Approches hybrides basées sur l'IA pour la spécification et le déploiement des politiques de réaction dans l'IoT

Codirecteurs :

Samiha Ayed (samiha.ayed@utt.fr); UTT

Lamia Chaari Fourati (lamia.chaari@isims.usf.tn); US

Contexte et problématique

L'Internet des Objets (IoT) représente un ensemble d'appareils connectés qui interagissent pour offrir des services intelligents dans divers domaines tels que la santé, l'industrie, la maison intelligente et les villes connectées. Cependant, cette interconnexion massive engendre des risques de cyberattaques en raison de la diversité des dispositifs, des protocoles et des contraintes de ressources. Les approches de cybersécurité classiques, souvent statiques et basées sur des règles prédéfinies, ne suffisent plus pour faire face à l'évolution rapide des menaces.

Dans ce contexte, l'automatisation et l'adaptation des politiques de réaction aux attaques deviennent essentielles pour garantir la sécurité des environnements IoT. Une approche prometteuse consiste à combiner Deep Learning (DL) et Apprentissage par Renforcement (RL) pour proposer des politiques de réaction intelligentes, dynamiques et contextuelles. Le DL permet une détection efficace des menaces en exploitant des techniques avancées d'apprentissage automatique, tandis que le RL permet une prise de décision optimisée et une adaptation continue aux nouvelles menaces.

L'objectif de cette recherche est d'explorer les architectures hybrides DL-RL pour la spécification et le déploiement des politiques de réaction en IoT, en les intégrant dans un cadre applicatif spécifique et en validant leur efficacité à l'aide d'outils formels et d'évaluations expérimentales.

Objectifs et contributions

Ce travail vise à :

- Étudier l'état de l'art des approches hybrides (DL et RL) dans la gestion des politiques de réaction en cybersécurité IoT.
- Spécifier formellement des politiques de réaction dynamiques et contextuelles pour améliorer la résilience des systèmes IoT.
- Proposer une approche hybride DL-RL pour automatiser la détection et l'adaptation des réactions face aux cybermenaces.
- Intégrer ces politiques en temps réel dans un environnement IoT à l'aide d'un cadre applicatif spécifique.
- Vérifier formellement la robustesse et la cohérence des politiques proposées à l'aide de modèles formels (langage Z, Model Checking, etc.).
- Évaluer expérimentalement l'approche sur des plateformes IoT et comparer les performances aux méthodes existantes.

Plan des travaux et tâches principales

Tâche 1 : Revue de l'état de l'art

- Étudier les menaces et vulnérabilités dans les environnements IoT.
- Analyser les approches basées sur le Deep Learning pour la détection des attaques et leur pertinence pour l'IoT.

- Étudier l'application de l'Apprentissage par Renforcement pour l'optimisation des réactions aux cyberattaques.
- Examiner les approches hybrides existantes combinant DL et RL pour la sécurité des systèmes distribués.
- Identifier les limitations des solutions actuelles et les opportunités pour de nouvelles améliorations.

Tâche 2 : Spécification formelle des politiques de réaction

- Définir un modèle formel des politiques de réaction en IoT.
- Spécifier des politiques dynamiques et contextuelles adaptées aux environnements IoT hétérogènes.
- Prendre en compte les contraintes de ressources et d'exécution des dispositifs IoT.
- Élaborer un modèle de prise de décision automatique basé sur la détection d'anomalies et l'apprentissage adaptatif.

Tâche 3 : Conception et mise en œuvre d'approches hybrides DL-RL

- Développer un modèle de Deep Learning pour la détection des menaces en temps réel.
- Implémenter un agent d'Apprentissage par Renforcement capable de prendre des décisions optimales en fonction du contexte de l'attaque.
- Proposer un cadre d'intégration DL-RL pour assurer une interaction fluide entre la détection et la réaction.
- Expérimenter différentes architectures DL-RL (ex. DQN, PPO, A3C) et optimiser leurs performances.

Tâche 4 : Intégration en temps réel des politiques de réaction

- Sélectionner un cadre applicatif IoT (ex. Edge Computing, Fog Computing) pour l'implémentation de l'approche.
- Développer un système embarqué permettant l'exécution des politiques de réaction en temps réel.
- Assurer la scalabilité et la compatibilité avec différents types d'objets connectés.
- Évaluer la latence et l'impact des politiques sur la performance des systèmes IoT.

Tâche 5 : Vérification formelle des politiques de réaction

- Utiliser un outil de spécification formelle (ex. Langage Z, Model Checking, TLA+) pour vérifier la cohérence et la sûreté des politiques de réaction proposées.
- Valider les propriétés de sécurité (ex. absence de comportements indéterministes, respect des contraintes de confidentialité et d'intégrité).
- Détecter et corriger d'éventuelles failles avant le déploiement.

Tâche 6 : Évaluation et validation expérimentale

- Mettre en place une plateforme de test pour évaluer l'approche hybride (simulateur IoT, banc d'essai réel).
- Comparer la précision de détection, la rapidité de réaction, et la résilience aux cyberattaques par rapport aux méthodes classiques.
- Analyser les gains en autonomie et en efficacité apportés par l'intégration DL-RL.
- Publier les résultats et discuter des perspectives d'amélioration et d'extension.

Résultats attendus

- Un état de l'art approfondi des approches hybrides DL-RL en cybersécurité IoT.
- Une modélisation formelle des politiques de réaction permettant une meilleure compréhension et validation des décisions de sécurité.

- Une solution hybride DL-RL efficace, capable de détecter et de répondre dynamiquement aux attaques en IoT.
- Un prototype fonctionnel intégré dans un cadre applicatif IoT, démontrant l'efficacité de l'approche en conditions réelles.
- Une évaluation expérimentale rigoureuse, validant les performances de l'approche par rapport aux solutions traditionnelles.
- Une approche vérifiée formellement, garantissant la robustesse et la fiabilité des décisions de sécurité.

Références :

1. Malka N. Halgamuge, Dusit Niyato, Adaptive edge security framework for dynamic IoT security policies in diverse environments, Computers & Security, Volume 148, 2025
2. Jehad Ali, Sushil Kumar Singh, Weiwei Jiang, Abdulmajeed M. Alenezi, Muhammad Islam, Yousef Ibrahim Daradkeh, Asif Mehmood, A deep dive into cybersecurity solutions for AI-driven IoT-enabled smart cities in advanced communication networks, Computer Communications, Volume 229, 2025
3. Heng Zeng, Manal Yunis, Ayman Khalil, Nawazish Mirza,
4. Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity, Journal of Innovation & Knowledge, Volume 9, Issue 4, 2024
5. Fatima Alwahedi, Alyazia Aldhaheri, Mohamed Amine Ferrag, Ammar Battah, Norbert Tihanyi, Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models, Internet of Things and Cyber-Physical Systems, Volume 4, 2024
6. Achref Haddaji, Samiha Ayed, Lamia Chaari Fourati, Artificial Intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey, Computers and Electrical Engineering, Volume 104, Part B, 2022
7. Fadhila Tlili, Samiha Ayed, Lamia Chaari Fourati, Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS), Computers & Security, Volume 142, 2024
8. Shunqi Zeng, Chunyan Huang, Fei Wang, Xin Li, Minghui Chen, A Policy optimization-based Deep Reinforcement Learning method for data-driven output voltage control of grid connected solid oxide fuel cell considering operation constraints, Energy Reports, Volume 10, 2023
9. Qiang Zhou, Yefei Yang, Fangfang Ma, A Stackelberg-based deep reinforcement learning approach for dynamic cooperative advertising in a two-echelon supply chain, Computers & Chemical Engineering, Volume 196, 2025
10. Serdar Coskun, Ozan Yazar, Fengqi Zhang, Lin Li, Cong Huang, Hamid Reza Karimi, A multi-objective hierarchical deep reinforcement learning algorithm for connected and automated HEVs energy management, Control Engineering Practice, Volume 153, 2024