Cognitive and programmable security for resilient next-generation networks

GRIFIN

anr agence nationale de la recherche

Appel : AAPG

Année : 2020

Instrument : PRC

Contact : gregory.blanc@telecom-sudparis.eu

COORDINATEUR : Gregory Blanc

PARTENAIRES : IMT-TSP, LORIA, SORBONNE UNIVERSITE(LIP6)

Les réseaux 5G (et au-delà) sont caractérisés par un volume de nœuds autonomes aux capacités accrues mais présente une surface d'attaque plus étendue et complexe. GRIFIN a pour objectif de développer une boucle de sécurité réseau programmable pilotée par les données afin d'améliorer la résilience des réseaux IoT futurs.

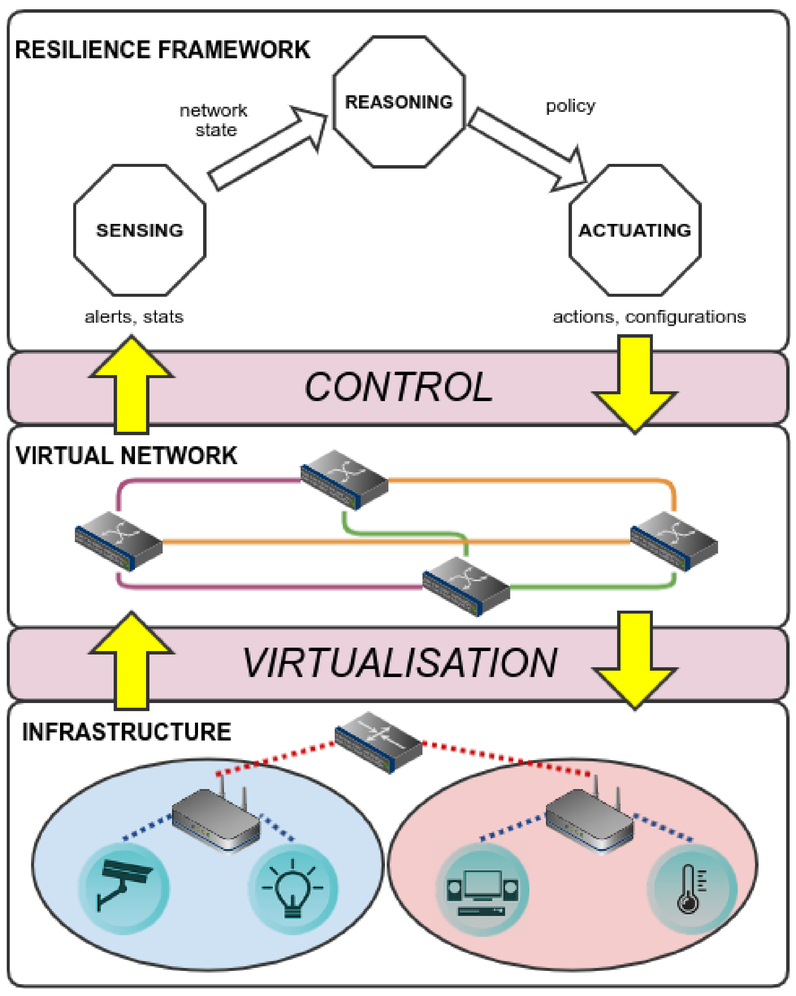
CONTEXTE ET OBJECTIFS

La mutualisation de *slices 5G* sur une même infrastructure réseau interconnectant de nombreux *objets* de *sensibilité hétérogène* constitue un défi de cybersécurité. Le projet GRIFIN vise à améliorer la *résilience* de ces réseaux en s'appuyant sur :

- les **données** de télémétrie et de sécurité par l'**apprentissage automatique** afin de remonter et caractériser les **incidents** de sécurité
- la **modélisation** de l'**état** du réseau afin de décider des **contre-mesures** de sécurité les plus appropriées
- la **programmabilité** des réseaux pour déployer des politiques de **résilience efficaces** et **vérifiables**

MÉTHODOLOGIE

Le projet se concentre sur deux axes principaux : exploiter le volume et l'hétérogénéité des données (*crowdsensing*) d'une part, et la programmabilité des réseaux virtualisés d'autre part. Les méthodes d'apprentissage automatique permettent d'extraire, à partir de données de trafic des objets connectés, collectées de manière **distribuée** et **périodique**, des motifs légitimes, permettant ainsi de proposer une approche de **détection d'anomalies** plus robuste. Un **canevas d'évaluation** est aussi proposée afin de tester notre approche de manière **reproductible**. Les incidents ainsi caractérisés représentent mieux l'état du réseau, afin d'améliorer sa **résilience** : les contre-mesures sont **sélectionnées** en fonction des menaces détectées et **qualifiées** selon leur impact sur l'état du réseau, en tenant compte d'éventuels **effets adverses**. Une approche d'**optimisation multi-objectifs** est ainsi envisagé. Puis, le déploiement des contre-mesures se fera au travers d'un langage de **programmation réseau** qui permet de **modéliser** finement les ressources et **vérifier** son adéquation à la **politique** de résilience.



RÉSULTATS

Dans sa première année, le projet GRIFIN s'est concentré sur la **détection distribuée et adaptative**, ainsi que sur l'**évaluation robuste** de la détection. En particulier, une **taxonomie** des différents travaux d'évaluation des détecteurs d'intrusion nous a permis de mieux appréhender le *manque de standardisation* des méthodes d'évaluation et les *lacunes* vis-à-vis des détecteurs d'anomalies, notamment ceux basés sur l'*apprentissage profond* ou exploitant l'*apprentissage non-supervisé*. D'autre part, nous avons étudié les aspects *distribué* et *adaptatif* (robuste aux changements) des détecteurs d'anomalies et proposé une approche combinant **réseaux récurrents** et **apprentissage par renforcement**.

FUTURS TRAVAUX

Un stage est proposé sur la modélisation de la politique de résilience et son déploiement vérifiable : https://anr-grifin.telecom-sudparis.eu/page/internships/

TELECOM SudParis | INSTITUT POLYTECHNIQUE DE PARIS | Loria | SORBONNE UNIVERSITÉ