Cognitive and programmable security for resilient next-generation networks

GRIFIN

Programme : **AAPG**

Édition : **2020**

Instrument : **PRC**

Contact :
gregory.blanc@telecom-suparis.eu

COORDINATEUR : **Gregory Blanc**

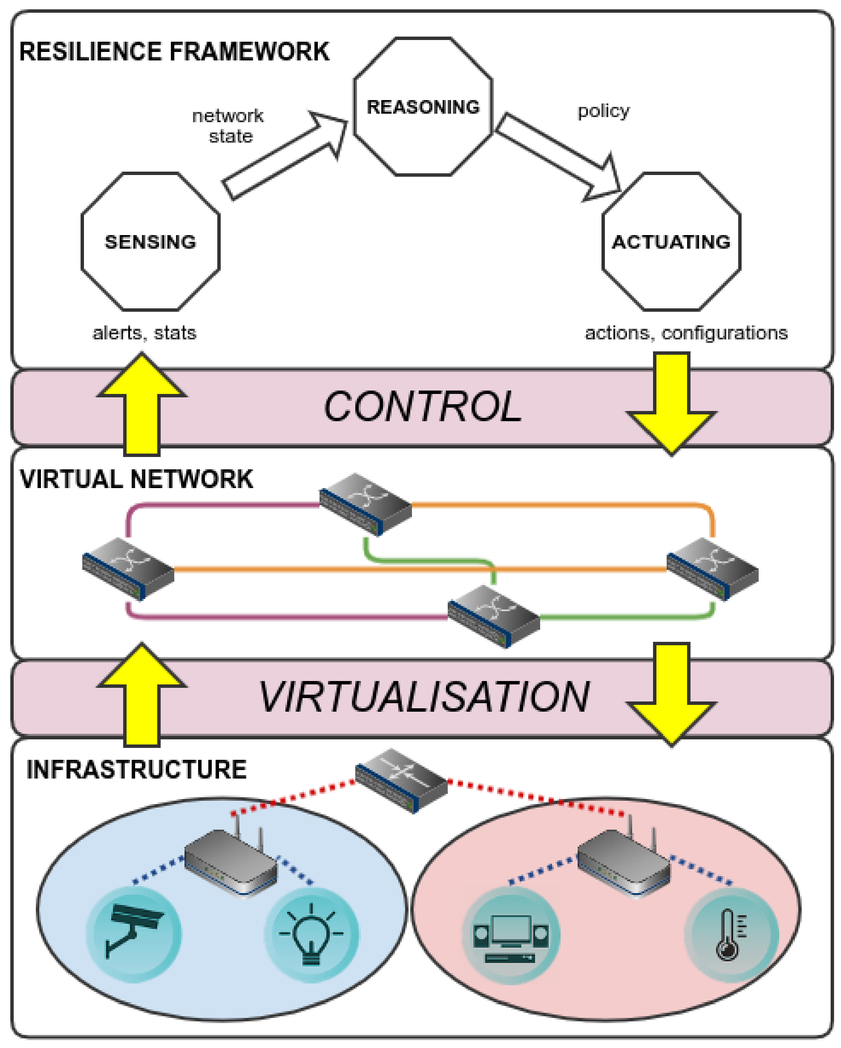
PARTENAIRE : **Télécom SudParis**

Résumé :
Les réseaux 5G (et au-delà) sont caractérisés par un volume de nœuds hétérogènes aux capacités très diverses et présente alors une surface d'attaque plus étendue et complexe. GRIFIN vise à développer une boucle de sécurité réseau programmable et pilotée par les données afin d'améliorer la résilience des réseaux 5G-IoT

CONTEXTE ET OBJECTIFS

Les réseaux 5G sont constitués de *slices* (réseaux virtuels) interconnectant de nombreux objets hétérogènes (de **sensibilités différentes**) sur une infrastructure **commune** (propulsée par des technologies telles que SDN ou NFV). Les menaces peuvent ainsi émaner des **objets terminaux**, que de l'**infrastructure virtualisée** et définie par les logiciels ou des multiples **prestataires** interagissant avec les slices et leurs utilisateurs. GRIFIN vise ainsi à renforcer la résilience de ces réseaux en s'appuyant :

- Une infrastructure de **collecte distribuée** permettant de modéliser précisément l'état normal du réseau afin de **détecter** toute **anomalie**, indicatrice d'intrusion
- Une infrastructure **programmable** permettant de **déployer** finement une **politique de sécurité abstraite**
- Un module de **sélection optimale de contremesures** permettant de **réduire l'impact** sur le trafic légitime



MÉTHODOLOGIE ET RÉSULTATS

Exploration de l'**apprentissage machine** pour exploiter la masse des données produites par les réseaux 5G :

- **apprentissage semi-supervisée** pour *modéliser le trafic normal* des objets IoT. Combinée à une approche d'**apprentissage par transfert**, pour *distribuer les capacités de détection* là où les données manquent;
- **apprentissage par renforcement** pour la *sélection de contremesures* prenant en compte l'état du réseau.

Par ailleurs, nous concevons un **canevas d'évaluation** de des détecteurs d'intrusion basés sur l'apprentissage machine qui soit *modulaire*, *vérifiable* et *explicable* :

- redéfinition de la **méthodologie de mesure** (propriété, jeu de données, métriques);
- formalisation de la **construction du jeu de données**;
- intégration des **bonnes pratiques** de l'apprentissage;
- focus sur la **qualité** des entrées, l'**explicabilité** des sorties et l'**amélioration continue** du processus

VALORISATION ET PERSPECTIVES

Ayoubi, Blanc, Jmila, Silverston, Tixeuil – *Data-driven Evaluation of Intrusion Detectors: a Methodological Framework* – FPS 2022

Formalisation du **module de construction de jeu de données**, et conception d'une solution de **sélection automatisée de contremesures** basée sur l'*apprentissage par renforcement*, en cours.