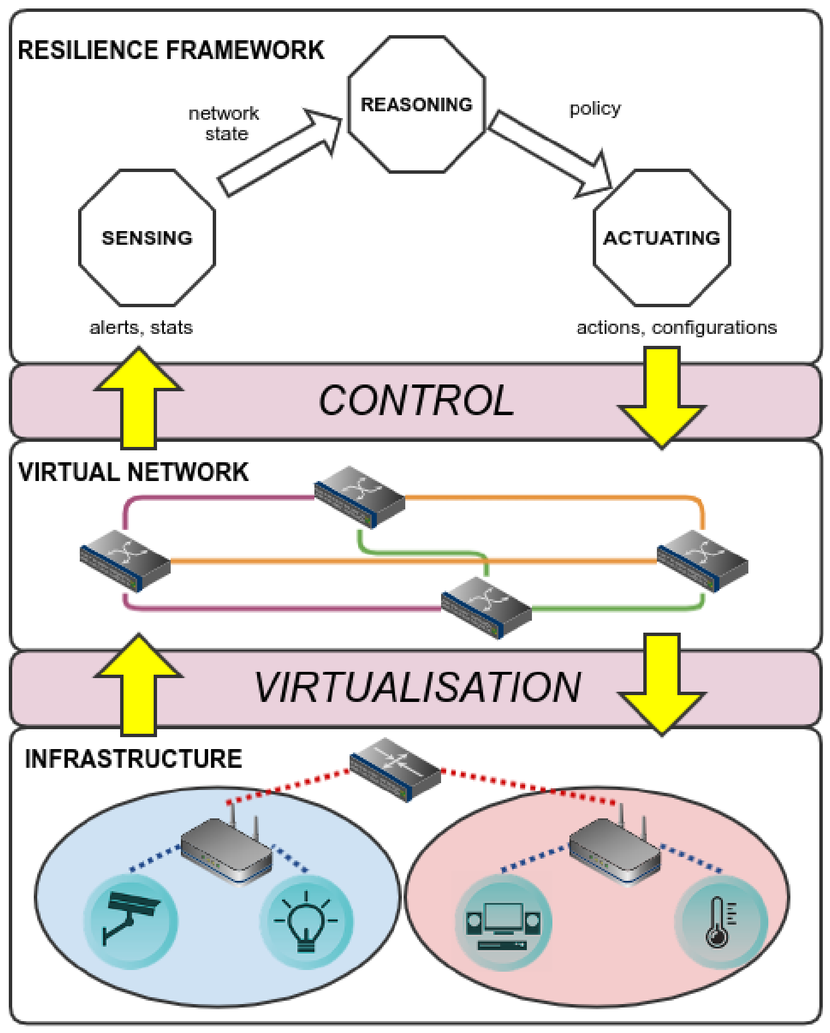
External Collaboration

Funding

ANR - PROJET FINANCÉ PAR L'ANR - PROJECT FUNDED BY THE ANR

TOWARDS RESILIENT NETWORK CONTROL

- IoT devices are a pervasive yet vulnerable resource, that can be compromised.
- Mirai is one such Internet catastrophe where 10^5 devices can be hijacked to generate TB/s of attack traffic.
- Such events are still rare but the number of (vulnerable) devices is growing: monitoring needs to be performed continuously.
- GRIFIN proposes to leverage **data-driven analytics** and **programmable network** infrastructure to provide **self-protection** to future, heterogeneous networks:
  - Distributed, fast, lightweight **sensing** for **anomaly detection**, leveraging *collaborative unsupervised learning*.
  - Situation-based **reasoning** for **countermeasure selection**, *assessing the network status in near real-time* and providing the most rewarding reactions.
  - Provable and programmable **actuating** for improved **resilience**, *ensuring* that network security policies are correctly and timely enforced with the infrastructure.



IOT ANOMALY DETECTION PRELIMINARY RESULTS

- Smart home devices exhibit *specific behaviours* that can be learnt by machines.
- Features such as the device's traffic **packets' sizes** and **inter-arrival times** can train an *auto-encoder* accurately.
- Lack of training data can be addressed:
  - Synthetic **traffic features generation** leveraging an *architecture mixing a GAN and an auto-encoder*
  - Learnt models in a *trustworthy* domain could be **transferred** to data-scarce ones

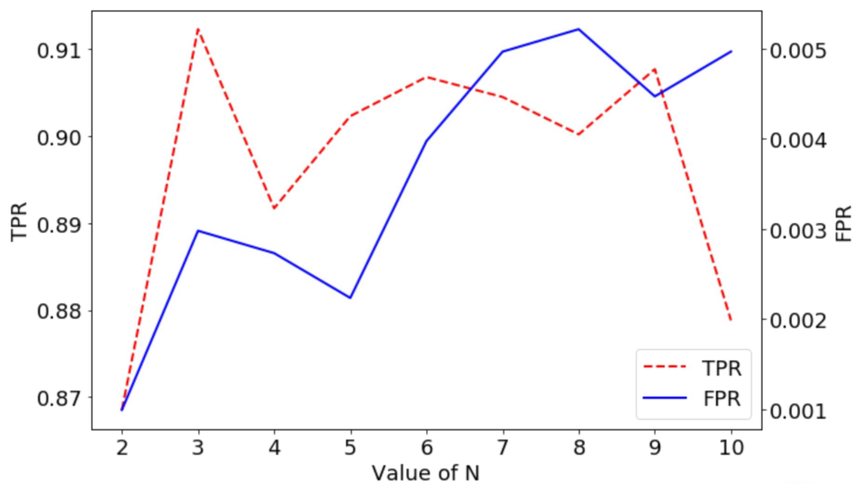


Figure 1. Performance of the anomaly detector w.r.t. the number of features (M.R. Shahid et al., NCA 2019)

PERSPECTIVES AND FUTURE WORKS

- Focus on **adaptive anomaly detection** to minimize retraining, by leveraging either *reinforcement learning* or *transfer learning*.
- Focus on intrusion detection **assessment** by producing *issue-specific datasets*.
- More information: https://cloudgravity.github.io/internships.html

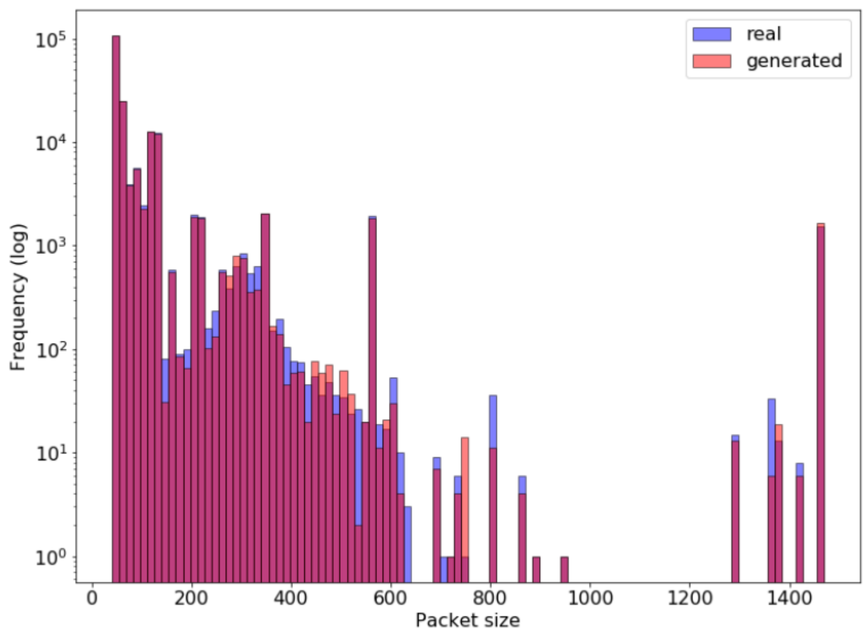


Figure 2. Distribution of packet sizes for real traffic and WGAN-C generated (M.R. Shahid et al., PRDC 2020)

4th Data Science Summer School
January 2021

Contact gregory.blanc@telecom-sudparis.eu

anr-grifin.telecom-sudparis.eu