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

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

Contact gregory.blanc@telecom-sudparis.eu