REPUBLIQUE DU CAMEROUN
Paix – Travail - Patrie

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR

UNIVERSITE DE NGAOUNDERE

B.P. : 454 Ngaoundéré
Fax./Tél. : (237) 222 254 002
Courriel : un@univ-ndere.cm

RECTORAT

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

MINISTRY OF HIGHER EDUCATION

THE UNIVERSITY OF NGAOUNDERE

P.O. Box: 454 Ngaoundéré
Fax./Tél.: (237) 222 254 002
E-mail : un@univ-ndere.cm

RECTOR'S OFFICE

Ref. ____________/UN/R/VR-EPDTIC/FS/DMI/ Ngaoundéré,

ANNOUNCEMENT

Project GAML-MuD^{2}IT : Call for applications for PhD candidates in Cybersecurity

As part of the project "**Game Theory and Machine Learning for Multi Domain Deception in Internet of Things** (GAML-MuD^{2}IT)," funded by **DEVCOM Army Research Laboratory** (ARL) and the **Office of Naval Research (ONR)-Global USA**, the Rector of the University of Ngaoundéré is pleased to announce, following approval from the Minister of State, Minister of Higher Education, that a call for applications is open until **October 31, 2024**, for the selection of eighteen (18) PhD researchers in advanced cybersecurity topics.

Application Submission

- A pre-registration form, downloadable at https://fs.univ-ndere.cm/doctorat-phd/, duly filled;
- A research project of no more than 5 pages, related to the GAML-MuD^{2}IT project, including the context, SMART objectives (specific, measurable, attainable, relevant, and time-bound), research methodology, expected results, and outcomes/impact;
- A stamped letter of motivation;
- 04 photos (4×4) taken within the last three months, with the candidate's name written on the back;
- Two certified true copies of the birth certificate, issued within the last 3 months;
- An updated and signed CV, highlighting relevant competencies;
- Certified copies of diplomas starting from the Baccalaureate or GCE AL or equivalent;
- The transcript from the degree cycle qualifying for the selection;
- An CCA BANK receipt showing payment of 10,000 CFA for pre-registration fees to the account (**Nº CM21 10039 10013 02373363601-57**);
- A non-refundable payment receipt for the sum of 15,000 CFA representing the application processing fee to the CCA Bank account **No. CM21 10039 10013 02373355702-86**.
- A 32 cm x 23 cm stamped envelope with the candidate's address;
- The complete physical application file must be submitted to the Faculty of Sciences' registry at the University of Ngaoundéré before the closing date;
- The complete file compiled in a PDF document may be submitted online at https://cybersecurity.univ-ndere.cm/ and via email to cybersecurity@univ-ndere.cm (copy to cyberdeception.at.univ.ngaoundere@gmail.com) with the subject: "PhD in GAML-MuD2IT – *Topic Chosen*."

Important Notes:

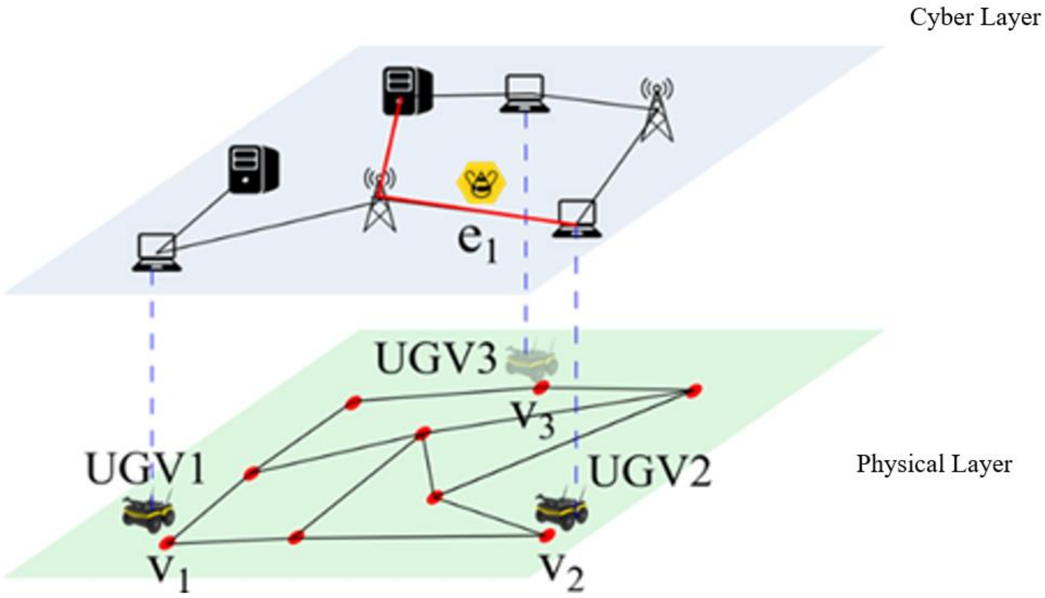
- This call is open to applicants from Cameroon and other nationalities who wish to pursue their PhD research at the **University of Ngaoundéré**, Cameroon;
- The research proposal must be written in **English and French** and presented to a pre-selection committee;
- The candidate should apply in one of the topics described at https://cybersecurity-univ-ndere.cm/ and should take into account the project objectives;
- Applicants who hold a Professional Master are not eligible;
- The deadline for submission is **October 31, 2024**;
- The interviews will take place afterwards at a date that will be announced to the candidates;
- **Female candidates** are highly encouraged to apply;
- Selected candidates must:
    - Submit a registration file for the PhD program at the Faculty of Sciences, including the documents listed at https://fs.univ-ndere.cm/doctorat-phd/;
    - Participate in the scientific activities of the **Doctoral Training Unit Mathematics, Computer Science, Engineering and Applications (M2IAP) of the Doctoral School Sciences, Technology and Engineering (STI)**;
    - Provide **medical insurance** (ONLY for international candidates);
    - Commit to **three years of full-time doctoral studies** in Ngaoundéré starting from the academic year 2024/2025, with no other concurrent employment;
    - Receive a **monthly stipend** to cover living expenses, with potential **financial support** for attending international conferences (for advanced candidates), and some may be included in **co-supervised doctoral programs**.

For more information about the project, please email to cybersecurity@univ-ndere.cm

1. PROJECT DESCRIPTION

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 his 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. Vanˇek, V. Conitzer, M. Pˇechouˇcek, 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. SCIENTIFIC TEAM

- Prof. Franklin Tchakounte, University of Ngaoundere, Cameroon (**Principal Investigator**)
- 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. RESEARCH COLLABORATORS

- Dr. Charles Kamhoua, Seniors Electronics Engineer, US Army Research Laboratory
- Pr. Yezekael Hayel, University of Avignon
- Pr. Nadjib AIT SAADI, University of Paris-Saclay

4. ELIGIBILITY

- Applicants MUST BE dedicated to three years of full time PhD study in Ngaoundere and cannot hold any other employment;

- Applicants must hold a Master’s of Science degree in Computer Science, Mathematics, or Electrical Engineering. Degrees related to cybersecurity, game theory, and artificial intelligence (AI) will be a plus. Preference will be given to candidates who have already obtained a certification in cybersecurity and AI, and to those who have (co-)published in this domain.
- Applicants who hold a Professional Master are NOT eligible.
- The GAML-MuD^{2}IT Doctoral Scholarship will be awarded to applicants of all nationalities.
- Applicants must conduct their studies at the University of Ngaoundere (Cameroon) and commence in the academic year 2024/2025;
- **Female candidates are highly encouraged to apply;**
- Ph.D students currently registered are not eligible to apply;

5. PROJECT REQUIREMENTS

- Be willing to relocate and reside in Ngaoundere (Cameroon) during the three years **GAML-MuD^{2}IT** research period;
- Be able to work in research groups, to collaborate with peers and to interact with international collaborators within **GAML-MuD^{2}IT;**
- **Be willing to actively participate to the activities of the Doctoral School;**
- Be fully engaged in the **GAML-MuD^{2}IT** activities (seminars, workshops, conferences.) while STRICTLY respecting regulation terms;

6. VALUE OF GAML-MuD^{2}IT DOCTORAL SCHOLARSHIP

The value of this Doctoral Scholarship will be 3.000 USD p.a. This amount will be used to cover the following charges:

- Accommodation;
- Living expenses.

Some other advantages that are not included in this value:

- Possibilities for international conference attendance allowance;
- Possibilities for PhD Cotutele with universities in France
- The opportunity to work with renowned research collaborators across the world;
- A quiet place to work in a collaborative and dynamic research environment.

7. PERIOD OF SUPPORT

- The scholarship funding will be awarded yearly for a maximum period of three academic years. The fellow is expected to complete the Doctoral programme within the minimum required period of three academic years.
- Renewal of the award is not guaranteed and is subject to a satisfactory progress indicator been uploaded by the Doctoral School each year indicating that the fellow can continue to the 2nd year or 3rd year.

- Students are expected to complete their PhD after three years. An unfunded extension request will only be considered under exceptional cases, the incumbent must submit a written motivation supported by the supervisor to the project leader.

8. TERMS AND CONDITIONS

Support for the subsequent years will be subject to:

- Submission of a Progress Report three months before the end of each year of study;
- Confirmation by the Supervisor(s) that the scholar's progress is satisfactory and supported by research publications and by the Head of Department in which the student is registered.

9. KEY DATES

- Student proposal due **October 31, 2024**. Late and incomplete applications will not be considered.
- The interviews will take place afterwards at a date that will be announced to the candidates;
- The program will start in **November 2024**.

10. SELECTION CRITERIA AND PROCEDURE

Award of this scholarship will be based on:

- Previous academic performance;
- Potential to undertake advanced research activities;
- Leadership qualities;
- Evidence of research accomplishment at the Masters' level by means of publications;
- Certitude for fully dedication during three years of the PhD research;
- Quality of proposal in conformity with the project.
- Oral presentation of the research proposal to a selection committee.

The selection process will be conducted by an **Independent Selection Committee** put in place for this purpose, responsible to avoid biases. This committee reserves the right to amend, without prior notice to the Applicants, the regulations and scholarship values and/or conditions applicable to the awarding of this scholarship.

Interviews will be organized ONLINE and ONSITE (IN NGAOUNDERE) following a schedule that will be appropriately released to the candidates.

The successful Applicant will be sent an official award letter via-email. Applicants, who have not received written notification should consider themselves unsuccessful.

NOTE:

There will be an online information session on **October 20, 2024** at a link that will be released on the website soon.