De l'Organisation des Systèmes Multi-Agents de Cyber-defense

Julien Soulé
Thales Land and Air Systems, BU IAS
Univ. Grenoble Alpes,
Grenoble INP, LCIS, 26000,
Valence, France
julien.soule@lcis.grenoble-inp.fr

Jean-Paul Jamont*, Michel Occello†
Univ. Grenoble Alpes,
Grenoble INP, LCIS, 26000,
Valence, France
{*jean-paul.jamont,†michel.occello}@lcis.grenoble-inp.fr

Paul Théron
Co-leader du RTG 152 OTAN, 1er Président de l'AICA IWG
La Guillermie, France
paul.theron@orange.fr

Louis-Marie Traonouez
Thales Land and Air Systems, BU IAS
Rennes, France
louis-marie.traonouez@thalesgroup.com

***Résumé*—Un système multi-agent est composé d'entités autonomes capables d'adapter leur comportement et leur organisation à des contraintes externes. Déployé au plus près des points sensibles du système hôte, il peut être un élément de réponse pour prendre en compte la complexité et l'évolutivité des cyber-attaques. L'objectif de cet article est de discuter des mécanismes organisationnels multi-agent permettant d'atteindre des objectifs de cyber-défense sous des contraintes liées à l'environnement. Il présente ensuite les défis et les premières pistes pour un système multi-agent auto/ré-organisé sécurisant un système en réseau.**

I. Introduction

Le développement de l'« Internet of Things » et de l'« Internet of Battle Things » a entrainé une augmentation de la surface d'attaque des systèmes en réseau permettant à des attaquants de s'y introduire en ciblant les nœuds les plus faiblement défendus. Tenant compte de ce contexte, le groupe de travail « AICA IWG »[1] a poursuivi le développement des travaux concernant l'agent AICA (Autonomous Intelligent Cyber-defence Agent). Un agent est par définition une entité autonome capable de percevoir son environnement local grâce à des capteurs, et d'agir sur cet environnement à l'aide d'effecteurs [15]. 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. À cette fin, il est conçu comme proactif, discret et capable d'apprendre.

L'agent AICA peut être vu comme un Système Multi-Agent (SMA). Le paradigme multi-agent offre des moyens de gérer l'ouverture, le passage à l'échelle et l'autonomie du système hôte en déléguant différents aspects de la cyber-défense à différents agents. L'agent AICA est alors un système collectif décentralisé et distribué d'agents cyber-défenseurs déployés au plus près des composants du système [11].

1. Ce groupe de travail (voir https://www.aica-iwg.org/) s'appuie sur les résultats du *Research Task Group IST-152* de l'OTAN qui a travaillé sur le concept des « Intelligent, Autonomous and Trusted Agents for Cyber Defense and Resilience ».

Concevoir un tel SMA, nécessite de porter une attention particulière à son organisation. L'objectif de cet article est de discuter des mécanismes organisationnels d'un SMA de cyberdéfense. La section II introduit un état de l'art de SMA existants assurant la cyber-défense sur leur système hôte. La section III identifie les verrous théoriques et techniques potentiels vers la conception d'un SMA de cyber-défense auto/ré-organisé et propose des préconisations.

II. État de l'art

A. Vers des systèmes multi-agents de cyber-défense

Nous inscrivant dans le prolongement des travaux menés dans le cadre de l'AICA IWG, nous considérons la **cyber-sécurité** comme l'ensemble des activités consistant à se protéger de façon préventive contre les cyber-attaques [17].

Nous désignons par **cyber-défense** l'ensemble des activités entreprises lorsqu'une cyber-attaque est détectée et qu'il faut réagir. Ces activités sont décrites dans le cadre du « P3R3 Resilience Engineering Framework » [16] et sont regroupées en trois fonctions de cyber-défense :

R1 - Detect and alarm : détection des cyber-attaques et déclenchement des mécanismes de réponse ;

R2 - Respond and restore : mise en œuvre et suivi des réponses apportées aux cyber-attaques et l restauration des niveaux de services/activités minimaux. La gestion de la crise provoquée par l'attaque est au cœur de cette fonction ;

R3 - Recover and rebound : rétablissement des parties endommagées du système à défendre et traitement final des conséquences. Ce point inclut une phase d'apprentissage permettant l'amélioration du système de cyber-défense.

Nous appelons **objectifs de cyber-défense**, tous les objectifs impliquant la mise en œuvre d'une ou plusieurs des fonctions de cyber-défense.

Dans un **SMA de cyber-défense**, plusieurs agents atteignent un objectif global de cyber-défense par un comportement collectif résultant de la réalisation de sous-objectifs individuels

et/ou de mécanismes locaux [10]. Des exemples de tels sous-objectifs pourraient être la détection des intrusions, la mise en œuvre d'un plan de récupération, la restauration d'une image, redirection des ports…

B. Mécanismes organisationnels dynamiques

L'autonomie de fonctionnement du SMA de cyber-défense, obtenue en déléguant aux agents certaines missions est une réponse face aux charges de travail des équipes cyber et à la rapidité des cyber-attaques [11]. Un tel SMA doit modifier sa structure et les relations entre ses agents pour continuellement s'adapter à son environnement [17].

En considérant un point de vue centré organisation, la cyber-défense globale est une tâche commune partagée par tous les agents à travers leur organisation. La **ré-organisation** est un moyen de basculer entre plusieurs organisations éprouvées qui semblent adaptées dans des circonstances données [14].

En considérant un point de vue centré agent, l'**auto-organisation** est définie comme un processus ascendant où l'organisation émerge des interactions et des actions locales des agents. La cyber-défense globale résulte alors des actions de cyber-défense locales et des interactions pair à pair entre les agents [14]. L'auto-organisation semble être un des moyens à mobiliser pour faire face aux cyber-menaces en évitant les écueils d'un contrôle centralisé.

C. Organisations des SMA de cyber-défense

Le choix d'une organisation de SMA de cyber-défense implique de tenir compte des relations entre les objectifs de cyber-défense et l'environnement de déploiement. L'analyse des SMA de cyber-défense disponibles est susceptible d'indiquer des tendances pour ces relations. Cela permettrait de favoriser la mise en œuvre d'une organisation à partir des objectifs de cyber-défense et l'environnement de déploiement.

Notre revue de littérature s'est concentrée sur le rapprochement des notions des SMA et de la cyber-défense.

Pour chacun des travaux de SMA de cyber-défense, nous nous sommes intéressés aux fonctions de cyber-défense couvertes. Un aperçu de cette classification est proposé en table II. Nous avons constaté que la plupart des objectifs de cyber-défense des SMA se concentrent principalement sur la détection d'anomalies et d'intrusions (plus de 50% des travaux de notre revue complète se focalisent ainsi sur la fonction R1).

Pour chacun de ces mêmes travaux, nous nous sommes aussi intéressés aux caractéristiques principales de l'organisation et de l'environnement de déploiement. Un aperçu de ce travail est présenté en table I Nous constatons qu'indépendamment des objectifs de cyber-défense, l'organisation centralisée et/ou hiérarchique est la plus répandue parmi les SMA de cyber-défense étudiés. La centralisation des données acquises de l'environnement, en un seul point, favorise de meilleures performances pour l'analyse de la situation globale et le contrôle du système de cyber-défense. Ces types d'organisation semblent moins facilement s'appliquer pour des réseaux dynamiques, mais sont répandus sur des systèmes de taille moyenne avec des contraintes connues [18]. Les organisations de type décentralisé tirent profit d'une approche davantage auto-organisée pour faire face aux cyber-menaces de façon à augmenter l'autonomie du SMA de cyber-défense comme proposé dans le « Artificial Immune System » [9] ou la « Ant-Based Cyber Security » [8].

III. Vers un mécanisme général d'organisation de la cyber-défense en réseau

La revue a permis d'identifier de premiers mécanismes sous-jacents à un SMA de cyber-défense. Cependant, il est nécessaire de la compléter par une étape d'expérimentation. En effet, notre classification ne permet pas de définir de façon certaine des recommandations de conception d'organisation pour un SMA de cyber-défense générique. La diversité (des objectifs, des environnements, des architectures d'agents, des protocoles d'interaction…) des SMA de cyber-défense disponibles rend l'appréciation entre ces derniers difficiles sans cadre commun.

A. Vers un modèle expérimental de la situation

Il apparaît nécessaire de caractériser le SMA de cyber-défense et l'environnement dans lequel il est déployé.

Un modèle générique permettrait alors de représenter des scénarios d'attaque sur un environnement réseau avec un ou pour plusieurs types de SMA de cyber-défense. Cependant, aucun des travaux étudiés ne répond précisément à ce besoin. Sa mise en œuvre prendrait la forme d'un simulateur de réseau sur lequel seraient déployés plusieurs agents d'attaque et défense. Cependant, les simulateurs de réseau du domaine les plus aboutis ne permettent d'avoir qu'un seul agent d'attaque ou de défense là où nous souhaiterions évaluer le passage à l'échelle des SMA de cyber-défense.

Pour répondre à ce besoin, il serait possible d'étendre un modèle générique de réseau pouvant subir une cyber-attaque, tel que dans le simulateur CYST [3], avec la possibilité d'avoir plusieurs agents d'attaque et de cyber-défense. Un tel modèle serait la base d'un simulateur qui permettrait un grand nombre de possibilités expérimentales pour appréhender l'impact de l'organisation des agents de cyber-défense.

B. Traitement des facteurs pour concevoir des organisations

Dans notre contexte, la conception d'une organisation d'un SMA de cyber-défense est un processus prenant en compte les facteurs suivant : les contraintes matérielles et logicielles de l'environnement de déploiement ; les menaces internes du SMA de cyber-défense lui-même ; et les modèles définis d'architecture et d'objectifs de cyber-défense.

Actuellement, il n'existe pas de méthodes ou de processus automatisés visant à trouver un consensus avec ces facteurs lors de la conception d'une organisation. La conception d'un SMA de cyber-défense auto/ré-organisé repose alors sur l'expérience empirique du concepteur en suivant des exigences définies. Une autre approche serait de s'appuyer sur des mécanismes automatisés pour développer une organisation adaptée avec peu d'intervention du concepteur. Une première piste serait le « Distributed Constrained Optimization Problem » (DCOP) où les facteurs d'organisation seraient modélisés par

TABLE I – *Un aperçu de quelques organisations et des environnement hôtes utilisés dans les SMA de cyber-défense étudiés*

Organisation	Avantages principaux	Inconvénients principaux	Environnement	Travaux
Centralisé	Haute précision pour l'analyse de la situation	Single-Point-Of-Failure (SPOF), manque de scalabilité	Petit à moyenne taille, non ouvert, petite entreprise	[4], [5], [18]
Hiérarchique (distribué)	Évolutivité, décomposition des tâches	Perte d'informations, goulots d'étranglement, retards	Taille moyenne à grande, ouvert, peu de variations	[7], [12]
Décentralisé (Peer-to-Peer)	Structure non définie a priori, Hautement adaptatif	Contrôle de l'organisation limitée, intensité de communication	Ouvert, toute taille, fortes variations	[6], [8], [9]
Coalition	Optimisation de l'organisation autour des tâches	Peu adapté sur le long terme	Toute taille, ouvert, peu de variations, peu de ressources	[2]
Équipes	Bonne performance pour des tâches régulières	Haute intensité de communication	Ouvert, hétérogène, toute taille, peu de variations	[1]
Marché	Organisation optimisée par concurrence, bonne gestion des agents	Processus d'allocation complexe et long	Toute taille, ouvert, peu de variations, peu de ressources	[13]

TABLE II – *Un aperçu des fonctions de cyber-défense prises en charge par les SMA de cyber-défense étudiés*

Objectifs principaux	Travaux
R1 : détection d'intrusion, surveillance du réseau, détection de menaces possibles	[1], [4], [5], [7], [12], [18]
R2 : application de contre-mesures, contrôles d'accès, correctifs de cyber-défense, stratégies de cyber-défense	[1], [7], [12]
R3 : investigations forensiques, élaboration de contre-mesures adaptées, apprentissage des cyber-attaques, adaptation aux cyber-attaques	[6], [8], [9], [13]

une fonction de coût que cherchent à minimiser *online* les agents cyber-défenseurs en s'organisant. Une deuxième voie serait le « Multi-Agent Reinforcement Learning » (MARL) où les agents cyber-défenseurs apprennent eux-mêmes les organisations possibles adaptées par rapport à une récompense reçue modélisant les objectifs de cyber-défense.

IV. CONCLUSION

Un SMA de cyber-défense déployé sur un système hôte en réseau permettrait de relever les défis liés à la complexité et la rapidité de cyber-attaques. Notre étude donne un aperçu d'organisations possibles respectant des objectifs de cyber-défense et des contraintes de l'environnement de déploiement d'un SMA de cyber-défense. Elle souligne aussi le besoin de définir un cadre théorique et technique spécifique à l'organisation d'un SMA de cyber-défense dans un environnement réseau. Un tel cadre permettra d'explorer, d'évaluer et de tirer des recommandations sur l'organisation d'un SMA de cyber-défense que nous valoriserons pour le développement d'un agent AICA.

RÉFÉRENCES

[1] S. M. Akandwanaho and I. Govender. A generic self-evolving multi-agent defense approach against cyber attacks. In *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, pages 165–181. IGI Global, 2018.

[2] M. Carvalho and C. Perez. An evolutionary multi-agent approach to anomaly detection and cyber defense. In *7th Annual Workshop on Cyber Security and Information Intelligence Research*, pages 1–1, 2011.

[3] M. Drasar, S. Moskal, S. Yang, and P. Zat'ko. Session-level adversary intent-driven cyberattack simulator. In *2020 IEEE/ACM 24th Int. Symp. on Distributed Simulation and Real Time Applications*, pages 1–9. IEEE, 2020.

[4] E. de la Hoz et al. A distributed, multi-agent approach to reactive network resilience. In *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems*, pages 1044–1053, 2017.

[5] V. Gorodetski, I. Kotenko, and O. Karsaev. Multi-agent technologies for computer network security. *Comput. Syst. Sci. Eng.*, 18(4) :191–200, 2003.

[6] E. M. Holloway. Self organized multi agent swarms (somas) for network security control. *Theses and Dissertations*, 2019.

[7] E. M. Holloway and G. B. Lamont. Self organized multi-agent entangled hierarchies for network security. In *Proc. of the 11th Annual Conference Companion on Genetic and Evolutionary Computation Conference : Late Breaking Papers*, pages 2589–2596, 2009.

[8] J. Haack et. al. Ant-based cyber security. In *2011 Eighth International Conference on Information Technology : New Generations*, pages 918–926. IEEE, 2011.

[9] J. Morteza et al. A method in security of wireless sensor network based on optimized artificial immune system in multi-agent environments. *arXiv preprint arXiv :1508.01706*, 2015.

[10] J.-P. Jamont and M. Occello. Meeting the challenges of decentralised embedded applications using multi-agent systems. international journal of agent-oriented software engineering 5 (1), 22–68, 2015.

[11] A. Kott and P. Théron. Doers, not watchers : Intelligent autonomous agents are a path to cyber resilience. *IEEE Secur. Priv.*, 18(3) :62–66, 2020.

[12] G. B. Lamont and E. M. Holloway. Military network security using self organized multi-agent entangled hierarchies. In *Proc. of the Genetic and Evolutionary Computation Conf.*, pages 2559–2566, 2009.

[13] M. Demir et al. An adaptive multi-agent physical layer security framework for cognitive cyber-physical systems. *arXiv preprint arXiv :2101.02446*, 2021.

[14] G. Picard, J. F. Hübner, O. Boissier, and M.-P. Gleizes. Réorganisation et auto-organisation dans les systèmes multi-agents. In *Journées Francophones sur les Systèmes Multi-Agents*, pages pages–89, 2009.

[15] S. Russell and P. Norvig. A modern, agent-oriented approach to introductory artificial intelligence. *Acm Sigart Bulletin*, 6(2) :24–26, 1995.

[16] P. Theron. Ict resilience as dynamic process and cumulative aptitude. *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, 3 :1–35, 01 2013.

[17] P. Theron, N. Evans, M. Drasar, and A. Guarino. Autonomous Intelligent Cyber Defence Agent Prototype 2021 - Project Report, Dec. 2021.

[18] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer. Taxonomy and survey of collaborative intrusion detection. *ACM Computing Surveys (CSUR)*, 47(4) :1–33, 2015.