Introduction

Genèse / contexte du sujet

- AICA, besoins nouveaux, IoT/IoBT, etc.
- Approche centralisée peu adaptée, etc. pour des raisons d'interruptions de communication, hétérogénéité des SI, etc.
- Une approche MA pourrait être appliquée -> Système Multi-Agents de Cyberdéfense (SMAC)
- Mais sujet nouveau : pas de modélisation, travaux formels…

Problématique générale

- Quelle méthode pour concevoir un SMAC qui atteint ses objectifs de cyberdéfense tout en satisfaisant les contraintes de déploiement et opérationelles du système hôte qu'il doit défendre ?

Positionnement et thèse défendue

- Un ensemble d'agents collaboratifs répond effectivement aux nouveaux besoins, etc. mieux que des solutions centralisées
- Une méthode modélisant le "domaine" (environnement réseau + actions/observations possibles des red/blue/green teams), du "problème" (objectif de cyberdéfense / blue team + contraintes opérationelles/déploiement) sous forme d'un **problème d'optimisation sous-contraintes** ; permet de fournir des moyens objectifs d'évaluer de façon consistante si le SMA tient ses promesses dans plusieurs scénarios d'attaque…

Un aperçu du domaine et du problème

Définitions et propriétés

- Définitions & propriétés fondammentales pour la suite
- cyberdéfense, RL et SMA (+IA hybride éventuellement)
- ex : ouverture, dynamique, auto/réorganisation, explicabilité, etc.

Travaux liés

- Travaux liés à l'AICA et autres SMA de Cyberdéfense
    - SMA : organisation, modèle organisationel...
    - Travaux de l'Autonomous Cyber Operation
    - ...

Limitations et discussion

- Manque de généricité, consistance, pas/peu objectif, peu formel, etc.
- Besoin d’un cadre théorique consistant et générique si possible

Choix du cadre théorique

- Motivation pour : Green, blue, red teams + réseau de noeud avec système d’ataque/contre-attaques d’après les standards de cyberdéfense, reste générique, etc.

Vers une méthode générale

- Motiver les choix préliminaires pour la méthode en mettant en relation les travaux liés de façon cohérente
    - Modèle organisationel et MARL, Cyberdéfense avec MITRE...
- Cela doit permettre au lecteur de comprendre où je veux en venir par la suite...

CybMASFM: Cyberdefense Multi-Agent Systems Formal Model

- **Ici, on cherche à poser les bases pour un modèle qui exprime de façon cohérente et sans-ambiguités/formellement les éléments dont nous avons besoin pour le domaine et le problème**
- **Cela est fondammental pour la suite car l'approche et l'outil se repose sur CybMASFM**

Approches de modélisation pour un SMA de Cyberdéfense

- Modèles partiels (Attack-defense tree, petri nets, etc)
- Modèles de la théorie des jeux (POSG, Dec-POMDP, etc.)

Comparaison et choix du modèle

- Tableau comparatifs, discussion…
- Motivations pour le Dec-PODMP d’après le rapprochement entre incertitude des observations, conditions pour les actions, dynamique de l’env, récompense collective et non individuelle, etc.
- Le Dec-POMDP reste assez générique : plusieurs approche d’organisation / mécanismes / algos d’IA sont envisageable dans ce cadre formel

Modèle formel du domaine

- Montrer comment le cadre théorique non-formel (environnement + teams) peut être formalisé dans le Dec-POMDP
    - Le domaine doit aussi inclure la question de l'organisation dans l'équipe bleu (+ rouge éventuellement)
- Le modèle formel du domaine (i.e le modèle formel de l'environnement et le modèle formel de l'organisation) doit permettre d'exprimer formellement la question de l'organisation comme un problème d'optimisation sous contraintes (i.e de l'environnement et de l'organisation voulue par le concepteur càd ses spécifications)

Modèle de l'environnement

- Montrer comment lier le Dec-POMDP avec les connaissances liées aux attaques (MITRE ATTACK) et où on peut mettre en place des contre-mesures (MITRE DEFEND)
- TODO...

Modèle d'une organisation dans les SMA

- Expliquer comment nous envisageons les organisations possibles au travers de : Conscience/inconscience de l'organisation + Centré agent / organisation.
    - Positionnement par rapport à la littérature
- Expliquer notre vision où une organisation dans un MAS peut être résumée comme : le résultat d'une recherche dans un espace des organisations contraint par les contraintes liées à l'environnement et celles du concepteur (spécifications initiales du concepteur)
- On peut illustrer cela dans les 3 cas ci-dessous
- **Les organisations "totalement prédéfinis"** :
    - Les spécifications initiales du concepteur contraignent totalement le processus de conception à une seule organisation possible
    - 1 seul épisode : chaque agent suit une liste de règles (associant un ensemble d'observation à une action) qui ne changent jamais (sans apprentissage mais basé sur la connaissance/expertise du concepteur) : hiérarchie, mécanisme d'enchère, coalition, etc.
    - Coalition based Multi Agent System AICA (CMASA), Market based Multi Agent System AICA (MMASA), etc.

- **Les organisations "totalement indéfinies"**
    - Les spécifications initiales du concepteur n'ont aucun impact sur la façon dont on peut concevoir les agents (le concepteur humain ou MARL peut choisir librement comment concevoir les règles des agents)
    - Plusieurs épisodes : chaque agent voit ses propres règles changer quand cela maximise la récompense (QLearning, DQN en full automatique ou bien le concepteur humain)
    - Aboutit à une solution local (ensemble de politique) mais pas facilement explicable en MARL (d'où le besoin d'avoir des spécifications en même temps)
    - QLearning based Multi Agent System AICA (QMAS), etc.

- **Les organisation "semi-définies"**
    - Les spécifications initiales du concepteur couvrent partiellement l'espace des organisations possibles

        - Par exemple : trouver des SMA satisfaisant l'architecture hierarchique mais sans savoir précisement quel agent doit adopter quel rôle, etc.
    - Mécanisme d'organisation déjà en place mais les hyper-paramètres doivent être ajustés avec un apprentissage
    - Mix entre agents aux politiques définis et indéfinis
    - D'abord indéfini avec recherche du mécanisme d'organisation défini optimal pour le scénario donné
    - Adaptive Multi Agent System AICA (AMASA) : Une architecture polyvalente pour un SMA de Cyberdéfense, etc.

Expression du problème

Ici, j'utilise les modèles formels précédents pour poser le problème de façon formelle

ici, on ne doit pas encore comprendre que le MARL sera choisi pour la suite en combinaison des modèles d'organisation de SMA comme Moise+

- L'environnement peut être traduit en contraintes qui réduit l'espace des organisations (i.e joint-policy) à celles qui sont réellement possibles (cf. Moise+)
- Les spécifications appliquées à l'OE contraignent également l'espace des organisations (i.e joint-policy) à celles qui sont spécifiées par le concepteur
- Les objectifs de cyberdéfense peuvent être traduits en une fonction à maximiser
- **Problème** : Trouver l'ensemble des politiques (joint-policy) respectant les contraintes telles que sur un épisode, la récompense cumulée des agents bleus soit maximale / supérieur à un seuil
    - Pour une fonction de récompense donnée Rew, les variables inconnues à maximiser sont les politiques PIj (1<j<nb agents): max (Sum{1, .., i, .., nb_it} Rew(PI1, PI2, …, PIn))
    - De plus, la joint-policy obtenue doit être associé à des specifications compréhensibles pour un être humain
        - Design(Env., Specs_init, JointPolicy_init) = (Specs_opt, JointPolicy_opt)
- **Maintenant que l'on a posé le problème il faut le résoudre...**

CybMASDA: Cyberdefense Multi-Agent Systems Developpment Approach

- **Ici, on se positione au niveau du concepteur et du développeur qui veut un résultat tangible à la fin**
- **On propose une approche qui utilise le problème formel décrit précédement pour concevoir l'organisation du MAS en simulation puis on l'implémente réellement en émulation**

Approche de conception théorique combinant MARL et modèle d'organisation de MAS

- Présenter les travaux qui visent à passer des joint-policy du MARL aux spécifications du modèle organisationel Moise+
    - Travaux sur les résultats obtenus en MARL après entrainement pour en extraire les spécifications en Moise+
    - Travaux pour contraindre l'entrainement MARL à respecter des spécifications décrites avec Moise+
- La définition du problème autorise au moins 2 cas différents qui seront présentés sous forme d'exemples :
    - **Spec_Init vide, joint-policy -> Moise+**: Moise+ intervient après l'entrainement en MARL
        - La joint-policy est obtenue après entrainement en MARL (qui inclut implicitement les contraintes de l'environnement) puis il faut faire un travail d'analyse (au moins partiellement automatisable) pour en extraire les spécifications de l'organisation de Moise+
    - **Spec_Init non vide, joint-policy -> Moise+**: Moise+ intervient après et pendant l'entrainement en MARL
        - La joint-policy est obtenue après entrainement en MARL qui doit prendre en compte les contraintes des Spec_Init (en plus des contraintes de l'environnement) puis il faut faire un travail d'analyse (au moins partiellement automatisable) pour en extraire les spécifications de l'organisation de Moise+
- Montrer qu'on peut aussi imaginer d'autres exemples...
    - On a définit "à la main" une joint-policy et on veut savoir les spécifications de l'organisation en Moise+
    - On a des spécifications initiales qui contraignent le MARL à converger vers une seule organisation possible et on veut determiner la joint-policy correspondante
- **L'attendu de cette approche est que le concepteur doit être en mesure de posseder une joint-policy / des joint-policies avec les spécifications de l'organisation associées qui sont suffisament performantes et respectent les contraintes**

Approche de développement basée sur des cycles de simulation et émulation

La simulation pour la conception d'organisation de MAS candidates

- Présentations des travaux correspondant au mieux aux besoins des SMA et de la cyberdéfense
- Comparaison et aboutissement sur l’idée d’étendre l’environnement CybORG du framework PettingZoo (code libre, issu d’un travail de recherche précédent publié à IJCAI, contexte d’application très proche et pertinent, compatibilité avec le modèle Dec-POMDP précédent, etc.)
- L'approche de conception de l'organisation peut être de façon sûre appliquée en simulation car il n'y a pas de risque d'endommager le système cible
- Possibilité de faire du "system identification" pour créer le modèle de simulation et ainsi réduire le gap entre émulation et simulation

    - Cela permettrait de ne pas utiliser CybORG
- + autres avantages de la simulation

L'émulation pour valider un SMAC candidat

- Reproduction du système cible sous une forme émulée (avec container)
- Mise en place d'un dispositif experimental pour transferer les agents de la simulation en émulation
- Validation des SMAC candidats et implémentation dans le système cible

---

CybMASDE: Cyberdefense Multi-Agent Systems Developpment Environment

- Montrer comment CybMASDE peut être utilisé de façon systématique/consistante pour définir un scénario (env, red team, green team) + une blue team (i.e un SMA de cyberdéfense) en définissant soit même les politiques des agents
- Montrer que les modèles de la simulation peuvent être mappés à des modèles émulés afin de verifier la veritable performance des SMA de cyberdéfense proposé AVEC l'intérêt du transfer learning pour l’apprentissage dans la simulation (car rapide et leger) et vérification dans l’émulation (machines virtuelles)

Mise en place d'un modèle AICA

- **Ici l'idée est de créer un modèle AICA integré dans notre méthode et qui pourra être utilisé comme un SMA polyvalent capable d'être ajusté pour des scénarios différents**

Traduction de MASCARA dans CybMASFM

- Traduire au moins dans l'idée les composants de MASCARA comme des spécifications de l'organisations qui seront pris en compte pour generer une organisation dans CybMASDA

Intégration de l'AICA dans CybMASDA et CybMASDE

- Expliquer comment nous avons pris en compte l'AICA dans l'outil afin qu'il soit utilisable directement
- Problématiques d'implémentation dues à la complexité de l'architecture

---

Expérimentation et comparaisons

- Présentation de 3 cas d’études : Drone swarm, company network et Kubernetes
- Sur le modèle du tutoriel en utilisant l'outil CybMASDE

Présentation des études de cas dans CybMASFM

- Montrer comment nous utilisons notre modèle concrètement avec CybMASDE pour comprendre et définir le problème dans chaque étude de cas

Evaluation pour les 3 cas d’étude dans CybMASDA

- Montrer comment nous utilisons CybMASDE pour résoudre le problème
    - En utilisant également le modèle AICA

Synthèse et discussions

- Discuter le niveau de l'impact de la méthode
    - Sans spécifications initiales
    - Avec spécifications initiales (incluant l'AICA)
- Discuter des organisations qui semblent pertinentes avec une analyse quantitative sur les 3 cas d'étude
- Discuter des résultats et la cohérence de ces-derniers par rapport à d'autres résultats

---

Conclusion

- Conclure sur la partie "académique" de la contribution
- Expliquer qu'au delà de répondre à la question de la thèse, la contribution permet aussi de répondre à des problèmes de l'industrie sur la protection de système sur certains aspects

Vers une application industrielle comme aide à la décision

- Simuler des événements qui pourraient arriver et essayer de gagner de l'expérience en prévision du moment où l’attaque sera déjà en cours
- Parler de l'experience de l'approche / outil en industrie avec Thales

Limitations et perspectives

- Evoquer la difficulté du passage à l'échelle
- Le manque de maturité (TRL ne dépasse pas 3/4)
- Travaux connexes sur l'explicabilité au niveau collectif via d'autres approches pas nécéssairement dans la sécurité des réseaux...

Bibliographie