Smart Grids Cyberphysical Security

Sujet de thèse IETR/IRISA

Mots-clés : Détection d'intrusion, Cyber-résilience-méthodes-résistance aux attaques, Systèmes cyber-physiques

Localisation : CentraleSupélec, campus de Rennes

Laboratoires : - IETR - Institut d'Electronique et des technologies du numérique, équipe Automatique
- IRISA - Institut de Recherche en Informatique et Systèmes Aléatoires, équipe Pirat

Contexte général

Dans un contexte critique autour de la gestion intelligente de l'énergie, la cybersécurité des infrastructures connectées est un enjeu crucial : en effet, les systèmes d'informations qui pilotent les systèmes physiques sont la cible de menaces croissantes et le bon fonctionnement de l'ensemble doit être garanti. Cette dimension physique de la cybersécurité s'ajoute au caractère classique de la sécurisation des réseaux et leurs nœuds : on parle de sécurité cyberphysique. La majorité des travaux actuels autour de la sécurité sont compartimentés, en étudiant le problème de manière très disciplinaire. L'objectif global de cette thèse est de définir des nouvelles méthodes de détection et de remédiation contre les attaques ciblant des systèmes de management de l'énergie dans bâtiments équipés de production électrique et connectés au réseau électrique. L'hypothèse retenue pour ce projet de thèse est qu'un attaquant peut corrompre un ou plusieurs composants du système (un capteur, un automate industriel, un onduleur), composants qui n'hébergent pas de solution de sécurité pour des raisons techniques et économiques. Il ne devient alors pas possible de détecter la compromission de manière isolée et seule une analyse du système dans sa globalité, qui exploite les incohérences entre la dimension numérique des données issues des capteurs et les dimensions physiques et énergétiques, peut détecter la compromission.

Afin d'exploiter au mieux les interactions énergétiques entre les composants, la démarche proposée se base sur la mise en place des modèles de consommation et de production qui seront utiles pour la synthèse d'observateurs et d'estimateurs d'état. Ces outils issus de l'automatique doivent permettre, en les combinant aux approches d'étude de compromission bas niveau, de développer de nouveaux mécanismes de détection et de mitigation. C'est bien cette combinaison transdisciplinaire qui offre une démarche de travail originale dans un domaine où de nombreux travaux sont menés. Les résultats seront éprouvés sur la plateforme « Smart And Secure Room » du laboratoire.

Description du travail

L'un des premiers objectifs de la thèse est d'offrir un cadre expérimental qui puisse collecter des traces (numériques et physiques) dans un système IoT couplé à un réseau d'énergie. Le second objectif est la simulation et l'émulation d'attaques attaques réalistes (IoT, automate de production d'énergie) afin de labelliser le dataset avec une vérité terrain. Les scénarios obtenus pourront ainsi être mis à disposition de la communauté et les données expérimentales pourront être valorisés en tant que dataset afin que la communauté puisse tester des méthodes de détection de compromission. Les verrous scientifiques sous-jacents à ces objectifs sont liés à la

difficulté de labellisation et de certification de jeux de données hétérogènes, qui prennent en compte la diversité des protocoles et les différentes natures physiques des signaux.

La seconde partie de la thèse sera consacrée à la détection d'attaque dans les Smart-Grids, sujet dans lequel la littérature se densifie fortement depuis deux ans. Les méthodes développées exploitent des techniques de synthèse d'observateurs mais en se limitant toujours au niveau « haut » dans un contexte très particulier : un type d'attaque donné sur un élément spécifique. Dans notre cas d'étude, l'hypothèse faite est que les objets connectés (capteurs, actionneurs, onduleurs, …) contribuant à la gestion du réseau d'énergie ne sont pas équipés de systèmes de sécurité. Il n'est ainsi pas possible de détecter la compromission au niveau composant, mais bien d'un point de vue global. Le défi scientifique inhérent est donc l'étude de la vulnérabilité du système énergétique dans son ensemble en combinant les différents niveaux d'étude, ce qui requiert une construction transdisciplinaire que nous voulons exploiter.

L'axe de travail proposé, constituant le troisième objectif de cette thèse, est alors est de concevoir des modèles reliant consommation, production d'énergie avec les autres grandeurs physiques à partir des données collectées. Les modèles obtenus seront utilisés pour prédire le bon fonctionnement du système dans sa globalité. C'est par cette approche que pourront être développées des méthodes de détection s'appuyant sur les traces observées couplées aux modèles énergétiques déterminés, constituant une véritable originalité par rapport aux travaux existants. Ces méthodes de détection seront ainsi éprouvées à la fois en simulation mais aussi en expérimentation réelle grâce à la plateforme « Smart And Secure Room », plateforme expérimentale de l'IETR et de l'IRISA dédiée aux vulnérabilités d'un système énergétique (https://www.ietr.fr/smart-and-secure-room).

Profil et compétences

Le profil recherché pour ces travaux est celui d'un étudiant ayant de solides bases en automatique (synthèse d'observateurs), une compréhension du système énergétique et/ou en informatique. La maîtrise de Matlab/Simulink est également souhaitée, tout comme le développement informatique (Python, Java ou C).

Compétences techniques

- Base de données
- Synthèse d'observateurs
- Sécurité (firewall, docker, OS linux)

Compétences transverses

- s'intégrer et échanger au sein d'une équipe de recherche
- communiquer de façon efficace et rigoureuse ses travaux, à l'oral et à l'écrit
- communiquer en anglais à l'oral et à l'écrit

Pour candidater

Envoyer un mail à Romain Bourdais (romain.bourdais@centralesupelec.fr) et Jean-François Lalande (jean-francois.lalande@centralesupelec.fr), accompagné d'un court CV et de relevés de notes récents. La date limite pour candidater est le **15/05/2024**.