

## Conception d'un récepteur AIS détectant les falsifications de messages

Type de contenu : Texte

Type de médiation : b

Type de support : Ressource dématérialisée

Titre(s) : Conception d'un récepteur AIS détectant les falsifications de messages : développement de stratégies et prototypage sur FPGA / Maelic Louart ; sous la direction de Abdel-Ouahab Boudraa

Auteur(s) : Louart, Maelic (1994-....)

Autre(s) auteur(s) : Boudraa, Abdel-Ouahab (19...-....)

Tourneret, Jean-Yves (19...-....) enseignant-chercheur en traitement du signal

Auger, François (1966-....) enseignant-chercheur en génie électrique

Jego, Christophe (1973-....)

Dupraz, Elsa (1987-....)

Ménard, Daniel (19...-....) professeur en électronique

Le Lann, Jean-Christophe (1971-....)

Szkolnik, Jean-Jacques (1964-....)

Baghdadi, Amer (1974-....) auteur en microélectronique

Le Roy, Frédéric (19...-....) auteur d'une thèse en sciences et techniques

École nationale supérieure de techniques avancées Bretagne Brest 2010-....

École doctorale Sciences pour l'ingénieur et le numérique

Production : 2023

Titre traduit ajouté par le catalogueur : Design of an AIS receiver detecting messages falsifications strategies development and FPGA prototyping eng

Autres classifications : 620

Classification décimale Dewey : 621.3

Note sur le titre et les responsabilités : Titre provenant de l'écran-titre

Note sur la responsabilité : Ecole(s) Doctorale(s) : École doctorale Sciences pour l'ingénieur et le numérique

Partenaire(s) de recherche : Laboratoire en Sciences et Techniques de l'Information- de la Communication et de la Connaissance / LabSTICC (Laboratoire), Institut de Recherche de l'École Navale / IRENAV (Laboratoire)

Autre(s) contribution(s) : Jean-Yves Tourneret (Président du jury) ; Elsa Dupraz, Daniel Ménard, Jean-Christophe Le Lann, Jean-Jacques Szkolnik, Amer Baghdadi, Frédéric Le Roy (Membre(s) du jury) ;

François Auger, Christophe Jegou (Rapporteur(s))

Note de thèses et écrits académiques : Thèse de doctorat Sciences et technologies de l'Information et de la communication Brest, École nationale supérieure de techniques avancées Bretagne 2023

Résumé ou extrait : L'AIS est un système de communication pour bateaux très répandu. Il permet l'échange automatique d'informations de navigation comme la position, la vitesse, la route, l'identité, le port de départ et d'arrivée, etc. Ces informations aident à la navigation, sécurisent le trafic maritime et simplifient la surveillance des autorités de contrôle. Cependant, ayant été développé dans les années 90, l'AIS est peu sécurisé. [...]. Partant de ce constat, dans ce manuscrit, trois stratégies ont été développées pour détecter ces attaques. La première suit les bateaux avec un filtre IMM pour détecter les falsifications de position et de vitesse. La deuxième vérifie le respect, par les bateaux, du mode d'accès TDMA lorsqu'ils communiquent. La vérification de ce mode d'accès, spécifié par la norme AIS, permet de détecter l'émission de faux messages et la création de bateaux fantômes. Enfin, la dernière stratégie calcule une signature radiométrique, à partir des signaux transmis par chaque transpondeur, afin de les identifier matériellement et non par l'identité qu'ils transmettent dans leurs messages [...]. Ces trois stratégies sont appliquées conjointement et ont été testées avec des signaux réels enregistrés dans la rade de Brest. Des taux d'erreur de première et de deuxième espèce respectivement de 0.0035 et 0.0171 sur la détection de l'usurpation d'identité ont été obtenus. Par ailleurs, des simulations de Monte Carlo ont montré une sensibilité aux falsifications de position allant de 35m à 250m. Une partie de ces stratégies a été implémentée sur un système embarqué de type FPGA pour être utilisée par la douane ou la marine française. Toute la chaîne de démodulation des signaux AIS a aussi été implémentée sur la même carte pour récupérer les signaux et les informations des messages utilisés par ces stratégies. La génération du code implémentant le FPGA s'est faite en utilisant la HLS qui est un outil de synthèse haut niveau. Ce cas d'application a montré que cet outil était aujourd'hui une technologie mature pouvant synthétiser efficacement et automatiquement des systèmes complets de grande taille à partir d'une modélisation haut niveau, supprimant ainsi la séparation qui existait autrefois entre les activités de traitement de signal et les activités de conception matérielle. Le récepteur AIS intelligent ainsi conçu peut, à partir de signaux en bande de base, détecter, en temps réel, les falsifications de position. Pour finir, un laboratoire virtuel sur FPGA, simulant, en même temps, le récepteur et son environnement, a été aussi développé. Il permet de générer facilement des scénarios de test variés afin de vérifier le comportement du récepteur dans ses conditions limites d'utilisation. La considération conjointe du récepteur, de son environnement et de leurs interactions nous a amené à parler des systèmes cyber-physiques et des difficultés, toujours actuelles, associées à la modélisation et la simulation de tels systèmes. Une nouvelle méthode a été proposée pour résoudre ces difficultés. Cette méthode modélise le CPS comme un ensemble d'acteurs s'exécutant de manière concurrente, utilise le FPGA comme plateforme de simulation et applique la HLS pour générer automatiquement la description matérielle à partir de la modélisation à base d'acteurs. Un laboratoire virtuel a été créé sur FPGA pour vérifier le comportement de notre récepteur. Il permet de simuler en même temps notre récepteur et son environnement maritime, pour lequel le nombre de bateaux communiquant, leur trajectoire, le SNR de leurs signaux transmis et le CFO de leur transpondeur peuvent être modifiés. En plus, des falsifications de position et des usurpations d'identité peuvent aussi être ajoutées aux messages échangés durant la simulation.

AIS is a widely used communication system for ships. It allows the automatic exchange of information such as position, speed, course, identity, port of departure and arrival, etc. This information assists navigation, secures maritime traffic and simplifies surveillance by the coastguard. However, having been developed in the 90s, AIS is not very secure. [...]. Based on this observation, in this manuscript, three

strategies have been developed to detect these attacks. The first one tracks ships with a filter to detect position and speed falsifications. The second verifies that the boats respect the TDMA access mode when they communicate. The verification of this access mode, specified by the AIS standard, makes it possible to detect the transmission of false messages and the creation of ghost ships. Finally, the last strategy calculates a radiometric signature from the signals transmitted by each transponder in order to identify them physically and not by the identity they transmit in their messages.[...]. These three strategies are applied jointly and have been tested on real signals recorded in the Brest harbour. First and second kind error rates of 0.0035 and 0.0171 respectively on the detection of identity spoofing have been obtained. In addition, Monte Carlo simulations have shown a sensitivity to position falsifications ranging from 35m to 250m. Some of these strategies have been implemented on a FPGA to be used by the coast guard or the navy. The entire AIS signal demodulation chain was also implemented on the same board to recover the signals and information used by these strategies. The generation of the code implementing the FPGA was done using the HLS which is a high level synthesis tool. This application case showed that this tool is now a mature technology that can efficiently and automatically synthesise large complete systems from high-level modelling, thus removing the separation that once existed between signal processing and hardware design activities. The resulting AIS receiver can detect position falsifications from baseband signals in real time. Finally, an FPGA-based virtual laboratory that simulates the receiver and its environment at the same time has also been developed. It allows to easily generate various test scenarios to verify the behaviour of the receiver in its limit conditions of use. The joint consideration of the receiver, its environment and their interactions led us to talk about cyber-physical systems and the difficulties, still current, associated with the modelling and simulation of such systems. A new method has been proposed to solve these difficulties. This method models the CPS as a set of concurrently executing actors, uses the FPGA as a simulation platform and applies HLS to automatically generate the hardware description from the actor based modelling. A virtual laboratory has been created for our receiver. It allows to simulate, at the same time, our receiver and its maritime environment for which the number of communicating vessels, their trajectories, the SNR of their transmitted signals and their transponder's CFO can be modified.

Configuration requise : Configuration requise : un logiciel capable de lire un fichier au format : PDF

Sujet(s) : Système d'identification automatique

Détection de falsification

FPGA-simulation basée sur système cyber-physique

Synthèse de haut niveau

Sujet - Nom commun : Systèmes d'Identification Automatique (transports maritimes)

Transports maritimes

Navigation -- Mesures de sécurité

Systèmes embarqués (informatique)

Synthèse de haut niveau (informatique)

Réseaux logiques programmables par l'utilisateur

Forme, genre ou caractéristiques physiques : Thèses et écrits académiques

Adresse électronique et mode d'accès : <http://www.theses.fr/2023ENTA0006/document>||Accès au texte intégral

<http://www.theses.fr/2023ENTA0006/abes>||  
<https://theses.hal.science/tel-04612536>||