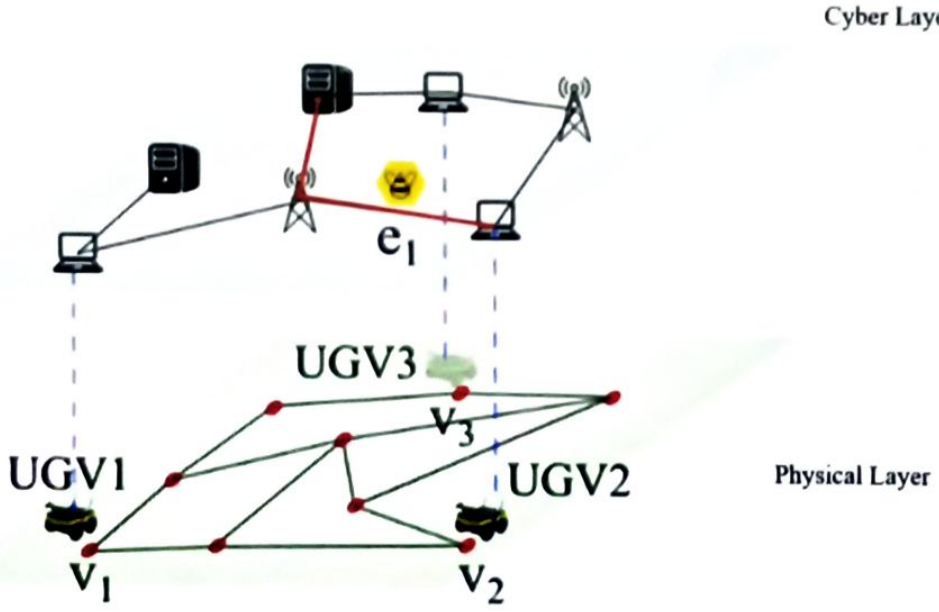
I. DESCRIPTION DU PROJET

Introduction

Deception is used is several conflicts to strategically manipulate the adversary belief, goals, and actions. Cyber deception, such as deploying honeypots, can slow the attacker, waste their time, and detect their intention. Thus, cyber deception has become a crucial strategy for misleading attackers and protecting critical assets in the digital realm. Similarly, physical deception tactics like using decoys and misinformation are used to safeguard valuable resources. Consider a multi-domain cyber psychical system where elements of the physical domain are connected to the elements of the cyber domain and security in one domain affects the other. In such scenarios, when cyber and physical security strategies are designed independently, they often lack coordination, creating vulnerabilities that adversaries can exploit across both domains. The research into single-domain security limitations and the exploration of integrated multi-domain deception and defense strategies seeks to enhance resilience and adaptability in complex security environments.



Objectives

Multi-domain deception aims to bolster the security of cyber-physical systems by designing strategies that can mislead adversaries across various operational domains. The core objective is to develop a comprehensive strategy that synchronizes deceptive tactics across the cyber and physical layer, ensuring these tactics are consistent and mutually reinforcing. This approach is vital for maintaining operational security and preventing adversaries from exploiting weaknesses in any single domain.

Key objectives include:

1. **Joint Optimization Across Multiple Layers**: The primary goal is to achieve a coordinated and optimized deception strategy across all relevant layers of operation. This ensures that the optimum deceptive actions in one domain is dependent on the deception on the other,

and vice-versa. This mean that the deceptive actions cannot be optimized independently across the different domain.

2. **Consistency Across Domains**: It's crucial to maintain a consistent deception narrative across various layers. Inconsistencies or contradictions between deceptive actions in different domains could alert adversaries, thereby reducing the effectiveness of the overall strategy. Deceptive action in one domain should not contradict or undermine those in another, but instead, they reinforce each other to create a more resilient defence mechanism.
3. **Long-Term Multi-Step Consistency**: Deception strategies must remain coherent and effective over time, even as they are implemented through multiple steps or stages. This long-term consistency is essential for sustaining the deception, particularly as adversaries adapt and change their tactics.
4. **Counter-Deception Strategies**: In an adversarial setting, it's essential to consider a multi-domain game setting that also anticipates and counters adversaries' deceptive tactics. Intelligent adversaries can attempt to deceive the adversary. We would like to develop robust counter-deception strategies to ensure that the defense remains effective even when adversaries attempt to mislead or manipulate the system.

Challenges

Implementing effective multi-domain deception presents several significant challenges:

1. **Coordination Across Domains**: One of the biggest challenges is coordinating deceptive strategies across diverse domains, each with its unique characteristics and vulnerabilities. Cyber and physical layers, for instance, require different approaches, yet they must work together seamlessly to ensure the deception is convincing. Moreover, the problem is more than the sum of its parts. The cartesian product of the action spaces in the physical and cyber domains for a player may not accurately capture the multi-domain game, and new actions may have to be considered that handle the interaction between the two domains.
2. **Scalability and Computational Efficiency**: The algorithm to evaluate the player strategies in large scale multi-domain deception games should be efficient. The large number of player actions that arise due to interaction between domains mean that some of the usual game solving methods may be inadequate.
3. **Resource Efficiency**: The deception strategy must be resource-efficient, balancing the benefits of deception with the costs and risks associated with its implementation.

Research Approaches

1. **Game-Theoretic Approaches**:

Game theoretic frameworks are useful to model these multi-domain deception scenarios since it includes adversarial players. Game theory is extensively used to model interactions between defenders and adversaries. By predicting potential adversarial moves and their responses to deception, game theory helps in developing strategies that are more likely to succeed in real-world scenarios. In [1] and [2], a multi-layer game representing a cyber-physical system is presented where a defender must protect a set of resources from an adversary. The defender employs deceptive actions in both the cyber and physical domains. The two domains are

interconnected, and the players' payoffs depend on their actions across both domains.

2. **Double-Oracle and Iterative Algorithms**:

To efficiently solve the complex multi-domain deception problems, advanced algorithms such as double-oracle techniques are utilized such as in [2]. These algorithms iteratively refine the strategy space, focusing on the most relevant strategies, which allows for more targeted and efficient deception.

3. **Machine Learning**:

Machine learning algorithms are increasingly employed to analyze patterns in large datasets, enabling the prediction of adversary behavior and the real-time adaptation of deception strategies [3]. This approach enhances the ability to deploy timely and effective deception tactics.

Research Opportunities

Deceptive defense strategies have been extensively studied at the single-domain level. For example, the use of honeypots in cyber networks—network decoys designed to distract potential attackers from more critical information and systems [4,5]. Honeypots serve to lure attackers away from valuable assets, allowing defenders to study the attackers' methods in real-time and after exploitation.

Similarly, physical deception involves the strategic manipulation of physical environments and assets to mislead adversaries. Tactics include deploying decoy objects, using camouflage, and placing misleading information to create false perceptions about the defender's capabilities, intentions, and critical assets [6,7]. Security games to assign resources efficiently in a physical region to protect against an adversary [8] have also been studied. These games can provide a framework to incorporate deceptive strategies and improve the overall operational security. The approaches, challenges and perspectives for deception in cyber networks are surveyed in [9,10].

Strategies confined to a single domain fail to capture the intricate dynamics of multi-domain scenarios. Traditional single-layer approaches are limited in addressing the complex interplay between cyber and physical domains, which is crucial for a comprehensive understanding of security threats and mitigation strategies. A well-designed cyber security system and an independently designed physical security system may not offer consistent deceptive and defensive strategies across both domains, potentially allowing an attacker to exploit this lack of coordination and launch coordinated attacks on both cyber and physical systems. This limitation underscores the need for a multi-domain model that integrates both cyber and physical layers. By adopting such an approach, defenders can conduct more nuanced simulations and analyses, leading to the development of more sophisticated and effective deception tactics that span both the digital and physical dimensions of their operational environments.

References

1. A.H. Anwar, A. B. Asghar, C. Kamhoua, J. Kleinberg, "A Game Theoretic Framework for Multi Domain Cyber Deception," *IEEE European Symposium on Security and*

Privacy Workshops, 2024.

2. A. B. Asghar, A.H. Anwar, C. Kamhoua, J. Kleinberg, "A Scalable Double-Oracle Algorithm for Multi-Domain Deception Game," *IEEE Conference on Communications and Network Security*, 2024 [to appear].
3. S. McAleer, J. B. Lanier, K. A. Wang, P. Baldi, and R. Fox, "XDO: A double oracle algorithm for extensive-form games," *Advances in Neural Information Processing Systems*, vol. 34, pp. 23128-23139, 2021.
4. A. H. Anwar, C. Kamhoua, and N. Leslie, "A game-theoretic framework for dynamic cyber deception in Internet of Battlefield Things," in *EAI Int'l Conf. on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 522–526, 2019.
5. A. H. Anwar, C. Kamhoua, and N. Leslie, "Honeypot allocation over attack graphs in cyber deception games," in *Int'l Conf. on Computing, Networking and Communications*, pp. 502–506, 2020
6. A. J. Mendez, "A classic case of deception," *Studies in Intelligence, Journal of the American Intelligence Professional*, Winter, vol. 2000, 1999.
7. M. Johnson and J. Meyeraan, "Military deception: Hiding the real-showing the fake," *USAF Joint Forces Staff College, Joint and Combined Warfighting School*, vol. 7, 2003.
8. M. Jain, D. Korzhyk, O. Van˙ek, V. Conitzer, M. P˙echou˙cek, and M. Tambe, "A double oracle algorithm for zero-sum security games on graphs," in *The 10th International Conference on Autonomous Agents and Multiagent Systems*, pp. 327–334, 2011.
9. M. Zhu, A. H. Anwar, Z. Wan, J.-H. Cho, C. A. Kamhoua, and M. P. Singh, "A survey of defensive deception: Approaches using game theory and machine learning," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2460-2493, 2021.
10. A. Alshammari, D. B. Rawat, M. Garuba, C. A. Kamhoua, and L. L. Njilla, "Deception for cyber adversaries: status, challenges, and perspectives," in *Modeling and Design of Secure Internet of Things*, pp. 141-160, Wiley Online Library, 2020.

2. COMITE SCIENTIFIQUE

- Prof. Franklin Tchakounte, University of Ngaoundere, Cameroon
- Prof. Issofa Moyouwou, University of Yaounde 1, Cameroon
- Prof. Blaise Yenke, University of Ngaoundere, Cameroon
- Prof. Bertrand Tchantcho, University of Yaounde 1, Cameroon
- Prof. Louis Aimé Fono, University of Douala, Cameroon
- Prof. Emmanuel Fouotsa, University of Bamenda, Cameroon

3. COLLABORATEURS DE RECHERCHE

- Dr Charles Kamhoua, Seniors Electronics Engineer, US Army Research Laboratory
- Pr Yezekael Hayel, Université d'Avignon
- Pr. Nadjib AIT SAADI, Université de Paris-Saclay

4. CRITERES D'ELIGIBILITE

- Les candidats DOIVENT s'engager à trois ans d'études doctorales à temps plein à Ngaoundéré et ne peuvent pas avoir simultanément d'autre emploi ;
- Les candidats doivent détenir un Master en Sciences (MSc) en Informatique, Mathématiques ou Génie Électrique. Les diplômes en cybersécurité, théorie des jeux et intelligence artificielle (IA) seront un atout. La préférence sera donnée aux candidats ayant déjà obtenu une certification en cybersécurité et IA, ainsi qu'à ceux qui ont (co-)publié dans ce domaine ;
- Les candidats titulaires d'un Master Professionnel NE SONT PAS éligibles ;
- La Bourse Doctorale GAML-MuD^{2}IT sera attribuée aux **candidats de toutes nationalités** ;
- Les candidats doivent effectuer leurs études à l'Université de Ngaoundéré (Cameroun) et commencer durant l'année académique 2024/2025 ;
- **Les candidatures féminines sont fortement encouragées ;**
- Les étudiants déjà inscrits en doctorat ne sont pas éligibles.

5. EXIGENCES DU PROJET

- Être prêt à résider à Ngaoundéré (Cameroun) pendant les trois années de recherche du projet GAML-MuD^{2}IT.
- Être capable de travailler en groupe de recherche, de collaborer avec ses collègues et d'interagir avec des partenaires internationaux au sein du projet GAML-MuD^{2}IT.
- Être disposé à participer activement aux activités de l'École Doctorale.
- S'engager pleinement dans les activités du projet GAML-MuD^{2}IT (séminaires, ateliers, conférences) tout en respectant STRICTEMENT les règles établies.

6. VALEUR DE LA BOURSE DOCTORALE GAML-MuD^{2}IT

La valeur de cette bourse doctorale sera de 3 000 USD par an. Ce montant servira à couvrir uniquement les frais suivants :

- Logement
- Frais de subsistence

D'autres avantages non inclus dans cette valeur :

- Possibilités de financement pour assister à des conférences internationales ;
- Possibilités de cotutelle de thèse avec des universités en France ;
- L'opportunité de travailler avec des chercheurs renommés à travers le monde ;
- Un environnement de travail calme, collaboratif et dynamique.

7. PERIODE DU SUPPORT

- La bourse sera attribuée chaque année pour une durée maximale de trois années académiques. Le boursier est censé terminer le programme doctoral dans le délai minimum requis de trois ans.
- Le renouvellement de la bourse n'est pas garanti et dépend d'un rapport de progression satisfaisant fourni par l'École Doctorale chaque année, confirmant que le boursier peut passer en 2^e ou 3^e année.

- Les étudiants doivent terminer leur doctorat après trois ans. Une demande de prolongation non financée ne sera considérée qu'en cas exceptionnel, et le candidat devra soumettre une motivation écrite appuyée par son directeur de these au responsable du projet.

8. CONDITIONS ET REGLES

Le soutien pour les années suivantes dépendra de :

- La soumission d'un rapport de progression trois mois avant la fin de chaque année d'études ;
- La confirmation par le(s) directeur(s) de thèse que la progression du boursier est satisfaisante, soutenue par des publications de recherche et par le Responsable du département où l'étudiant est inscrit.

9. DATES CLES

- Les candidatures doivent être soumises au plus tard le **31 octobre 2024** à minuit. Les candidatures tardives et incomplètes ne seront pas prises en compte ;
- Les interviews se dérouleront ultérieurement à une date qui sera communiquée à chaque candidat ;
- Le programme commencera en **Novembre 2024**.

10. CRITERES DE SELECTION ET PROCEDURE

L'attribution de cette bourse se fera en fonction de :

- La performance académique antérieure;
- Le potentiel à mener des activités de recherche avancées ;
- Les qualités de leadership;
- Les preuves de réalisations en recherche au niveau du Master, à travers des publications ;
- L'engagement certain à se consacrer pleinement aux trois années de recherche doctorale ;
- La qualité de la proposition en conformité avec le projet ;
- La présentation orale de la proposition de recherche devant un jury.

Le processus de sélection sera conduit par un Comité de Sélection Indépendant mis en place à cet effet, chargé d'éviter tout biais. Ce comité se réserve le droit de modifier, sans préavis aux candidats, les règlements et les conditions de la bourse.

Les entretiens se dérouleront EN LIGNE et SUR SITE A NGAOUNDERE selon un calendrier qui sera communiqué aux candidats.

Le candidat retenu recevra une lettre officielle de confirmation par email. Les candidats qui n'auront pas reçu de notification écrite devront considérer que leur candidature n'a pas été retenue.

NOTE :

Une session d'information en ligne aura lieu le **20 octobre 2024**. Le lien pour y accéder sera bientôt disponible sur le site Web.