Sécurisation des communications dans un réseau ad hoc au sein d'un essaim de drones

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : Sécurisation des communications dans un réseau ad hoc au sein d'un essaim de drones / Christophe Guerber ; sous la direction de Mickaël Royer

Est une reproduction de : Sécurisation des communications dans un réseau ad hoc au sein d'un essaim de drones Christophe Guerber 2022

Auteur(s) : Guerber, Christophe

Autre(s) auteur(s) : Royer, Mickaël (1981-....)
Institut national des sciences appliquées Toulouse 1961-....
École doctorale Systèmes Toulouse 1999-....

Diffusion / Distribution : Toulouse : INSA Toulouse, 2022

Description matérielle : 1 vol.(vi-121 p.) : ill.en coul. ; 30 cm

Titre traduit ajouté par le catalogueur : Securing communications in an ad hoc network of a swarm of drones eng

Classification décimale Dewey : 358.418

Note sur la responsabilité : Ecole(s) Doctorale(s) : École doctorale Systèmes
Partenaire(s) de recherche : ENAC-LAB - Laboratoire de Recherche ENAC (Laboratoire), Laboratoire de recherche ENAC (Laboratoire)
Autre(s) contribution(s) : Vincent Nicomette (Président du jury) ; Mickaël Royer, Rida Khatoun, Thi Mai Trang Nguyen, Jean-François Lalande, Serge Chaumette (Membre(s) du jury) ; Rida Khatoun, Thi Mai Trang Nguyen (Rapporteur(s))

Note sur les bibliographies et les index : Bibliogr.p.109-117

Note de thèses et écrits académiques : Reproduction de Thèse de doctorat Systèmes embarqués Toulouse, INSA 2022

Résumé ou extrait : Les drones sont de plus en plus présents, dans nos vies pour le loisir comme dans l'industrie. Les prévisions sur le marché des drones civils envisagent une croissance importante sur les

prochaines années et pourrait atteindre 10 à 20 milliards d'euros au niveau mondial.Si les missions confiées aux drones ont tout d'abord considéré des drones isolés, certains types de missions nécessitent la collaboration de plusieurs d'entre eux au sein d'une flotte.Une flotte de drones nécessite la mise en œuvre et la disponibilité d’un réseau sans fil pour toute les tâches ayant trait d’une part à la mission et d’autre part à toute coordination ou synchronisation. Les réseaux sans fil sont par nature ouverts sur l’extérieur et il se pose donc la question de leur sécurisation. Plusieurs travaux de recherche ont abordé cette question avec différents angles d’attaque : la couche physique, les protocoles de routage, les systèmes multi agents. Mais aucun n’aborde la question de la sécurisation de l’accès à ce réseau et peu ont étudié la question des réponses à apporter en cas d’attaque.Dans cette thèse nous proposons une architecture orientée vers la sécurité permettant une meilleure maîtrise des communications dans le réseau, et s'affranchissant entièrement de toute infrastructure fixe au sol. Cette architecture allie les réseaux définis par logiciels (SDN), qui est une technologie qui a émergé récemment, avec AODV, un protocole de routage adapté aux réseaux ad hoc de type FANET. Nous démontrons que cette architecture permet de protéger le réseau contre la plupart des attaques depuis l'extérieur. Cette architecture nous permet également d'obtenir une bonne connaissance de l'activité dans le réseau, pré-requis pour améliorer la sécurité.De cette connaissance, nous proposons d'une part une technique de détection d'injection de trafic depuis l'extérieur et une méthode pour s'en défendre. D'autre part, nous proposons un ensemble de caractéristiques mesurables de l’activité du réseau propres à être utilisées avec un algorithme d’apprentissage automatique.Nous démontrons la pertinence de ces mesures en entraînant un modèle de classification par apprentissage supervisé de type Random Forest sur un ensemble de captures réseaux présentant des attaques sur le réseau: déni de service (DoS), balayage de ports, découverte de mot de passe (brute force) et déni de service distribué (DDoS). Les performances en terme de détection d’attaques basées sur ces caractéristiques sont prometteuses, non seulement en terme de précision mais également en terme de vitesse de détection, offrant ainsi la possibilité d'une réaction en temps réel. Cette réaction peut être mise en œuvre grâce à l'architecture proposée dans cette thèse. Des tests sur des scénarios représentatifs d'un trafic réseau pour une flotte de drones montrent que le modèle est capable de généraliser avec de bonnes performances sur notre cas d'étude.

Drones become more and more frequent in our everyday life as a leasure and also in the industry. Analysts forcast a steady growth of the civilian drones market which could reach 10 to 20 billion euros worldwide in the coming years.Nowadays, missions mostly operate single Unmaned Aerial Vehicle (UAV). But researchers are now considering swarms of drones to be more efficient to solve specific problems. Drones now have to collaborate and coordinate.Teams of drones require the availability of a wireless network for all the tasks required by the mission but also for additional coordination and synchronisation needs.Wireless networks are open to the outside by nature and securing such network is a challenging task. Several solutions proposed to tackle this issue from different aspects of data communication and securing either the physical layer or the routing protocols, or at the application level in multi-agent systems. None, however, considered securing the access to the network and few proposed efficient counter-measures.In this thesis, we propose a security oriented network architecture that allows controlling the communication in the network, with no fixed ground based infrastructure and with a single wireless interface card. It brings emerging Software Defined Network technology together with AODV, a routing protocol suitable for flying ad hoc network (FANET). We demonstrate that the architecture allows to protect the network against most sorts of attacks from the outside. In addition, it brings a good knowledge of the activity within the network, which is a prerequisite to further improve security.From this knowledge, we propose a detection algorithm for traffic injection attacks from an outside node and the corresponding counter-measure. Then, we propose a set of measurable features on the activity within the network suitable for a machine learning algorithms to detect abnormal behaviors.We demonstrate the

relevance of these features by training a Random Forest classification machine learning algorithm on a dataset consisting of network captures including several network attacks : denial of service (DoS), port scan, password cracking using bruteforce and distributed denial of service (DDoS). The performances of the detection based on these features are promissing, not only in terms of precision but also in terms of speed, paving the way for applying counter measures in real time. The latter may be conveniently put in place using the proposed architecture. Tests using representative scenarios of network traffic for a swarm of drone show a good generalization of the ML model and good performances.

Sujet - Nom commun : Drones
SDN (architecture des réseaux d'ordinateurs)
Apprentissage automatique

Forme, genre ou caractéristiques physiques : Thèses et écrits académiques
Thèses et écrits académiques