Announcement

GMC-DRA project: Call for proposal for the Selection of PhD students for research in cyber-security

Within the framework of the research project "Game Theory and Machine Learning for Cyber Deception, Resilience and Agility (GMC-DRA)" funded by the US Army Research Laboratory, within URIFIA (Fundamental Computer Science, Engineering and Application Research Unit) of the Department of Mathematics and Computer Science (DMI), The Dean of the Faculty of Science (FS) of the University of Dschang (UDs) is launching a special call for the selection of fifteen (15) researchers wishing to continue their PhD research on the topic of cyber-security.

How to Apply:
- Submit an application file for registration into Year 1 according to the current criteria at the UDs Doctoral School; or be regularly registered in PhD Year 1 or PhD Year 2 at UDs (in the latter case, having produced a high-level article on the same topic is a plus);
- Provide legalized copies of all university transcripts and certificates of achievement of graduate levels; the candidate must have obtained an average greater than 12/20 in Master 1, Master 2 and possibly in PhD 1;
- Provide an updated and signed CV, highlighting the candidate's strengths;
- Provide a 5 pages research proposal written in English to be presented in English with PPT, in front of the preselection jury;
- Send a letter of motivation to the Dean of the Faculty of Science.
- The full application package in WORD or PDF should be submitted by email at <dept.math-info@univ-dschang.org> with cc to <marcellin.nkenilfack@gmail.com>

The email subject should be "PhD in Cyber Security".

Note:
- This PhD call for admission is open to the best candidates from Universities in Cameroon and abroad wishing to pursue a PhD at the University of Dschang;
- Applicants should be able to write and speak English fluently;
- The deadline for submitting applications is 12 September 2021; research presentation will be scheduled right after;
- Applicants should ensure that they have carefully read the information contained in this announcement beforehand;
- The selected candidates will participate in all specialized seminars in the field, within the URIFIA of DMI;
- Selected candidates must be fully dedicated to their PhD research for 3 years and not be involved in any other activities. They will receive a monthly stipend to cover their living expense;
- Selected candidates will receive financial assistance for participation in top-tier international conferences;
- A few PhD co-tutele will be supported under this project;
- Application from women and underrepresented group in cyber security is highly encouraged.

The Dean
Faculty of Science

Ngameni Emmanuel
professeur
Project Description

Cyber security is a serious concern to our economic prosperity and national security. Despite an increased investment in cyber defense, cyber-attackers are becoming more creative and sophisticated. Moreover, the scope and repercussions of cyber-attacks has increased over time. This exposes the need for a more rigorous approach to cyber security, including methods from artificial intelligence including game theory and machine learning. Using a game theoretic approach to cyber security is promising; however, one has to deal with many types of uncertainty such as incomplete information, imperfect information, imperfect monitoring, partial observation, limited rationality, and the computational complexity of finding equilibrium or optimum policies. On the other hand, artificial intelligence (AI) algorithms have typically been designed to optimize in a random stochastic environment. Recent advances in adversarial machine learning are promising to make AI algorithms more robust to deception and intelligent manipulation. However, they are still vulnerable to adversarial inputs, data poisoning, model stealing and evasion attacks. The above challenges and the high risk and consequence of cyber-attacks drive the need to accelerate basic research on cyber security.

The technical approaches on this project focuses on two primary areas of AI that are especially promising and relevant for cyber security: game theory and machine learning. These areas overlap to some extent, but game theory focuses more on decision making in adversarial settings, while machine learning focuses more on using large data sets for prediction and adaptation. We are also interested on a proactive cyber defense highlighting cyber deception, cyber resilience, and cyber agility or moving target defense.

Cyber deception is any attempt to disguise a network and impair the attacker’s decision with false information to protect critical nodes. Deception can delay a cyber-attack by increasing uncertainty. Deception also forces the attacker to perform more trial and error in the reconnaissance phase which increases the probability of intruder detection. The use of honeypots is a basic form of cyber deception used to create the appearance of important targets to the attacker. Honeypots also help to identify attackers and provide a means to learn about their behaviors in a safe environment. The attacker’s strategies learned via the use of honeypots aid in securing critical components. A honeynet is a decoy network that contains one or more honeypots. Valuable deception techniques must confuse the attacker while being transparent to the defender and legitimate users. Advanced deception techniques can dynamically hide or create fake vulnerabilities, data, protocols, communication links, hardware, software and applications. However, given enough time, an attacker may be able to discover the defender’s deception strategy. Therefore, a sophisticated cyber deception technique is most often combined with cyber agility.

Cyber agility or moving target defense is the dynamic reconfiguration of network parameters, components, topology, and protocols to oppose an attacker’s ability to collect information about the system. A static configuration gives enough time to attackers to learn about the system and identify potential vulnerabilities or exploits in the reconnaissance phase. An agility strategy randomly changes the attack surface and network pattern faster than an attacker can learn.

Cyber resilience refers to the network capability to continuously maintain mission essential functions after a cyber-attack. As information systems become ever more complex and the interdependence of these systems increases, defending our network becomes more and more critical. Unfortunately, it is not always possible to anticipate every type of component failure and cyber-attack within a large information system. Therefore, a mission-critical system placed in cyberspace should be resilient and have the fight-through ability to sustain damage yet survive and recover with mission assurance.

We encourage PhD proposal submission on research topic related to the following topics of interest (suggestive but not exhaustive, not in any order):

5. Epidemic model against cyber deception [17] - [18]
7. AI for cyber deception [21]
8. Intelligent and rapid honeynet generation [22] - [23]
9. Design of high interaction honeypot [24]
11. Location deception
12. Autonomous cyber security [27], [28]
13. Behavioral game theory for security [29] - [31], [58]
14. Planning and stochastic games for security [32] - [34]
15. Hypergames for cyber security [35] - [38]
16. Uncertainty and robustness for security [39], [59]
17. Proactive cyber defense [40] - [44]
19. Anomaly detection [46] - [47]
21. Internet of Things (IoT) and Cyber Physical System (CPS) security [25], [41], [51]
22. Cyber resilience [52] - [55]
23. Novel methods to combine complementary techniques for cyber resiliency, such as game theory and machine learning [1], [6]
24. Development of agents that are doers, not just watchers: autonomy and intelligence for rapid response to a compromise and rapid recovery that aids resilience of system [56] - [57]
25. Knowledge based planning of implementation of an autonomous intelligent cyber defense agent [27] - [28]
26. Adaptive learning, development of a structured world-model, and mechanism for dealing with explicitly defined, multiple and potentially conflicting goals.

A successful proposal should address the following questions well known as DARPA Heilmeier question:
- What are you trying to do? Articulate your objectives using absolutely no jargon.
- How is it done today, and what are the limits of current practice?
- What is new in your approach and why do you think it will be successful?
- Who cares? If you are successful, what difference will it make?
- What are the risks?
- How long will it take?
- What are the mid-term and final “exams” to check for success?

Research Team:
- Pr Marcellin Nkenlifack, Head of Department of Math and Computer Science, University of Dschang
- Pr Gabriel Deugoue, Associate Professor, University of Dschang
- Dr Vianney Kengne Tchendji, Assistant Professor, University of Dschang
- Dr Elie Fute Tagne, Assistant Professor, University of Dschang
- Dr Jean Pierre Liemou Tchawc, Assistant Professor, University of Dschang

Research Collaborators:
- Dr Charles Kamhoua, Senior Electronics Engineer, US Army Research Laboratory
- Dr Frederica Nelson, Senior Computer Scientist, US Army Research Laboratory
- Dr Jaime Acosta, Senior Computer Scientist, US Army Research Laboratory
- Dr Ahmed Hemida, Postdoctoral Fellow, US Army Research Laboratory
- Dr Laurent Njilin, Research Electronics Engineer, US Air Force Research Laboratory
- Pr Yezekael Harel, University of Avignon
- Pr Sachin Shetty, Professor, Old Dominion University
- Pr Danda Rawat, Professor, Howard University
- Pr Christophe Bobda, Professor, University of Florida
- Dr Deepak Tosh, Assistant Professor, University of Texas El Paso

References


18) Olivier Tsmogine, Yezekeal Hayel, Charles A. Kamhoua, Gabriel Detouge “Partially Observable Stochastic Games for Cyber Deception against Network Epidemic” in the proceedings of the Conference on Decision and Game Theory (GameSec 2020), College Park, USA, October 2020.


Communiqué

Projet GMC-DRA : Appel à candidatures pour la Sélection de Doctorants pour les recherches avancées en cyber-sécurité

Dans le cadre du projet de recherche « Game Theory and Machine Learning for Cyber Deception, Resilience and Agility (GMC-DRA) » financé par l'US Army Research Laboratory, au sein de l'URIFIA (Unité de Recherche en Informatique Fondamentale, Ingénierie et Applications) du Département de Mathématiques et Informatique (DMI), le Doyen de la Faculté des Sciences (FS) de l'Université de Dschang (UDS) lance un appel à candidatures pour la sélection de quinze (15) chercheurs désireux de poursuivre leurs travaux de recherche en Doctorat/PhD sur cette thématique de la cyber-sécurité.

Conditions de candidature :
- Déposer un dossier de candidature pour l'inscription en première année de Doctorat (D1) selon les critères en vigueur à l'école doctorale de l'UDS ; ou être régulièrement inscrit en D1 ou en D2 à l'UDS (dans ce dernier cas, avoir produit un article de haut niveau dans la même thématique est un atout considérable) ;
- Fournir des copies légalisées des relevés de notes et attestations de réussite des niveaux universitaires ; le candidat doit avoir obtenu plus de 12/20 de moyenne en Master 1, en Master 2 et éventuellement en D1 ;
- Fournir un CV actualisé et signé, mettant en évidence les points forts du candidat ;
- Fournir une synthèse du projet/proposition de recherche sur 5 pages rédigées en Anglais à présenter en Anglais (avec PPT), devant le jury de présélection ;
- Adresser une lettre de motivation à Monsieur le Doyen de la Faculté des Sciences ;
- Le dossier de candidature complet au format WORD ou PDF doit être soumis par courrier électronique à l'adresse <dept.math-info@univ-dschang.org> avec cc à <marcellin.nkenlifack@gmail.com>.

L'objet de l'e-mail doit être « PhD in Cyber Security ».

NB:
- Cet appel à candidatures est ouvert aux meilleurs candidats des Universités du Cameroun et de l'étranger désirant poursuivre en cycle de Doctorat/PhD à l'Université de Dschang ;
- Les candidats doivent être capables d'écrire et de parler couramment l'anglais ;
- La date limite de dépôt des candidatures est le 12 septembre 2021 ; la présentation des projets de recherche sera programmée juste après ;
- Les candidats doivent s'assurer d'avoir lu attentivement les informations contenues dans cette annonce au préalable ;
- Les candidats retenus participeront à tous les séminaires spécialisés dans le domaine, au sein de l'URIFIA du DMI ;
- Les candidats sélectionnés seront entièrement dédiés à leur recherche doctorale pendant 3 ans et ne peuvent donc pas être impliqués dans d'autres activités (les travailleurs sont exclus). Ils recevront une allocation mensuelle pour couvrir leurs frais de subsistance ;
- Les candidats sélectionnés recevront également une aide financière pour participer à des conférences internationales de haut niveau ;
- Un certain nombre de cotutelles doctorales seront soutenues dans le cadre de ce projet ;
- Les candidatures de femmes et de groupes sous-représentés dans le domaine de la cybersécurité sont fortement encouragées.