**Canevas du cahier des charges relatif à un projet de fin d’études de l’ERA**

|  |  |
| --- | --- |
| Encadrants : | Cne Tariq MOUATASSIM |
| GSM : | 0707015499 |
| Email : | tariqmouatassim@gmail.com |

1. Intitulé du sujet du projet :

**Conception d’un Système intelligent pour la détection d’intrusion au sein des drones.**

1. Présentation du sujet

L'utilisation des drones grand public dans les armées du monde est devenue de plus en plus courante, principalement en raison de l'accessibilité et de la polyvalence de ces dispositifs. En effet, ces drones peuvent être utilisés à des fins de surveillance pour observer des zones d'intérêt, notamment dans le cadre de missions de recherche et de sauvetage, de surveillance des frontières, de lutte contre la contrebande ou de surveillance des installations militaires. Ils peuvent servir également de relais de communication pour établir des liaisons de communication dans des zones où les infrastructures de communication sont détruites ou indisponibles. De surcroît, ils peuvent être équipés d'armes légères pour fournir un appui aérien rapproché aux troupes au sol.

Cependant, ces dispositifs sont vulnérables par défaut aux attaques les plus élémentaires, du fait qu’ils sont conçus pour être faciles à utiliser, abordables et accessibles au grand public. Ainsi, ils ne sont pas équipés de fonctionnalités de sécurité avancées, telles que des systèmes de détection d'obstacles sophistiqués ou des mécanismes de détection et de prévention des intrusions.

Donc, il devient nécessaire, pour les armées qui envisagent de mettre à profit ces nouveaux dispositifs, de les sécuriser avant de les utiliser.

1. Objectifs :

Le présent projet se fixe comme objectif de développer un système capable de détecter les intrusions au sein d’un système drone UAS ‘Unmanned Aerial System’ par l’utilisation des algorithmes de Machine Learning. Ce système sera utilisé pour sécuriser des drones grand public, ou commerciaux, qui pourront être employés par nos forces.

1. Apport pour :

* Les FRA
  + Doter les drones grand public, susceptibles d’être employés par les FRA, d’une solution intelligente de détection des intrusions;
  + Développer les capacités défensives en matière de protection des drones contre les acteurs malveillants ;
  + Développer une expertise dans le domaine la sécurisation des drones qui peut servir lors des projets de réalisation de nos propres drones.
* L’ERA
  + Disposer d’une solution technique pour sécuriser les drones en dotation utilisés à des fins pédagogiques durant les projets de fin d’étude.
* Les stagiaires
  + Développer une expertise dans le domaine de la cybersécurité appliquée aux systèmes drones ;
  + Mettre en application les acquis en matière de gestion de projet, de réseau informatique, intelligence artificielle…

1. Description et détails techniques

Après l’assimilation de la problématique, le stagiaire est appelé à effectuer une recherche bibliographique détaillée pour d’une part, comprendre les attaques drones et les mécanismes de détection d’intrusion au sein d’un UAS (type d’intrusion, mode de déploiement du système…), et d’autre part de maîtriser les outils de Machine Learning, le processus d’entraînement des modèles et de validation des résultats.

Le stagiaire utilisera un jeu de données ‘Dataset’ adéquat pour l’entraînement des modèles de détection d’intrusion. En fonction des ressources disponibles, ce Dataset sera ou bien choisi parmi les datasets de détection d’intrusion disponibles sur Internet, ou encore conçu en concertation avec les stagiaires des projets similaires. Le choix du Dataset, étant une étape cruciale, doit s’effectuer d’une manière logique et raisonnable et prendre en considération les spécificités des systèmes drones (nature du trafic réseau, protocoles de communication spécifiques…).

Le stagiaire doit effectuer un prétraitement sur le Dataset choisi pour s’affranchir des problèmes éventuelles qui peuvent impacter les performances du système, tels que l’équilibrage des classes pour remédier aux problèmes de sur-apprentissage, et la réduction des attributs pour faire face à la restriction des ressources de calcul dans un système drone.

Le stagiaire choisira les algorithmes de Machine Learning parmi ceux qui sont déjà implémentés dans des librairies python disponibles sur internet, tout en justifiant son choix.

Par la suite, il procédera à l’entraînement de ces modèles de détection d’intrusion sur une partie du Dataset choisi, et évaluera leurs performances sur l’autre partie en utilisant la matrice de confusion et les différentes métriques possibles (précision, exactitude…).

La dernière phase consiste à optimiser les résultats obtenus en recourant à des différentes techniques (Grid Search, l’optimisation bayésienne…). Finalement, une étude de faisabilité doit être conduite pour discuter de l’implémentation de la solution.

1. Ressources nécessaires :

* Une station de travail performante ;
* Navigateur Anaconda (Jupiter notebook…) ;
* Kit Pixhawk ;
* Tello EDU UAV

De plus, le stagiaire doit avoir des connaissances en programmation en langage python, et des notions en cybersécurité.

1. Etapes et déroulement

Phase I : Assimilation de la problématique

Phase II : Préparation de la solution

1. Choix ou conception du Dataset ;
2. Prétraitement du Dataset ;
3. Choix des algorithmes de Machine Learning.

Phase III : Entraînement et évaluation des modèles

1. Choix des métriques de performances ;
2. Entraînement des modèles ;
3. Evaluation des performances

Phase IV : Optimisation de la solution et étude de l’implémentation

1. Choix de la méthode d’optimisation des hyper paramètres
2. Application de la méthode et évaluation des résultats
3. Etude de la faisabilité d’implémentation de la solution.