OFFRE DE STAGE :

Recherche d'attaques de sûreté de fonctionnement et de cybersécurité d'une application de robots mobiles coopératifs

Lieu : Clermont Ferrand

Finalité : Besoin Client -LPA i-SMART

Responsable Equipe /Tuteur	Durée envisagée	Référence
D DENIS	6 mois	ST 2024 – DD 4

Présentation de l'entreprise

Acteur de la conception de systèmes complexes depuis **plus de 25 ans**, SHERPA Engineering met au service de ses clients ses compétences en **Ingénierie système** et en **modélisation** pour la conception et la validation de systèmes techniques dans les domaines industriels de l'automobile, de l'aéronautique, de l'énergie, du naval, du militaire et du spatial.

Nos activités sont concentrées dans 4 grands domaines :

- Les systèmes énergétiques
- Les ADAS et véhicules autonomes
- L'ingénierie des systèmes
- La modélisation multiphysique et le contrôle-commande

Welcome to the Jungle

Pour renforcer nos activités à l'international avec l'Europe dans les secteurs de l'automobile et de l'aéronautique et aussi accroître notre développement à l'international, nous nous sommes également implantés en Roumanie (SHERPA Roumanie), au Maroc (NOMADE Engineering) et en Tunisie (SHERPA MENA).

Nos politiques sociétale, RH & RSE

Mettant la qualité de nos études en avant au même titre que les aspects RSE, SHERPA Engineering est reconnu par la **qualité** de ses études (ISO9001, Awards Safran…) et son **engagement sociétal** et **environnemental** (Lucie 26000, Ecovadis)

333 Avenue Georges Clemenceau,
92000 NANTERRE
Tél : (33) 1 47 82 08 23
www.sherpa-eng.com

Recherche d'attaques de sûreté de fonctionnement et de cybersécurité d'une application de robots mobiles coopératifs

Lieu : Clermont Ferrand

Finalité : Besoin Client -LPA i-SMART

Contexte

Plusieurs études ont montré que la robotique pourrait être un réel tremplin vers l'émergence d'une agroécologie, soit une agriculture productrice beaucoup plus respectueuse de l'environnement.
C'est dans cet ordre d'idées que SHERPA Engineering et l'INRAE-TSCF se sont associés dans un cadre de recherche public-privé pour créer le Laboratoire Partenarial Associé (LPA), i-SMART dont l'objectif est le développement de méthodes et d'outils innovants et durables pour la robotique agricole et la navigation autonome en milieux tout-terrain.

Description

L'objectif du stage est de développer un système évaluant la robustesse d'une application agricole dans un champ utilisant deux robots travaillant en coopération face à des attaques/intrusions liées aux aspects de cybersécurité et de sûreté de fonctionnement. Les robots agricoles sont équipés de différents capteurs proprioceptifs (IMU, Encodeurs de roues…), extéroceptifs (Lidar, GPS, …) et d'une connexion 4G/WIFI assurant la communication entre les engins autonomes. Le robot *follower* communique avec le *leader* afin de récupérer sa position sur la trajectoire et ainsi contrôler sa vitesse pour maintenir une distance constante entre eux.
Aussi, ils se coordonnent pour effectuer le demi-tour l'un après l'autre afin d'éviter toute éventuelle collision pendant la manœuvre.
Concrètement, il s'agira de réaliser des tests d'attaque/intrusion dans l'application robotique agricole décrite ci-dessus sur trois volets avec pour objectif de vérifier les propriétés de sécurité que le système doit valider.

1- Communication du GPS RTK
Il s'agit d'une communication entre le GPS du robot et un autre GPS qui fait office de station de référence.
Les propriétés de sécurité à valider sont:
- Authenticité de la station GNSS: le robot doit pouvoir s'assurer que le destinataire correspond bien à la station de référence
- Intégrité: les corrections GNSS ne doivent pas être altérées. L'injection de données conformes mais malveillantes pourrait perturber l'estimation de position du GNSS du robot
- Disponibilité : les données doivent être accessibles en permanence. Sans les données de correction GNSS, le robot serait contraint de s'arrêter ou d'utiliser une autre méthode pour se localiser

2- Communication interne du robot
Les robots sont équipés d'un ordinateur faisant tourner un ensemble de programmes ayant chacun une tâche spécifique. La communication entre ces programmes se fait grâce à l'utilisation d'un outil logiciel nommé ROS (Robot Operating System) qui assure le transport de messages par un système de *publisher /subscriber* basé sur de la communication TCP ou UDP.

En considérant qu'un attaquant ait accès au réseau interne du robot, l'objectif serait de s'assurer que l'agent intrusif ne puisse pas prendre le contrôle du robot.

A cet effet, la liste de propriétés de sécurité que le système doit valider est la suivante :
- Confidentialité : certains messages ne doivent pas être lisibles (ex: les images caméra, la position GNSS du robot).
- Authenticité : l'attaquant ne doit pas pouvoir se faire passer pour un envoyeur ou un destinataire.

333 Avenue Georges Clemenceau,
92000 NANTERRE
Tél : (33) 1 47 82 08 23
www.sherpa-eng.com

- Intégrité : les messages ne doivent pas être corrompus.
- Disponibilité : l'interruption de certains messages peuvent bloquer le fonctionnement du robot.

3- Mesure de distance par émetteur UWB

L'UWB (ultra wideband) est une technologie de communication radio qui a la particularité d'émettre des impulsions sur une large bande de fréquence. Il offre ainsi la possibilité d'effectuer des mesures de distance avec une précision centimétrique entre deux émetteurs. En plaçant plusieurs balises UWB dans l'environnement et sur le robot, il est alors possible de localiser ce dernier par trilatération. Un attaquant pourrait interférer sur la communication entre les balises UWB et potentiellement contrôler la position du robot. Voici une liste de propriétés de sécurité que le système doit valider :

- Authenticité : le robot doit éviter de communiquer avec des balises non reconnues.
- Intégrité : la mesure de distance entre deux balises ne doit pas être altérée par un attaquant

Résultats Attendus :

.

Un système d'évaluation des aspects de sûreté de fonctionnement et de cybersécurité des applications robotiques

Profil recherché	Compétences requises
Stage dernière année Cycle Ingénieur BAC +5 ou Master 2 dans une filière en cybersécurité ou en informatique robotique	Bonne capacité en programmation en C++ Bonne maitrise de GIT ou GITLAB Des connaissances de ROS, en particulier ROS2 et également en communication radio seraient un plus. Aptitude à travailler de manière autonome et en équipe avec une bonne capacité à communiquer. Bon niveau d'anglais

Plus de détails
Ce stage est rémunéré à hauteur de 850 € brut / mois Tickets restaurant Prise en charge de 50% des frais de transport Vous évoluerez dans un environnement de travail convivial et dynamique, vous serez formé en continu par des experts de l'entreprise.

Si cette offre ne vous correspond pas, n'hésitez pas à produire une candidature spontanée dans la rubrique nous rejoindre de notre site internet, nous l'étudierons en détail pour mettre à profit vos compétences et répondre à vos besoins.

333 Avenue Georges Clemenceau,
92000 NANTERRE
Tél : (33) 1 47 82 08 23
www.sherpa-eng.com