Optimisation dynamique de l'apprentissage fédéré pour la détection d'intrusions dans les réseaux IoT basée sur des GNN et la sélection intelligente des clients

Le développement rapide des systèmes Internet des Objets (IoT) et des infrastructures cyber-physiques a considérablement accru la complexité de la gestion et de la sécurisation des environnements distribués. Dans ce contexte, les systèmes de détection d'intrusions (IDS) basés sur l'intelligence artificielle constituent une solution prometteuse pour identifier efficacement les comportements malveillants dans des environnements dynamiques et hétérogènes.

Parmi les approches récentes, les Graph Neural Networks (GNN) se distinguent par leur capacité à modéliser les relations complexes entre équipements, flux réseau et interactions topologiques, permettant ainsi d'améliorer significativement la détection d'attaques dans les réseaux IoT. Toutefois, l'apprentissage centralisé de ces modèles présente plusieurs limitations majeures, notamment des contraintes liées à la confidentialité des données, à la scalabilité, aux coûts de communication et aux ressources computationnelles limitées des dispositifs IoT. L'apprentissage fédéré (Federated Learning, FL) constitue une alternative pertinente en permettant un entraînement collaboratif des modèles tout en conservant les données localement sur chaque client. Cette approche améliore la confidentialité et la scalabilité, mais son efficacité dépend fortement de la sélection des clients participant à chaque cycle d'apprentissage. En effet, dans les réseaux IoT, les clients présentent une forte hétérogénéité en termes de capacité de calcul, disponibilité, qualité des données locales et conditions réseau.

Cette thèse vise ainsi à adresser deux verrous scientifiques complémentaires. Le premier consiste à développer des architectures de GNN fédérés adaptées à la détection d'intrusions dans les réseaux IoT, capables d'exploiter efficacement les structures relationnelles des données distribuées tout en assurant robustesse et performance de détection. Le second porte sur l'optimisation dynamique de la sélection des clients dans le processus d'apprentissage fédéré.

Dans ce cadre, la sélection des clients sera modélisée comme un problème d'optimisation combinatoire multi-objectif sous contraintes, visant à sélectionner dynamiquement un ensemble optimal de clients permettant de maximiser les performances globales du modèle tout en minimisant les coûts de communication, le temps d'exécution et l'utilisation des ressources computationnelles.

Pour répondre à ce problème, des approches d'optimisation exactes (programmation linéaire en nombres entiers, branch-and-bound) ainsi que des approches approchées basées sur des heuristiques et métaheuristiques (algorithmes génétiques, recherche tabou, méthodes hybrides) seront étudiées et adaptées au contexte dynamique du FL.

Les approches proposées seront évaluées dans le cadre de systèmes IDS pour réseaux IoT, afin d'analyser conjointement l'impact des architectures GNN fédérées et des stratégies de sélection dynamique sur la qualité de détection, la convergence du modèle et l'efficacité globale du processus fédéré.

Cette recherche vise ainsi à proposer une approche intégrée combinant intelligence artificielle distribuée, cybersécurité et optimisation, afin de développer des solutions robustes, scalables et adaptées aux contraintes réelles des environnements IoT.