Soutenance de thèse

Ruohao ZHANG soutiendra sa thèse de doctorat, préparée au sein du laboratoire ENAC et intitulée «*Détection d'intrusion dans une flotte de drones*»

Le 18 janvier 2022 à 10h00, salle des thèses ISAE-SUPAERO

devant le jury composé de

M. Jean-Philippe CONDOMINES	Professeur ENAC	Co Directeur de thèse
M .Julien BOURGEOIS	Professeur Université Bourgogne Franche Comté	Rapporteur
M. Promethee SPATHIS	Maître conférences Sorbonne Université	Rapporteur
M. Jérôme LACAN	Professeur ISAE-SUPAERO	
M. Yann LABIT	Professeur Université Toulouse 3	
M. Pierre-Ugo TOURNOUX	Maître de conférences Université de la Réunion	

Résumé : Ces dernières années, le développement du système aérien sans pilote (UAS) impliquant des essaims de véhicules aériens sans pilote (UAV) a connu des progrès sans précédent. Cependant, les systèmes de réseau mis en œuvre dans les UAS commerciaux actuels sont souvent des variantes des systèmes de réseau existants. Ainsi, des vulnérabilités préexistantes peuvent persister, tandis que de nouvelles vulnérabilités émergeant des nouvelles propriétés des UAS, telles que la mobilité et l'interconnectivité, sont encore plus préoccupantes. Étant donné que les UAS opèrent dans l'espace aérien civil, la sûreté et la sécurité sont essentielles.

Cette thèse a été créée en réponse à une demande croissante. Dans ce rapport de thèse, trois stratégies sont explorées pour chercher à résoudre différentes attaques que l'on peut s'attendre à observer dans un UAS.

La première partie de la thèse implique l'utilisation de théories cybernétiques : des techniques d'observation robustes pour réaliser une détection robuste d'anomalies dans un réseau TCP (Transmission Control Protocol). Les travaux se sont concentrés sur la conception d'un observateur robuste basé la méthode des fonctionnelles de Lyapunov-Krasovkii et d'un système de gestion de file d'attente active (AQM) dans un réseau TCP. En exploitant la dynamique du réseau TCP, nous pouvons détecter un trafic réseau anormal.

La deuxième partie de la thèse utilise la théorie multifractale pour identifier les trafics présentant une anomalie. Les travaux se sont concentrés sur la conception d'un prototype d'IDS fonctionnel basé sur l'analyse Wavelet Leader Multifractal (WLM) pour identifier des anomalies telles que la congestion du réseau générée par une attaque DoS. Dans l'expérience, nous observons que la signature WLM d'un réseau UAS simulé peut être radicalement différente entre un trafic normal et un trafic affecté par une attaque DoS. Par une simple comparaison analytique entre les différentes signatures, nous pouvons identifier le trafic avec ou sans attaque.

La troisième partie de la thèse consiste à utiliser l'intelligence artificielle (IA) pour améliorer les performances de détection. Nous avons introduit un réseau de classification Long Short-Term

memory (LSTM) (et d'autres réseaux de neurones) pour augmenter la qualité de détection. Ici, au lieu de cibler une attaque évidente, telle que l'attaque DoS, nous avons tourné notre attention vers une attaque plus délicate, telle que l'attaque Man in the Middle (MITM). En adaptant l'analyse WLM et les principes d'apprentissage automatique, nous avons constaté qu'il est possible d'atteindre un niveau de détection prometteur pour une attaque de falsification des coordonnées géographiques des drones dans un réseau UAS simulé.

Mots-clés : Détection d'intrusion, Réseau, Drones

Summary: In recent years, the development of the Unmanned Aerial System (UAS) involving swarms of unmanned aerial vehicles (UAVs) has experienced unprecedented progress. However, network systems implemented in current commercial UASs are often variations of existing network systems. Thus, pre-existing vulnerabilities may still exist, while new vulnerabilities emerging from the new properties of a UAS, such as mobility and interconnectivity, are of even greater concern. As UASs operate in civilian airspace, safety and security are essential.

This thesis was created in response to growing demand. In this thesis report, three strategies are explored to seek to resolve different attacks that we would expect to observe in a UAS.

The first part of the thesis involves the use of cybernetic theories: robust observation techniques to achieve robust detection of anomalies in a TCP (Transmission Control Protocol) network. Work focused on the design of a robust observer based on the Lyapunov-Krasovkii functional and queuing dynamics of an Active Queue Management system in a TCP network. By exploiting the dynamics of the TCP network, which contains AQM, we can distinguish anomalous network traffic.

The second part of the thesis consists in using the multifractal theory to identify the traffics presenting an anomaly. Work focused on designing a working prototype of an IDS based on Wavelet Leader Multifractal (WLM) analysis to identify anomalies such as network congestion generated by a DoS attack. In the experiment, we observe that the WLM signature of a simulated UAS network can be radically different between normal traffic and traffic affected by a DoS attack. By applying a simple analytical comparison between the different signatures, we can identify traffic with or without attack.

The third part of the thesis consists in using artificial intelligence (AI) to improve detection performance. We introduced a long short-term memory (LSTM) classification network (and other neural networks) to increase detection accuracy. Here, instead of targeting an obvious attack, such as the DoS attack, we turned our attention to a more delicate attack, such as the Man in the Middle (MITM) attack. By adapting WLM analysis and Machine Learning principles, we have found that it is possible to achieve a promising level of detection for an spoofing attack on the geographic coordinates of individual UAVs in a simulated UAS network.

Keywords: Drones, intrusion detection, network