Ecole Doctorale Interfaces
Université Paris-Saclay

Formation doctorale en Ingénierie des Systèmes Complexes

Un cadre de modélisation basé sur la simulation pour l'analyse et la protectiondes réseaux intelligents contre les fausses attaques tarifaires

A simulation-based modelling framework for the analysis and protection of smart grids against false pricing attacks

par Daogui TANG

Résumé de thèse

Doctorat d'Ingénierie des Systèmes Complexes

Laboratoire Génie Industriel - CentraleSupelec

N° 2021 – .01.

Thèse soutenue le 23 février 2021 à CentraleSupélec

Devant le jury composé de :

Min OUYANG Professeur, Huazhong University of Science and Technology	**Rapporteur**
Kash Barker Professeur Aoocié, University of Oklahoma	**Rapporteur**
Sonia Leva Professeur, Politechnico di Milano	**Examinateur**
Martin Hennebel Maître de Conférence, CentraleSupélec, Université Paris-Saclay	**Examinateur**
Enrico Zio Professeur, Politechnico di Milano	**Directeur de thèse**

Résumé:

L'intégration des technologies de l'information et de la communication (ICT) dans les réseaux électriques permet un échange de communication bidirectionnel entre les clients et les services publics, ce qui contribue engager les clients dans divers programmes de réponse `a la demande (DR) des réseaux intelligents (SG), tels que la tarification en fonction du temps d'utilisation (TOU) et la tarification en temps réel (RTP). Toutefois, cela expose les réseaux intelligents `a des menaces supplémentaires provenant de la couche ICT du système cyber physique. En effet, la menace de cyber-attaques est devenue une préoccupation majeure.

Dans ce contexte, la thèse se concentre sur la modélisation, la détection et la défense d'un type spécifique de cyber-attaques aux systèmes de DR, `a savoir les fausses attaques de tarification (FPA). L'étude aborde le problème tout d'abord en modélisant les FPA initiées dans les réseaux sociaux (SN). Le processus de propagation des faux prix de l'électricité´ est décrit par un modèle de propagation d'influence `a plusieurs niveaux qui tient compte des caractéristiques de la personnalité des clients et de la valeur de l'information. La simulation de Monte Carlo est utilisée pour tenir compte des caractéristiques stochastiques du processus de propagation de l'influence. Ensuite, en considérant l'intégration des ressources ´énergétiques renouvelables distribuées (DRER) dans le contexte des RTP, nous ´étudions les FPA où les attaquants manipulent les prix de l''électricité en temps réel en injectant de fausses informations sur la consommation et la production d''énergie renouvelable. En conséquence, un d´détecteur d'attaques en ligne base´ sur un réseau neuronal convolutif (CNN) est proposé pour d´détecter les FPA considérées.

Enfin, pour atténuer l'impact des FPAs, une stratégie de d´défense optimale est ´étudiée, compte tenu des ressources de d´défenses limitées. L'interaction dynamique entre les attaquants et les défenseurs est modélisée comme un jeu de Markov `a somme nulle où aucun des deux joueurs ne dispose d'informations complètes sur le modèle de jeu. Une méthode d'apprentissage de renforcement multi-agents sans modèle est proposée pour résoudre le jeu et trouver les politiques d'équilibre de Nash pour les deux joueurs.

Les résultats de la thèse donnent un aperçu de la façon dont les APF ont un impact sur les systèmes d''énergie cyber physique en trompant une partie des clients sur le marché de l''électricité et fournissent des implications sur la faon d'atténuer cet impact en d´détectant et en d´défendant les attaques.

Mots clés :

Réseaux intelligents, réponse la demande, cyber-attaques, réseaux neuronaux convolutifs, jeu de Markov, apprentissage par renforcement.

Abstract:

The integration of information and communication technology (ICT) systems with power systems enables a two-way communication exchange between customers and utilities, which helps engaging customers in various demand-response (DR) programs of smart grids (SGs), such as time-of-use (TOU) pricing and real-time pricing (RTP). However, this makes SG cyber-physical system exposed to additional threats coming from the ICT layer. For this reason, the threat of cyber attacks of various types has become a major concern.
In this context, the focus of the thesis is on the modeling of , detection of and defense from a specific type of cyber attacks to DR schemes, namely, false pricing attacks (FPAs). The study approaches the problem firstly by modeling FPAs initiated in social networks (SNs). The false electricity prices spreading process is described by a multi-level influence propagation model considering customers' personality characteristics and information value. Monte Carlo simulation is utilized to account for the stochastic nature of the influence propagation process.
Then, considering the integration of distributed renewable energy resources (DRERs) in the RTP context, we study FPAs where attackers manipulate real-time electricity prices by injecting false consumption and renewable generation information. A convolutional neural network (CNN)-based online detector is developed to detect the considered FPAs.
Finally, to mitigate the impact of FPAs, an optimal defense strategy is defined, under limited resources. The dynamic interaction between attackers and defenders is modeled as a zero-sum Markov game where neither player has full information of the game model. A model-free multi-agent reinforcement learning method is proposed to solve the game and find the Nash Equilibrium policies for both players.
The thesis provides a simulation-based framework for modelling FPAs to smart grids. The findings of the thesis give insights into how FPAs can impact cyber-physical power systems by misleading a portion of customers in the electricity market and provide implications on how to mitigate such impact by detecting and defending the attacks.

Key words:

Smart grids, demand-response, cyber attacks, false pricing attacks, convo-lutional neural networks, Markov game, reinforcement learning

L'Ecole Doctorale Interfaces de l'Université Paris-Saclay

L'Ecole Doctorale **INTERFACES - Approches interdisciplinaires: fondements, applications et innovations** rassemble des équipes dont les sujets de recherche se caractérisent par un positionnement principalement au **croisement de plusieurs disciplines** : la physique, la chimie, la biologie, mais également les mathématiques appliquées ou l'informatique.

L'ED Interfaces est co-opérée par 4 établissements de l'Université Paris-Saclay : Ecole Polytechnique, Université de Versailles - Saint-Quentin, CentraleSupélec, Ecole Nationale Supérieure des Techniques Avancées.

Le Laboratoire Génie Industriel

Le Génie Industriel se donne comme **défi scientifique** de "**maîtriser la conception et le management des systèmes complexes**".

- Maitriser c'est modéliser, simuler, optimiser, dimensionner, spécifier ...
- La conception est traitée en terme de faisabilité, utilité, utilisabilité, opérabilité, maintenabilité
- Le management est vu sous ses aspects performance, création de valeurs, risques, sûreté de fonctionnement, métriques

Les systèmes complexes abordés sont indifféremment des systèmes techniques, organisationnels, opérationnels, informationnels, décisionnels, tactiques, stratégiques

Le Laboratoire s'organise en quatre équipes de recherche :

- **Equipe DE : Design Engineering**
- **Equipe OM: Operations Management for production and distribution systems of goods and services**
- **Equipe SR : Safety & Risks**
- **Equipe SE : Sustainable Economy**

Les thèses se font principalement dans l'un des domaines scientifiques relatifs à une équipe, même s'il peut arriver qu'elles se fassent transversalement à ces dernières. C'est la complexité des approches (robust-design, axiomatic-design, approche systémique, recherche opérationnelle, modèles stochastiques, évaluation des performances …) qui fait la force, la performance et l'originalité du Laboratoire.

LGi
Laboratoire Génie Industriel