HAL open science

Holistic Approach of Integrated Navigation Equipment for Cybersecurity at Sea

Clet Boudehenn, Jean-Christophe Cexus, Ramla Abdelkader, Maxence Lannuzel, Olivier Jacq, David Brosset, Abdel Boudraa

To cite this version:

Clet Boudehenn, Jean-Christophe Cexus, Ramla Abdelkader, Maxence Lannuzel, Olivier Jacq, et al.. Holistic Approach of Integrated Navigation Equipment for Cybersecurity at Sea. International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science, Jun 2022, Wales, United Kingdom. pp.75-86, 10.1007/978-981-19-6414-5_5 . hal-04028968

HAL Id: hal-04028968

https://hal.science/hal-04028968v1

Submitted on 14 Mar 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Holistic Approach of Integrated Navigation Equipment for Cybersecurity at Sea

Clet Boudehenn and Jean-Christophe Cexus and Ramla Abdelkader and Maxence Lannuzel and Olivier Jacq and David Brosset and Abdel Boudraa

Abstract Recent studies have demonstrated the interest of analyzing GNSS (*Global Navigation Satellite System)* and AIS (*Automatic Identification System)* data to improve the safety of naval infrastructures for a wide spectrum of maritime applications. However, in-depth analyzes also underline the sensitivity of these systems to attacks such as jamming and spoofing. In this context, it is essential that researchers, specialized organisations and companies rely on realistic data to improve these types of systems to better detect and cope with potential threats. However, because of the lack of open data sets, or due to financial, technical or operational reasons, the use of simulated data is preferred in most cases over real life data, which can lead to biases. To cope with this challenge, we have developed a prototype called "HAPPINESS" for "**Holistic APProach of Integrated Navigation Equipment for Cybersecurity at Sea**". The main objective of this dedicated and autonomous embedded system is to collect navigation data in real time without using proprietary or restrictive protocols. The generated open data, then continuously feeds a cyber naval platform able to reproduce the functional and operational systems of a ship. This prototype allows to reproduce the kinematics of a ship in various contexts (like specific maneuvers, long tracks, docking...) in NMEA format in order to design highly realistic scenarios based on real life data and allowing to obtain more complete and richer data (than those freely accessible online) in terms of information, giving additional means to detect anomalies on navigation systems.

Maritime Systems, Navigation Systems, GNSS, GPS, AIS, NMEA, Embedded systems, Data Collection, Navigation datasets generation.

Clet Boudehenn
Naval Academy Research Institute (IRENav), Arts et Metiers Institute of Technology, Brest, France,
e-mail: clet.boudehenn@ecole-navale.fr

Jean-Christophe Cexus
LAB-STICC, UMR CNRS 6285, Ensta-Bretagne (29806 Brest Cedex 9, France),
e-mail: jean-christophe.cexus@ensta-bretagne.fr

1 Introduction

Transportation by sea is the main mean for worldwide goods exchange and represents an essential resource for economic exchanges all over the world. Nowadays, more than 90% of the world's trade in volume is carried out by sea, with nearly 290 tons of goods transported via maritime means every second. In this global context, the digital field has been widely deployed for several years now, especially on-board of merchant ships, thus conducting the maritime sector into a continuous shift towards digitalization. A ship built during the last decade shows all characteristics of a full information system. For instance, programmable logical controllers are used for engine and power management, while the bridge is now highly relying on digital sensors, networks and displays for navigation [5]. Internal systems are increasingly complex and not necessarily designed with a cyber security approach. Meanwhile, the number of cyber attacks targeting these types of systems is increasing, especially due to criminal and non-state actors having a real interest in them. Thus, understanding how these systems work through the analysis of field data is a major challenge in order to implement efficient countermeasures and cyber threat detection policies.

Generic and specific vulnerabilities are discovered every day, widening the attack surface of the sector, potentially endangering thousands of ships worldwide [10]. Experts have demonstrated that disrupting the operational functions and functional elements of a ship at sea is not fictitious [1]. These demonstrations came some time after researchers spoofed and jammed the *GPS* and *AIS* sensors of a super yacht at low cost during her navigation [9]. The number of *GNSS* and *AIS* spoofing cases has increased steadily over the last decade, impacting the whole sector (civilian and military ships and harbors), elevating the risks of accidents, especially in critical navigation areas such as straits or channels, where sometimes the current geopolitical context is more and more tense. Increasingly frequent events highlighting the vulnerabilities and potential consequences of this sector have put cybersecurity issues back on the table and are now part of the decision-making process [1, 8]. In addition, the International Maritime Organisation (*IMO*), responsible for maritime space, has now applied guidelines [2] to require shipowners to take into account appropriate cybersecurity regulations and policies on-board the ships [4].
The Suez canal obstruction in March 2021 for more than 6 days by the large container ship Ever Given impacted more than 10% of the world's freight transport and caused Ever Green company to lose millions of dollars[3] The cause of the accident has been attributed to a combination of environmental factors like high winds and human error in navigational inputs by the bridge team. Even though it is unlikely that a

[1] Available:https://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424 (accessed 09 2021).

[2] https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

[3] Available: https://www.bloomberg.com/news/features/2021-06-24/how-the-billion-dollar-ever-given-cargo-ship-got-stuck-in-the-suez-canal (accessed 09 2021).

cyber-attack was the cause, it is a reminder that this type of maritime incident can have high economic and geopolitical consequences.
A ship is a complex system of systems: from the bow to the stern, from the engine room to the bridge, tens of Information Technology (IT) and Operational Technology (OT) systems are interconnected to ensure her mission and safety. Among the potentially vulnerable systems of the ship, we can cite more precisely the various systems contributing to the navigation function, such as *GPS* and *AIS*, but also the *NMEA* (National Marine Electronic Association) interconnection standard [2, 6, 7].
In order to develop solutions able to reduce the cyber attack surface of vulnerable systems, it is important to understand how this type of system works and to collect a large number of data representing a wide spectrum of situations. Designing relevant scenarios able to reproduce advanced cyber attacks is really useful, especially in a domain where data are not easily accessible due to proprietary systems [3]. It can definitely contribute to perform in-depth studies, detect incidents in specific situations and support operators in decision-making, whatever the context.
In this paper, we present an autonomous on board system capable of collecting in real time *GNSS* and *AIS* information from a moving ship without impacting its on-board functional and operational systems. The prototype is presented in the form of a small suitcase capable of being embarked on any type of vessel and able to collect a huge amount of navigation data such as *GNSS* tracks and *AIS* data. In section 2, we detail the architecture of this system. In section 3, we describe the data collection strategy through the acquisition system and show how useful and relevant it can be for conducting in-depth analysis. In section 4, before the conclusion, we detail some perspectives, as well as the future improvements of the system.

2 Architecture of the system

The on-board *GNSS* data acquisition system we designed had to respect several constraints: it had to be fully autonomus in case of software operation. Moreover, it had to be fully autonomous in case of software operation but also had to be able to fully operate when only powered by a battery.

Most of the components and elements used are very often exploited together, which means that it was very easy to connect them and achieve desired purpose. Fig. 1 shows the complete architecture of our system with the different elements that compose it. Here is the complete list of the chosen elements :

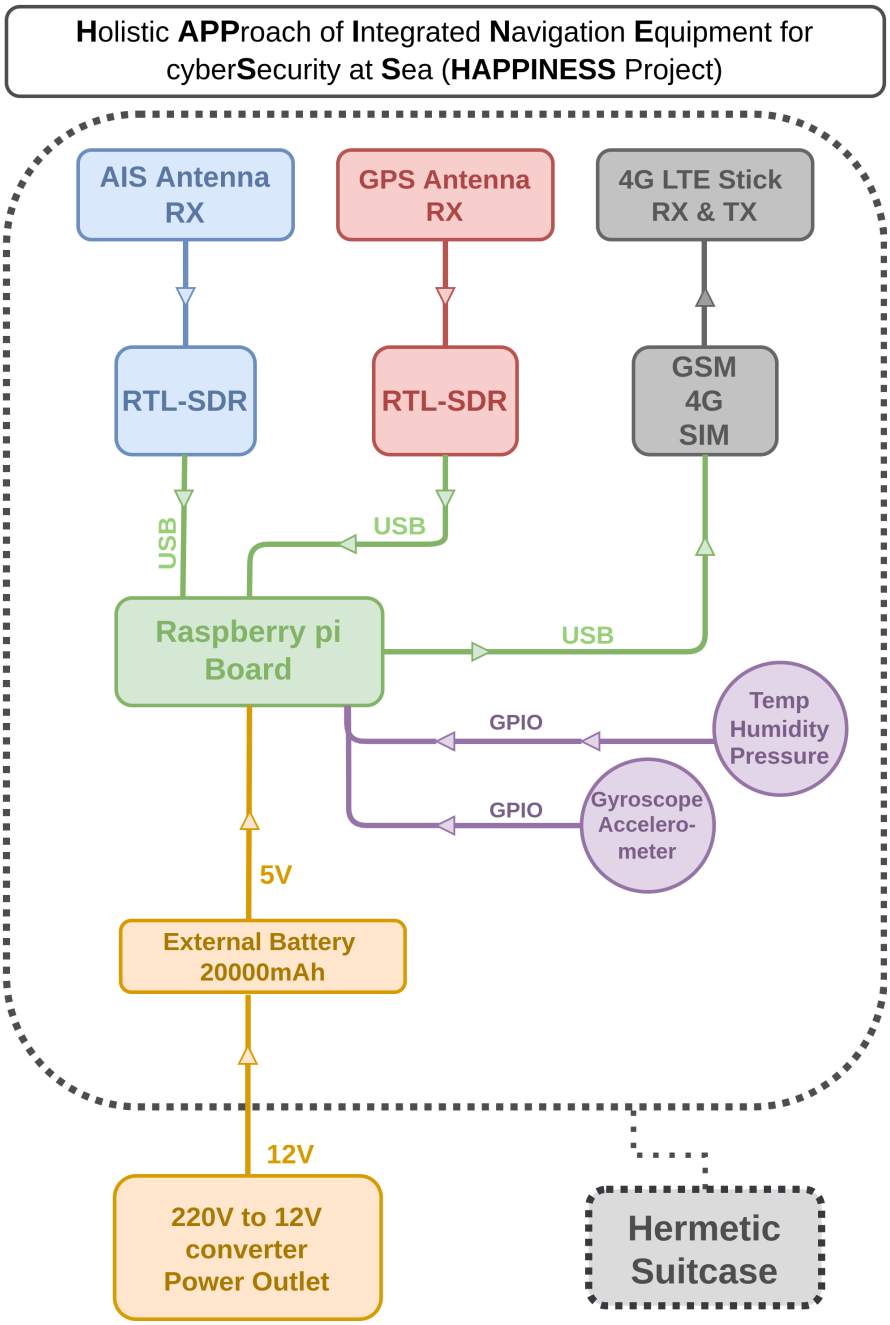

Fig. 1 HAPPINESS Project Architecture.

Here is the complete list of the chosen elements:

- A **Nano computer**. Nano computers are well established in the development board market. In terms of performance, while many boards would be more suitable for embedded operational needs, the Raspberry Pi 4, for example, remains very easy to use, has a very active and growing community, is affordable, its Linux base is fully adapted to the projects for embedded and easy programming. Moreover it is sufficiently powerful for this type of tiny data collection project.
- **RTL-SDR (Software Defined Radio) dongle** is a dongle that can be used as a computer-based radio scanner for receiving live radio signals, ideal for *GPS* and *AIS* data reception. It is plugged into one of the USB ports of the Raspberry Pi.
- **GPS receiver** with its remote antenna to increase accuracy, is connected via USB to the Raspberry Pi.
- An **AIS antenna** (tuned for the Maritime *VHF* (*Very High Frequency*) band where the AIS frequencies of 161.975 and 162.025 MHz are located) connected to the RTL-SDR dongle.
- More traditional **sensors**: Accelerometer *MMA8451*, Gyroscope *GYR03b* and a weather sensor *BMEE680*, to measure humidity, pressure and temperature values. All these sensors have a low power consumption and are connected to the *I2C* (*Inter-Integrated Circuit* pins on the **GPIO** (*General Purpose Input/Output*) pins of the Raspberry board.
- An **USB 4G stick**, allowing to have a sufficiently large 4G coastal coverage in the navigation areas and a SIM subscription to send information in real time via the Internet. This transmission is achieved in a secure way, via the use of a Virtual Private Network.
- An **External Battery of** 20000 **MAh**, which supplies the needed power for the Raspberry board and its components in a continuous manner. It allows the system to have autonomy of about 24 hours. The external battery is also constantly plugged into a 220 V power outlet on board the ship, ensuring a high level of power resilience, which has proven to be useful during maintenance operations.
- All elements are embedded into a **hermetic and electrically insulated suitcase**.

3 Methodology for Data Collection

This section describes the method used to receive, collect and interpret the data in real time, but also how to save it in a long term retention database.

Once the whole system built, a thorough definition of the collect and visualization processes was necessary. Data flowing from the different sensors and receivers of the suitcase are first recorded on the embedded system for local storage and then sent to shore to a remote server to be ingested into a more global database. For the first phase of this prototype, we asked "***Morlenn Express***" shipping company [4]) the

[4] http://www.morlenn-express.com/

authorization to set up the system on one of their boats. The boats of this company, specialized in the local transportation of passengers, can accommodate an average of 200 people to travel between different cities in Brittany, especially between the maritime cities of Brest and Crozon, on the French west coast. Those boats, 35 meters long and 7 meters wide, make simple and regular maneuvers throughout the day, achieving 4 round trips per day with an average duration of 1 hour per trip, suitable for the validation phases of the prototype. The following diagram (Fig. 2) shows the data collection methodology.

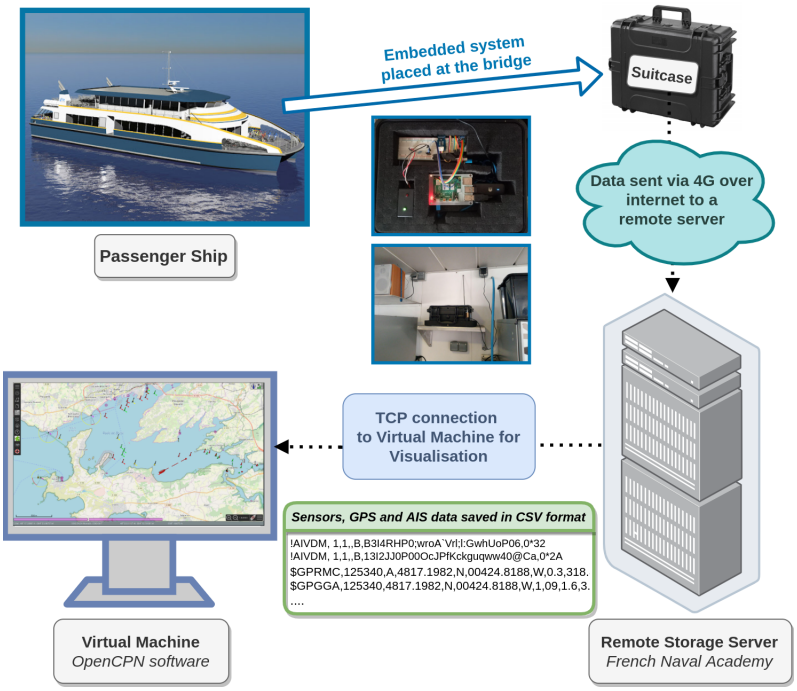

Fig. 2 Data Collection Methodology.

This prototype was placed directly on the bridge of one of the company's boats so that it is electrically powered and easily accessible. Once the system is in place, the 4G LTE connection allows us to send data to the remote server. Ashore, data are sorted, parsed and cleaned in real time to ease and enrich further analysis before being stored on the server. Finally, we send those data to an open-source **ECS** (Electronic Chart System) called *OpenCPN*[5].

[5] https://www.opencpn.org/

The data, whether from sensors, *GPS* or *AIS*, are all first of all stored using the "*.csv*" format, with different headers and timestamps. The reception of navigation data is *NMEA-0183* standard compliant. This format, very similar to the operation of the CAN bus protocol, was created to ease connections between navigation systems (Lock, Speedometers, Echosounders, GPS and AIS receiver, . . .) over serial interfaces. Tab. 1 details some examples of *NMEA* frames Talkers and Sentence IDs received for *GPS* and *AIS*. NMEA frames are coded in ASCII and composed of *Talkers ID* (the first two letters of the frame, indicating which system transmits information ("GP" for GPS, "AI" for AIS, "II" for Integrated Instruments, ...). Then, *Frame Type* gives indications on the content of the complete frame: for example, if we consider a frame with the "GP" Talker, the following type "GGA" will give satellites information, "RMC" will give speed and rudder angle information while "RMB" will give waypoints information. Thoses frames are dedicated to "Listeners" like *ECDIS* (Electronic Chart Display Information Systems) indicating to the operator precise information on the environment in which the boat evolves.

Talker ID	Code	Message Description
GP	GGA	Global Positioning fix data (GPS)
GP	GLL	Latitude / Longitude data (GPS)
GP	RMC	Recommended Minimum data (GPS)
GP	GSV	Satellites in view (GPS)
GP	GSA	GPS DOP and active satellites (GPS)
AI	VDM	Received data from other vessels (AIS)

Table 1 Examples of NMEA messages

During the whole experimentation phase, the acquisition system has been placed for more than 2 months on 3 different ships of the company "***Morlenn Express***", respectively named "*Tibidy*", "*Louarn*" and "*Dervenn*".

The following figures (Fig. 3, 4 and 5) show an examples of data collected on ***August 17 2021*** from 11:09am to 01:10pm (about 2h of data sending) with a round trip of the boat during this period.

Here is the number of frames collected :

- about **2200** NMEA-0183 GPS frames per hour,
- about **5750** NMEA-0183 AIS frames per hour,
- about **4250** frames from various sensors per hour.

Timestamp, NMEA-0183 GPS Data
11:12:02.930554,b"b'$GPGGA,091205.000,4821.7160,N,00433.
11:12:06.929698,b"b'$GPGGA,091209.000,4821.7160,N,00433.
11:12:10.919613,b"b'$GPGGA,091213.000,4821.7160,N,00433.

Timestamp, NMEA-0183 AIS Data
11:12:02.413, !AIVDM,1,1,,A,13HO:bP000Ob7TnKbvP;;AP200S
11:12:04.987, !AIVDM,1,1,,A,13HO:bP000Ob7UHKbvIUWiR`00S
11:12:05.668, !AIVDM,1,1,,B,B3IM:L001OrQs?6rh:Df?wf5WP06

Timestamp, Temp, Pressure, Humidity, Acc X, Acc Y, Acc Z, ..
11:12:01.802633,19.84, 1012.95, 56.385, -2.1068974609374997
11:12:05.796078,19.82, 1012.98, 56.433, -2.1499930908203124
11:12:09.790809,19.8, 1012.98, 56.387, -2.1356278808593747,

Fig. 3 Some samples of collected data.

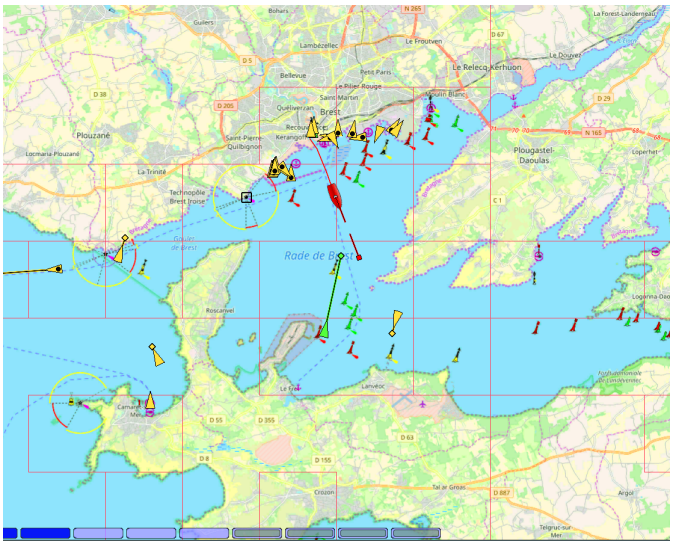

Fig. 4 Example of AIS message visualisation (in black) and ship trajectory (in green) during about 2h.

Thus, since ***June 29 2021***, we have collected a certain amount of data (*GNSS* tracks, NMEA frames and sensors data) thanks to this system that is later intended to remain on board for a long time (probably two years).

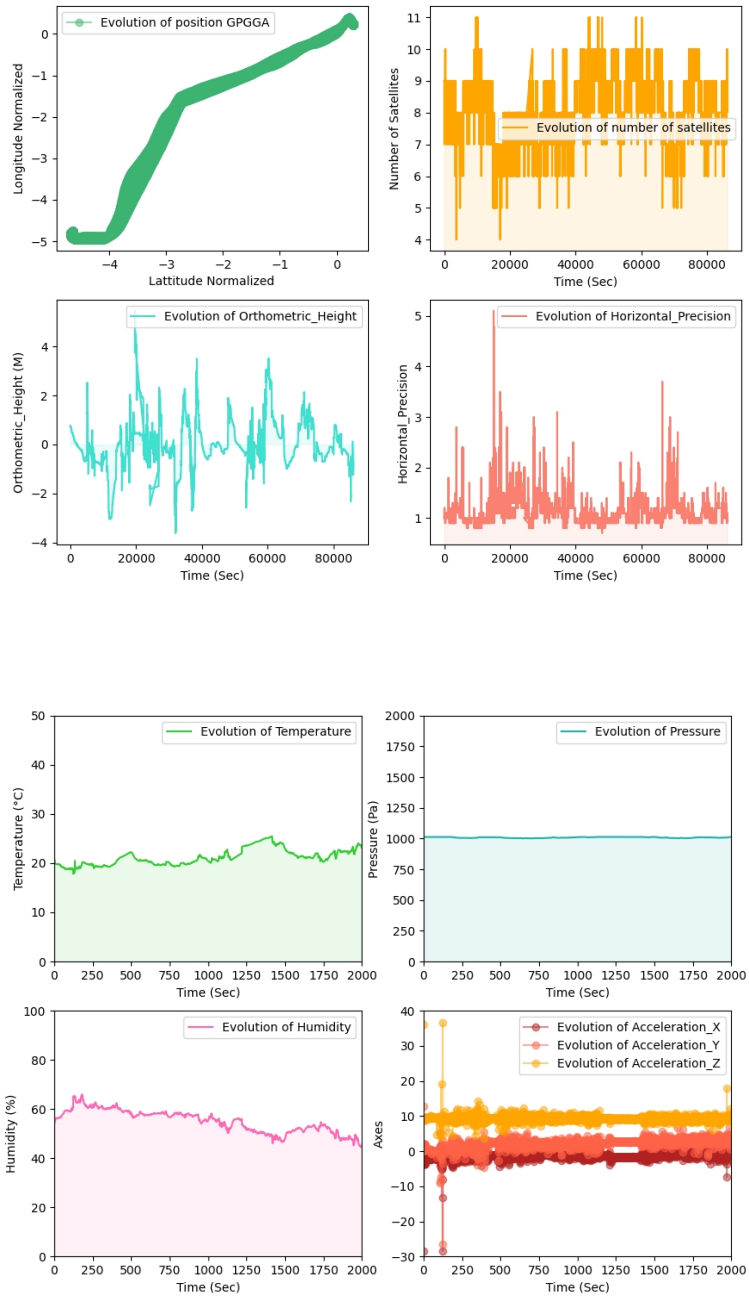

Fig. 5 Evolution of GPGGA and sensors data.

Thus, for an average of 10 hours data reception per day (the moments when the boat is sailing and not at the dock) for 2 months, we obtain a database of more than $19,738,300$ raw frames totaling fairly less than 7 ***Gb***. These data are dedicated to the elaboration of a model representing the normal behavior of a ship of this size. Once cleaned and parsed, we identified **20** features to conduct data-driven analysis such as :

- *Latitude*,
- *Longitude*,
- *Reception_Status*,
- *Speed_Over_Ground*,
- *Track_Angle*,
- *GPS_Receiver_Quality*,
- *Number_Satellites_in_View*,
- *Orthometric_Height*,
- *Horizontal_Dillution_Of_Precision*,
- *Vertical_Dillution_Of_Precision*,
- *Positions_Dillution_Of_Precision*,
- *Satellite_ID, Satellite_Elevation*,
- *Satellite_Azimuth*,
- *SNR*,
- *Maritime_Mobile_Service_Identity*,
- *Ais_Status*,
- *Course*,
- *Heading*,
- *Raim*,
- *Radio*,

These characteristics are the ones that are likely to change when GNSS systems fall victim to cyberattacks such as spoofing. A long-term analysis of the evolution of these features would eventually allow to determine the normal behavior of the detect and can help to detect outliers. The interest of collecting this type of data allows us to have richer information than what we could find on sites that simply give free access to AIS frames. Although these frames are interesting to analyze, the GPS data that we recover here allows us to have additional precise information on the quality of the satellite reception, with for example indications on the constellation of satellites used with by the respective satellites ID (which can be useful in the case of spoofing attack). In the same way, more detailed information on speed and direction and heading is collected. Here, the goal of combining data from AIS, GPS and different sensors allows or correlation for further analysis.

4 Conclusion

In this paper, we present the concept of an embedded and autonomous on-board system able to collect and store local *GNSS* and *AIS* information. As of August 2021, 2 prototypes of this project are currently operating on 2 different ships from the maritime transport company "***Morlenn Express***" and 2 others in the final step of development. This project allows us to gather huge amount of *GNSS* tracks data (such as *GPS*, *AIS*, and various kinetic and motion sensors such as accelerometers, gyroscopes and also weather sensors). It feeds a database for long term retention, thanks to the real-time transmission to a remote shore server in a secure infrastructure, generating open data to feed a *Naval Cyber Range*. These data allow us to reproduce typical scenarios of this kind of passenger-carrying vessels, merchant ships or cargoes. Since the beginning of the project, we have captured almost 4 full months of data and more than 19 million GPS and AIS frames. In addition, this project makes it possible to easily conduct data sets generation experimentations, ship motion and kinetics in-depth features analysis in the context of cyber attacks such as *GNSS* spoofing, which are increasing in this critical domain. Future work will include improvements in the quality of the antennas and receivers, more suitcases will be placed in different types of ships in a longer period, and conduct more global studies in order to select and study the relevant features and to model the normal behavior of a ship.

Acknowledgements This work is supported by the Chair of Naval Cyber Defence and its partners Thales, Naval Group, French Naval Academy, IMT-Atlantique, ENSTA-Bretagne and the Region Bretagne. Special thanks to the maritime transport company "*Morlenn Express*", who agreed to collaborate with us for the testing and the validation of this project.

The following abbreviations were used in this manuscript:

GNSS Global Navigation Satellite Systems
AIS Automatic Identification System
GPS Global Positioning System
NMEA National Marine Electronics Association
IMO International Maritime Organisation
GPIO General Purpose Input Ouput
I2C Inter Integrated Circuit
VHF Very High Frequency
HDOP Horizontal Dilution of Precision
VDOP Vertical Dilution of Precision
MMSI Maritime Mobile Service Identity
ECS Electronic Chart System
ECDIS Electronic Chart Display Information Systems

References

1. Alincourt, E., Ray, C., Ricordel, P.M., Dare-Emzivat, D., Boudraa, A.: Methodology for AIS signature identification through magnitude and temporal characterization. In: OCEANS 2016 - Shanghai (2016)
2. Balduzzi, M., Pasta, A., Wilhoit, K.: A security evaluation of ais automated identification system. In: Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC '14 (2014)
3. Becmeur, T., Boudvin, X., Brosset, D., Héno, G., Costé, B., Kermarrec, Y., Laso, P.M.: Generating data sets as inputs of reference for cyber security issues and industrial control systems. In: 2017 11th International Conference on Research Challenges in Information Science (RCIS) (2017)
4. Blauwkamp, D., Nguyen, T.D., Xie, G.G.: Toward a deep learning approach to behavior-based AIS traffic anomaly detection. In: (DYNAMICS) Workshop, San Juan. (2018)
5. Boudehenn, C., Cexus, J.C., Boudraa, A.: A data extraction method for anomaly detection in naval systems. In: International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (2020)
6. Boudehenn, C., Jacq, O., Lannuzel, M., Cexus, J.C., Boudraa, A.: Navigation anomaly detection: An added value for maritime cyber situational awareness. In: International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (2021)
7. Iphar, C., Napoli, A., Ray, C.: An expert-based method for the risk assessment of anomalous maritime transportation data. Applied Ocean Research (2020)
8. Iphar, C., Napoli, A., Ray, C., Alincourt, E., Brosset, D.: Risk analysis of falsified automatic identification system for the improvement of maritime traffic safety. In: 26th European Safety and Reliability Conference (2016)
9. K., J.: From super-yachts to web isolation. Computer Fraud & Security **2017**(12) (2017)
10. Mileski, J., Clott, C., Galvao, C.: Cyberattacks on ships: a wicked problem approach. Maritime Business Review **3** (2018). DOI 10.1108/MABR-08-2018-0026