De l'organisation d'un système multi-agent de cyberdéfense

Julien Soulé[1,2]
julien.soule@lcis.grenoble-inp.fr

Jean-Paul Jamont[1], Michel Occello[1]
{jean-paul.jamont, michel.occello}@lcis.grenoble-inp.fr

Paul Théron[3]
paul.theron@orange.fr

[1]Univ. Grenoble Alpes, Grenoble INP, LCIS, Valence, France

[2]Thales Land and Air Systems, BL IAS, Rennes, France

[3]AICA IWG, La Guillermie, France

Résumé

Ce poster présente un travail de thèse s'intéressant aux systèmes de cyberdéfense vus comme des ensembles d'entités autonomes coopérantes et déployables au plus près des points sensibles d'un environnement hôte en réseau.

Mots-clés : *cyberdéfense, système multi-agent, organisation*

Abstract

This poster presents a PhD work focusing on cyber-defence systems modeled as a set of cooperating and deployable autonomous entities as close as possible to the critical points of a host networked environment.

Keywords : *cyber-defence, multi-agent system, organization*

1 Contexte et problématique

Le groupe de travail *AICA IWG* [1] développe des travaux sur les agents *AICA (Autonomous Intelligent Cyber-defence Agent)*. L'agent *AICA* doit pouvoir être déployé sur un système hôte pour détecter, identifier et caractériser des anomalies/attaques, élaborer et piloter l'exécution de contre-mesures et dialoguer avec l'extérieur. L'agent *AICA* peut être vu comme un Système Multi-Agent (SMA) permettant ainsi de prendre en charge l'ouverture, le passage à l'échelle et l'autonomie de la cyberdéfense en déléguant ses différentes fonctions aux agents. Notre problématique consiste à définir l'organisation du SMA qui permettrait d'assurer la cyberdéfense compte tenu des contraintes de l'environnement hôte.

2 Aperçu des travaux

Nous avons conduit une revue des SMAs de cyberdéfense disponibles[3]. La majorité des systèmes étudiés ont une organisation centralisée et se concentrent sur la détection d'anomalies. Peu de travaux traitent d'organisation et d'objectifs de cyberdéfense différents (recherche de contre-mesures adaptées…) et ils sont peu établis dans la pratique. Cependant, en raison de la subjectivité de la classification et du manque de cohérence entre les systèmes, une modélisation commune des SMAs de cyberdéfense évoluant dans un environnement cyber permet leur comparaison dans un cadre d'évaluation de référence.

Une première proposition de modèle repose sur les *Decentralized Partially Observable Markov Decision Process (Dec-POMDP)* et permet de représenter l'environnement, des agents d'attaque et de défense ainsi que leurs interactions. Nous avons implémenté ce modèle au travers du simulateur *Multi Cyber Agent Simulator* [2] qui permet de modéliser, implémenter et évaluer plusieurs organisations de SMA de cyberdéfense.

3 Conclusion et perspectives

Outre l'amélioration du simulateur, l'utilisation plus approfondie de la décentralisation et de la coopération pourrait contribuer à concevoir des systèmes de cyberdéfense plus adaptatifs et opérationnels dans des contextes réalistes.

Références

[1] AICA IWG. `https://www.aica-iwg.org/`.

[2] Multi cyber agent simulator. `https://github.com/julien6/MCAS`. Accessed : 2023-03-07.

[3] J. Soule et al. De l'organisation des systèmes multi-agents de cyber-defense. In *RESSI*, 2023.