# Navigation anomaly detection : An added value for Maritime Cyber Situational Awareness

Clet Boudehenn, Olivier Jacq, Maxence Lannuzel, Jean-Christophe Cexus, Abdel Boudraa

# Navigation anomaly detection: An added value for Maritime Cyber Situational Awareness

Clet Boudehenn†, Olivier Jacq†, Maxence Lannuzel†, Jean-Christophe Cexus* and Abdel Boudraa+
†Chair of Naval Cyber Defence, Ecole Navale (CC 600, 29240 Brest Cedex 9, France).
+IRENav, EA 3634, Ecole Navale (CC 600, 29240 Brest Cedex 9, France).
*LAB-STICC, UMR CNRS 6285, ENSTA-Bretagne (29806 Brest Cedex 9, France).
clet.boudehenn, olivier.jacq, maxence.lannuzel, boudra@ecole-navale.fr, cexusje@ensta-bretagne.fr.

***Abstract*—The maritime sector is facing a continuous shift towards digitalization. A ship built during the last decade shows all characteristics of a comprehensive information system, combining information and operational technologies. While industrial programmable logic controllers are used for engine and power management, the bridge is now highly relying on digital sensors, networks and displays for navigation. Meanwhile, over the last few years, many cyber attacks targeting maritime assets and made publicly confirm a real interest of criminal and non-state actors in this critical sector for our globalized economies. In this work, a concept designed to detect and visualize advanced navigation cyber attacks on maritime systems using contextual NMEA data analytics is presented. A strategy is built to enhance the detection of navigation spoofing attacks, assess possible physical impacts onboard and support decision makers.**

***Index Terms*—Maritime Systems, Cyber Situational Awareness, Machine Learning, Anomaly Detection, Visualisation**

## I. Introduction

Ever since the first times of sea trading, piracy has been an immediate concern. Whether in a will for competition over the importation of goods, fishing or protection of national seaplanes and territories, the maritime sector is definitely a high-value target. Modern civilian and military ships highly rely on information systems to achieve their daily activities. For instance, a nuclear aircraft carrier combines *Information Technology* (IT) and *Operational Technology* (OT) systems of an airport, an airline company, a nuclear power plant, a major hotel and restaurant for thousands of employees, logistic and traditional ship management systems. With a construction cost of 200M$, the latest 400-meter long container ships, operated by a crew of 20 people only, are also high value units, carrying over 21,000 twenty-feet Equivalent Units (TEU) containers[1] for a value reaching over 1 billion. Operating 90 percent of global world trade[2], shipping industry also needs efficient shore IT and OT infrastructures. A disruption of logistic systems is a feared event for the shipping sector, and recent incidents have shown the possible impacts on activity for shipowners[3] and harbours[4]. Naval OT systems may use proprietary and dedicated protocols and software such as *Electronic Chart and Display Information Systems* (ECDIS), *Voyage Data Recorders* (VDR) or *National Marine Electronics Association* (NMEA Standard). But, in most cases, usual operating systems and *Industrial Control Systems* (ICS) technologies and brands are used. This means that any vulnerability found on *Commercial Off The Shelf* (COTS) systems is most of the time also found onboard a ship. As the average lifetime of a ship is approximately 30 to 40 years, with one or two important maintenance and overhauling periods, the attack surface can be very high if no patching process has been notified to contractors.

Detecting and reacting in due time to a cyberattack targeting a ship in the middle of the ocean, need efficient and specific situational awareness tools. To achieve *Maritime Cyber Situational Awareness* (MCSA), the first step is a specific architecture to safely and efficiently gather metadata of interest in order to elaborate the perception of the situation [1]. Comprehending the situation, assessing the causality and the potential impact as well as the attacker's perception, is done in the second step. Tracking the situation and predicting its evolution is the final process known as the situation projection [2]. The final process, termed as situation projection, consists in tracking the situation and predicting its evolution. Some studies also add a fourth process, known as situation resolution [3]. When applied to cyber, this additional process would help decision makers to take the proper action, made on experience, threat intelligence, best practices and impact understanding.

Detection of cyber attacks is essentially achieved by the use of sensors, such as *Network Intrusion Detection Systems* (NIDS), *Host Intrusion Detection Systems* (HIDS) and by analysing logs of IT and OT assets. Most antivirus and NIDS solutions rely on misuse detection and the use of signatures to detect attacks. This detection scheme is only efficient in the case of known public attack vectors: in most cases, NIDS contribution to detect zero-day exploits is very limited. This lack of efficiency is better illustrated in the case of intrusion detection on specific protocols, because NIDS require specific pre-processing tools to understand the application layer, to decode it, and to produce relevant metadata. Spoofing those sensors, which is an efficient method for an attacker to retard detection, can be done in various ways. For example, NIDS sensors often use as signatures the same threat intelligence sources, therefore it is easy to identify their limitations or to produce a high level of false positives and overload sensors and *Security Operations Center* (SOC) analysts. Recent works

[1]https://www.marineinsight.com/know-more/10-worlds-biggest-container-ships-2017
[2]http://www.ics-shipping.org/shipping-facts/key-facts
[3]http://investor.maersk.com/releasedetail.cfm?ReleaseID=1031559
[4]https://www.portofsandiego.org/press-releases/general-press-releases/port-san-diego-releases-additional-information-cybersecurity

have presented promising results in intrusion detection in naval systems on board ships, based on data extraction method to perform anomaly detection [4], as well as in impact analysis to identify the propagation of threats within complex systems such as ICS and *Cyber Physical Systems* (CPS) [5]. The aim of this work is the detection and visualization of advanced navigation cyber attacks on maritime systems using contextual NMEA data analytics. We focus on NMEA 0183 protocol. A strategy is developed to enhance the detection of navigation spoofing attacks, assess possible physical impacts on board and support decision makers. The structure of the paper is as follows. NMEA 0183 standard, used in most navigation systems, is presented as well as its vulnerabilities in section 2. Methodology designed to improve advanced cyber attacks detection on a navigation system and also combines MCSA principles in order to allow decision makers to react in due time is detailed in section 3. Section 4 presents our conclusions and future research.

## II. Threats to the NMEA 0183 protocol

*National Marine Electronics Association* (NMEA) has designed a number of standards widely used in the maritime sector to achieve interoperability and enable information exchange across sensors and actuators made by different manufacturers by standardizing a common interface. NMEA 2000 standard was released to enhance the 0183 version, the latest being still widely used on most maritime navigation installations. All NMEA-compatible devices can send or receive and interpret data sent using the standard and gateways were also designed to enable exchanges between NMEA 0183 and NMEA 2000 networks.

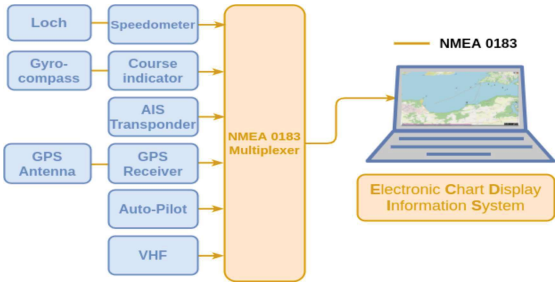



Fig. 1: Example of the NMEA-0183 Network.

On board sources producing and sending NMEA data on the bus/network can be depth sensors or echosounders, heading sensors, motion sensors, weather sensors and ECDIS. NMEA data can also depend on some external systems: they usually use radio receivers and antennas to catch Radio Frequency (RF) signals, demodulate and output them in the NMEA format. Those sources are mainly *Global Navigation Satellite System* (GNSS) receivers, such as the *Global Positioning System* (GPS), and surface information awareness tools, such as the *Automatic Information System* (AIS). Data consumers usually comprises physical actuators, such as automatic pilot and ECDIS. NMEA 0183 standard allows an unidirectional communication from a transmitter to one or more receivers, the data is transmitted at a low throughput. This standard is rather restrictive since only one transmitter is allowed per node. For several NMEA 0183 transmitters, a multiplexer is required to aggregate all these sources and output them to one or more displays as shown in figure 1. NMEA protocol has been retro-engineered over the past few years. It is composed of a variety of sentences, following a pre-defined and proprietary format, some manufacturers having defined their own sentences (Tables I and II).

| ID | Talker |
|---|---|
| AI | Mobile AIS station |
| EI | ECDIS |
| GA | Galileo |
| GP | GPS |
| II | Integrated Instrumentation |
| IN | Integrated Navigation |
| SD | Sounder Depth |

TABLE I: Examples of an usual NMEA talkers IDs.

| Code | Message Description |
|---|---|
| AAM | Waypoint Arrival Alarm (GPS) |
| GGA | Global Positioning fix data (GPS) |
| GLL | Latitude / Longitude data (GPS) |
| RMC | Recommended Minimum data (GPS) |
| RMB | Recommended Minimum data (GPS) |
| RPM | Revolutions (GPS) |
| RSA | Rudder Sensor Angle (GPS) |
| VTG | Track Made Good and Ground Speed (GPS) |
| ZDA | Time and Date (GPS) |

TABLE II: Examples of an usual NMEA message description.

The physical layer of the NMEA protocol does not provide any cybersecurity feature. For instance, data can be read as plain text as soon as access to the network is provided, and no integrity nor authenticity can be achieved. Those multiple flaws can be explained because, at first, the protocol was designed to be used on serial links, compromising on board sensors would then be a rather complicated task. Attack vectors are multiple: direct threats to ECDIS (ransomware, remote access) are a reality and some incidents have already occurred. Another plausible threat to maritime assets is a direct corruption of the data received by RF sensors, such as AIS or GPS, whether by spoofing or jamming signals and data. For civilian ships, detecting jamming or spoofing is tedious but have a tremendous impact: on a ship fully relying on its digital instruments for navigation, in case of poor watch standards or bad weather, a precise spoofing could lead to navigation discrepancies and, in narrow waters or channels, grounding. AIS is another maritime protocol which was not designed with cybersecurity in mind [6].

## III. Proposed detection methodology

For efficient detection of anomalies such as jamming and spoofing, a detection methodology and an architecture to retrieve data from a maritime navigation system and analyze it before sending to the ECDIS (Fig. 2) are developed. This architecture has evolved in several phases: the first step represents the most commonly found architecture on board a ship, which is a direct communication between navigation equipment without any cybersecurity component. The second step implements an external spoofing or jamming attack via an external RF transmitter, compromising the navigation system: this case is found when a civilian or military ship is navigating

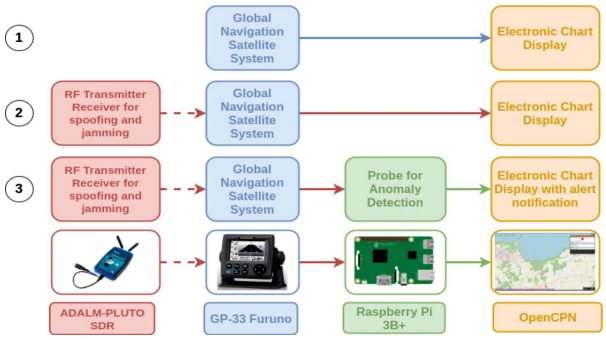



Fig. 2: Evolution of the architecture.

in crisis zones where access to GPS information can be denied. Finally, the third step of this architecture includes an additional embedded system that allows real-time analysis of NMEA traffic thanks to a dedicated sensor and returns data that can be interpreted by an ECDIS. Then we represent the implementation of our architecture with realistic devices and systems to perform all of our experiments. To carry out our detection strategy, various equipment (Fig. 2) are used

- *Software Defined Radio* (SDR) RF Transmitter Receiver: Adalm-Pluto used as a spoofing and jamming device,
- GPS Receiver: a Furuno GP-33 connected with a receiving antenna,
- A Raspberry Pi 3B+ board used as a probe to analyse in real time NMEA flow and to ensure anomaly detection,
- ECDIS (more precisely, an *Electronic Charting System*): a laptop with OpenCPN (a simulation software receiving and interpreting NMEA flow).

In our secured research environment, the system is set up to generate a false GPS satellite constellation using GPS ephemeris data (a file containing positions of satellites in time at regular intervals). As shown in Fig. 2, a RF transmitter & receiver to generate an external attack on the NMEA network is used. This system is able to momentarily collecting ephemerides and generating false constellation of satellites, according to a previously defined position. In this configuration, the system sends a stronger message than the one sent by the satellites, first jamming the GPS system and then spoofing a new position. Today, existing sensors for anomaly detection are often subjective or require extensive setup and expertise. The increasing affordability and reduction in size of relatively high-performance computing systems combined with promising results from anomaly detection related machine learning (ML) research, make it possible to create compact and portable systems for early anomaly detection. This work describes a Raspberry Pi Based portable, real-time data acquisition, and automated processing system that uses ML to efficiently identify and detect spoofing and jamming attacks. Several experiments have been carried out. Different recordings of GPS data on a 3D navigation simulator software set up for sailing in the bay of Brest (French West Coast) with different types of vessels and using a realistic behavior and cinematic have been realized. We then repeated the experiment in real conditions on board a motorized inflatable boat for several hours in the vicinity of Brest. All these data allowed us to build a reference model for the automatic learning algorithm. Representation of one of the cyber attacks that was realised on the GPS is depicted in Fig. 3.

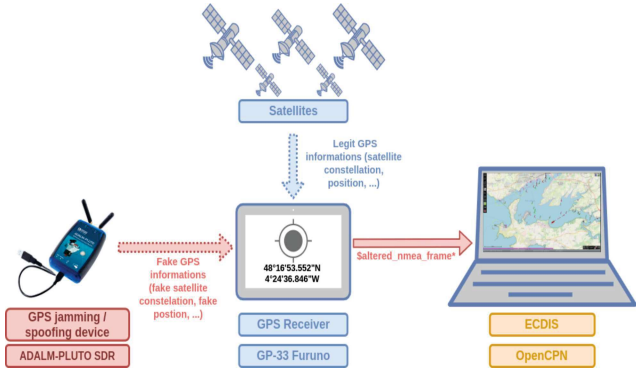



Fig. 3: Attack within the NMEA network by an external attacker.

Recent studies have shown the potential of mining traffic from the GPS in a variety of maritime applications [7]. However, prior works also show that GPS can be prone to erroneous messages due to device misconfiguration or cyber attacks which are critical to classify. By observing that a data-driven learning approach has proven effective way to collect and gather all of the NMEA flow, we conducted a study to understand how to make real-time anomaly detection on GPS message. To the best of our knowledge, there is no ML method that combines maritime data flow and MCSA principles. For the ML process, *One Class Support Vector Machine* (OC-SVM) was used because in our simulations and experiments the system used must be fast and easy to implement in a low-cost and low-performance detection embedded probe. As ML is data-driven, it requires substantial training data to be effective. Furthermore, the characteristics of data used for a problem domain, particularly how many candidates features the data has and how diverse they are, directly impact the applicability of a ML approach. We conducted a series of studies using the generated dataset to obtain the necessary insights about GPS data. This algorithm has been one of the most successful ML techniques that can be used in a variety of classification problems such as images classification, Bag-of-Word classifier or outliers detection. SVM is binary classifier, although it can be modified for multi-class classification as well as regression. Unlike logistic regression and other neural network models, SVMs try to maximise the separation between two classes of points. In particular, this method is widely used in anomaly detection [8], and several studies have been conducted on network traffic [9] [10] and OC-SVM can be employed as novelty detectors. For efficient detection of anomalies within the NMEA network traffic, pertinent features must used. Different features are extracted and normalised in order to compare them, and are listed as follows:

- GPRMC: *Latitude, Longitude, Speed-Over-Ground(knots), Track-Angle(degrees)*,
- GPGGA: *GPS-Quality, Number-of-SVs, HDOP, Orthometric-Height*,

- GPVTG: *Course (magnetic degrees), Speed (km/h).*

In each of the different scenarios, we have highlighted cases of GPS jamming and spoofing (by starting with brutal changes). SVM novelty detection algorithm is used to detect abnormal NMEA traffic by comparing normalised values nested in NMEA 0183 frames. We have normalised the data with a standard scaler method (which mean the data distribution will have a mean value 0 and standard deviation of 1). The reference learning model is based on 3 hours data recorded on the sea with a legitimate behavior and cinematics, represented in Fig. 4. This method is compared with another statistical one based on previous track angle and distance. Results are reported in Table III.

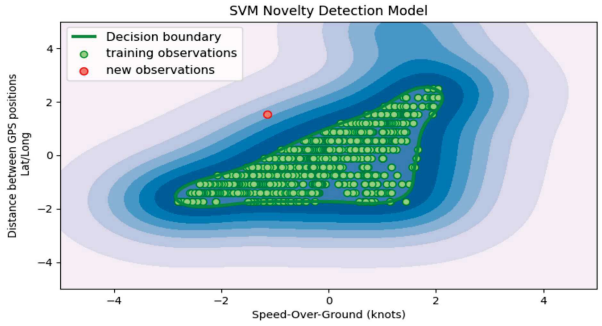
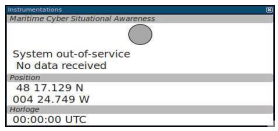


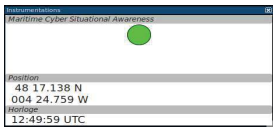

Fig. 4: Exemple of SVM model for novelty detection.

| Spoofing distance | Classification | Statistic method | OC-SVM |
|---|---|---|---|
| 100 yards | Detection Score | 89% | 100% |
| | False Positive | 1% | 0% |
| 10 yards | Detecion Score | 86% | 99.2% |
| | False Positive | 2% | 0% |
| 1 yard | Detection Score | 74% | 91.7% |
| | False Positive | 3% | 0% |

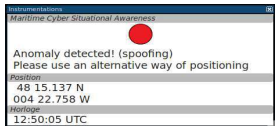
TABLE III: Classification Results for 3 distance attacks.



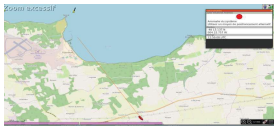

(a) Gray status.




(b) Green status.




(c) Red status.



(d) ECDIS Plugin with alert warning.

Fig. 5: Some examples of the navigation alert warning plugin.

To facilitate the understanding of this kind of interaction, we have created a plugin able to intercept the new NMEA frames embellished which the navigation system could potentially be. A ”green” status, which indicates that there is nothing abnormal given the reception of NMEA 0183 frames, the operator is informed that there is nothing to report at the navigation level. A ”gray” status: indicating that there is a problem of reception of the frames or a reception failure from the GPS or AIS systems with a specific message indicating the operator that there is a problem. And finally, a ”red” status: indicating to the operator that there is a potential cyber attack. An alert message is displayed to warn the operator that something is wrong and suggests he uses alternative positioning methods. Examples of warning on ECDIS using the proposed anomaly detection are depicted in figure 5. Classification results reported in Table III show the potential of our detection strategy.

## IV. Conclusion

In this paper, a machine learning approach for vessel-behavior-based GPS anomaly detection with data driven process is proposed. We perform a sequence of data analysis, starting with a dissector analysis of GPS traffic flows collected messages. The Cyber Situational Awareness proposed a way to alert on board operators of potential cyber attacks. A portable device that can perform a real-time anomaly detection strategy with a low-cost embedded system and easy to implement is designed. Cyber Situational Awareness methods can be more relevant than before to ensure cyber security on board the ship. As future work, we plan to conduct more global studies in order to identify learning models for several ships depending on the context, to use other ML process and to extend the experiment to the AIS pattern scheme.

## Acknowledgment

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 Region Bretagne.

## References

[1] O. Jacq, X. Boudvin, D. Brosset, and *et al.*, “Detecting and hunting cyberthreats in a maritime environment: Specification and experimentation of a maritime cybersecurity operations centre,” in *2nd Cyber Security in Networking Conference, IEEE (CSNet)*, 2018, pp. 1–8.

[2] P. Barford, M. Dacier, T. G. Dietterich, and *et al.*, “Cyber SA: situational awareness for cyber defense,” in *Cyber situational awareness*. Springer, 2010, pp. 3–13.

[3] B. McGuinness and L. Foy, “A subjective measure of SA: the crew awareness rating scale (CARS),” in *First human performance, situation awareness, and automation conference, Savannah, Georgia*, vol. 16, 2000.

[4] C. Boudehenn, J.-C. Cexus, and A. Boudraa, “A data extraction method for anomaly detection in naval systems,” in *Inter. Conf. on Cyber Situational Awareness, Data Analytics and Assessment IEEE (CyberSA)*, 2020, pp. 1–4.

[5] N. Pelissero, P. M. Laso, and J. Puentes, “Naval cyber-physical anomaly propagation analysis based on a quality assessed graph,” in *2020 Inter. Conf. on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. IEEE, 2020, pp. 1–8.

[6] M. Balduzzi, A. Pasta, and K. Wilhoit, “A security evaluation of ais automated identification system,” in *Proceedings of the 30th annual computer security applications conference*. ACM, 2014, pp. 436–445.

[7] D. Blauwkamp, T. D. Nguyen, and G. G. Xie, “Toward a deep learning approach to behavior-based ais traffic anomaly detection,” in *(DYNAM-ICS) Workshop, San Juan.*, 2018.

[8] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection: A survey,” *ACM Comput. Surv.*, p. 75, 07 2009.

[9] B. Lamrini, A. Gjini, S. Daudin, and *et al.*, “Anomaly detection using similarity-based one-class svm for network traffic characterization.”

[10] Q.-A. Tran, H. Duan, and X. Li, “One-class support vector machine for anomaly network traffic detection,” *(CERNET)*, vol. 310, 2004.