

Data Variety and Integrity Assessment for Maritime Anomaly Detection

Cyril Ray
Naval Academy Research Institute
Brest, France
cyril.ray@ecole-navale.fr

Abstract — The ever-increasing spread of mobile technologies and connected sensors necessitates the continuous updating of methods and techniques to cope with growing volume of data. While fast processing and data management has received lots of attention, data veracity and its assessment based on a large variety of contextual data seriously pose question. Indeed, sensors-based data collected through automated processes can be altered at every stage of their collection and process, accidentally or maliciously. In the maritime domain, several embedded sensors continuously report vessel's positions. Beyond known errors (human, misconfiguration), recent works have shown that falsification of such data is easy, and therefore could mask or favor illegal actions, lead to disturbance of monitoring systems and new maritime risks. This research presents maritime data quality issues and a methodological approach for modelling, analyzing and detecting such anomalies in data.

Keywords — *Data quality assessment, data falsification, maritime data, maritime cyber threats.*

I. INTRODUCTION

The maritime environment undergoes an ever-growing activity. In order to mitigate the risk of grounding or creating a collision, passive and active systems have been developed for mariners and set by international authorities. The Automatic Identification System (AIS) is an electronic system set on board vessels which transmits its location, amongst many other data. The AIS broadcasts, on a regular basis, 27 kinds of messages, each one having its own purpose in information transmission (positioning, nominative information, management...). The messages are openly broadcast on two dedicated Very High Frequencies (VHF). As messages are sent and received by vessel and coastal stations within the radio horizon (circa 40 nautical miles), it enables a better understanding of the surroundings for vessel and coastal states, thus supporting several uses such as fleet control, traffic control or boarding prevention, etc.

The number of messages is important: in a mean day, 19 million messages can be received in Europe from about 80,000 unique vessels [3]. With a great amount of, mainly spatial and temporal, but not only, data to process, issues linked to big data analyses arise. In particular, this research takes focuses on the veracity aspect. Indeed, sent messages contain errors (unintentional), falsifications (intentional) and undergo spoofing (intentional) due to the unsecured channel of transmission, and that weakens the whole system and the safety of navigation.

This work reports on the design and results of a methodology for the detection of AIS falsification. The objectives are the determination of the false messages in real-time and the improvement of both the effectiveness of the system as a security system and the maritime situational awareness.

II. A SYSTEM WITH WEAKNESSES

Three major cases of bad data quality can be distinguished: the errors (when false data in non-deliberately broadcasted), the falsifications (when false data is deliberately broadcasted) and the spoofing (when data is created or modified and broadcasted by an outsider) [5]. Data contained in AIS messages can be erroneous, falsified or spoofed for several reasons: there is no strong verification of the transmission, the transmission is done using a non-secured channel, some pieces of information might not be well known by the crew or the crew may want to hide some data from other people's knowledge. Those operations modify and handicap the understanding of the maritime traffic.

The errors, by nature unintentional, can be caused by transponder deficiency, a wrong input of manual data, an input of manual data of poor quality, erroneous pieces of information that come from external sensors, and can have an impact on the name of the vessel, its physical characteristics, the position or the destination for instance. Those pieces of information can then be false, incomplete, impossible according to the norm or impossible according to the physics (for instance a latitude field value shall be inferior to 90°). According to [7], circa 50% of the messages contain erroneous data.

A falsification is the fact to voluntarily degrade a message by the modification of a genuine value by a false value, or by stopping the broadcast of messages, made in order to mislead the outer world. Identity theft [8], the disappearances [9], the broadcast of false GNSS coordinates or the statement of a wrong activity [10] are types of falsification. According to [7], about 1% of the vessels broadcast falsified data.

The spoofing of messages is done by an external actor by the creation ex nihilo of false messages and their broadcast on the AIS frequencies [4]. Those spoofing activities are done in order to mislead both the outer world and the crews at sea, by the creation of ghost vessels, of false closest point of approach trigger, a false emergency message or even a false course (in the case of a spoofed vessel).

The whole chain of AIS data transmission can be affected by one of these three problems; from the GPS signal to human supervision, going through data transmission and distributed data processing and information systems involved. In order to formally identify these threats, an EBIOS risk analysis of the AIS has been performed [11]. This consists in the analysis of vulnerabilities, failures and risks associated with it, enabling the identification of issues that could actually emanate from the use of AIS. This method has been chosen for its

compliance to ISO norms and a list of circa 350 threat scenarios and a typology of anomalies has been established.

III. A VARIETY OF DATA

Depending on the objectives, variety of data can be more important than volume. Variety variations consider the usage of heterogeneous data sources, used to complement a core dataset in the understanding of a given situation. Indeed, data analysis at large, including detection of abnormal situations can be resolved or confirmed only by means of algorithms taking advantages of additional, complementary sources of information. This variety of data is absolutely required where (sensor-based) data with known issues of quality are analysed despite a lack “ground truth”. Beyond the understanding of data, the use of variations in variety which consists in progressively include additional sources is also mean of understanding quality of algorithms processing data (e.g. data compression, mining, visualisation).

While efforts have been initiated to centralise maritime data and information, most of the data are of heterogeneous type and format and still independently sourced and maintained [1]. These data can support maritime situational awareness as far as they are harmonised, properly combined, integrated, summarised, and possibly cleaned up from inconsistencies. Indeed, it is expected that the analysis and understanding of maritime activities cannot be deduced solely from vessels kinematics but would strongly benefit from complementary data of various types. However, the integration, combination (or fusion) of such data remains challenging (e.g., spatio-temporal alignment of data, fusion of data from different sensors, maritime anomaly detection, activity classification) and research is still needed to develop such efficient techniques.

In this research, ship information collected through the Automatic Identification System has been prepared together with correlated data aligned in space and time. The dataset has been carefully prepared and validated in order to offer the research community a set of heterogeneous real data to challenge, test and validate their research developments [2], and in the scope of this research to assess falsification cases of the AIS data.

The dataset¹ contains four categories of data: navigation data (vessel positions acquired automatically by an AIS receiver), vessel-oriented data (public, official nominative vessel position), geographic data (cartographic, topographic or regulatory context of vessel navigation), and environmental data (weather and ocean data from forecast models and from observations). It covers a time span of six months, from October 1st, 2015 to March 31st, 2016 and provides ship positions over the Celtic sea, the North Atlantic Ocean, the English Channel, and the Bay of Biscay.

IV. INTEGRITY ASSESSMENT

Since the AIS does not carry perfectly genuine data (beyond data errors), that those inaccuracies are not perfect and therefore are detectable, and that impacts on the real-world can be substantial, a set of objectives has been set for

detection of falsifications. Relying on the accurate understanding of the way the system is supposed to work, of its vulnerabilities and the errors and falsification that have been highlighted, these objectives include the creation of an attacking platform allowing the creation and the broadcast of falsified data, the modelling of a statistic and algorithm-based falsification detection mechanism, the creation of an information system for the real-time handling of data taking into account archived or forecasted data, and the modelling of risks that are induced by an inadequate use of AIS, as well as an assessment of the risks linked to AIS errors, anomalies, falsification or spoofing.

Intentional broadcast of false AIS information can be understood at both the physical and logical levels. The first approach focuses on signals transmitted by transponders while the second considers information exchanged where fraud and attacks can be identified by message-based data mining methodology to identify abnormal messages (and parameters). In our approach we are considering a combination of both analyses within a single information system.

A. Message-based analysis

Method for the integrity assessment of messages and the discovery of anomalous data is particularly based on spatial information, which is the cornerstone of AIS messages but not only as AIS also broadcast many contextual and control information along 27 messages [6].

Considering the data within the fields of the 27 AIS messages, four ways to discriminate the inner integrity of those data can be distinguished. The first way consists of the control of the integrity of each field of each message taken individually. The second way is at the scale of one single message, and assesses the integrity, in this very message, of all the fields with respect to one another. As there are 27 types of messages, messages of the same type have the same fields and it is thus possible to compare them, as time series, and assess their integrity, this makes the third way. Eventually, the fourth way is the comparison and integrity assessment of the fields of different messages. Indeed, although pieces of information can come from different messages, it is possible to assess their integrity as some fields are either the same or linked or comparable (i.e. id-based cross verification in order to link information received by different stations). Those four ways are referred as first-order, second-order, third-order and fourth-order assessments, respectively.

Depending on the type of messages assessed and the order of assessment, the number of items to check is fixed. We established a list of 935 integrity items for the 27 messages, and an ad-hoc nomenclature has been established so that each item can have a clear unique identifier. Predicate logic can present, under a formal form, the actions that lead on the integrity determination of an item in a rigorous and unambiguous way. Relying on three main elements: the data fields values, the syntax and the expert knowledge values, a logic-based formalism based on predicate logic has been chosen for item assessment. 666 have been implemented.

A falsification being the fact either to transmit erroneous data or to trick the system by making him behave in a way it is not supposed to, a falsification scenario can take numerous forms. Linking integrity assessment with falsification

¹ C. Ray, R. Dréo, E. Camossi, A.-L. Jousselme, Heterogeneous Integrated Dataset for Maritime Intelligence, Surveillance, and Reconnaissance (Version 0.1). Data set. Licence CC-BY-NC-SA-4.0. Zenodo. doi.org/10.5281/zenodo.1167594, February 2018

scenarios is essential for the identification of cyber threats relying on the AIS. A set of 23 algorithms (so called flags) has been designed for the identification of 4 falsification scenarios: falsified identity, positions, control messages, and saturation. Amongst these flags, let's cite for instance *f_quadruplet* that analyse if one element of identity quadruplet (MMSI number, IMO number, Callsign, Name) has changed along time. The flag *f_ubiquity* analyse if a vessel reports two distinct locations at the same time.

B. Signal-based analysis

We also studied physical characteristics of the signal which are intended to be integrated in the mining process. We considered five parameters. The first parameter is the power of the received signal and the four others are time-dependent and are relative to the shape of the signal. While these parameters cannot fully qualify ship's identity and presence, the regularity of these parameters can conversely help to identify inconsistent values.

C. Processing principles

A synoptic diagram of the proposed architecture can be found in the Figure 1. The AIS stream can be received from various sources and goes towards a centralised processing. The parser provides messages parameters (P_i). It includes a statistical analysis of messages (per ship identity, per type and at the global level) for the identification of AIS saturation. All this architecture is built around the central database (DéAIS DB) where historical data described in Section 3 are stored and where streamed data are processed asynchronously. The implementation of the database relies on the relational database model (postgres/postgis).

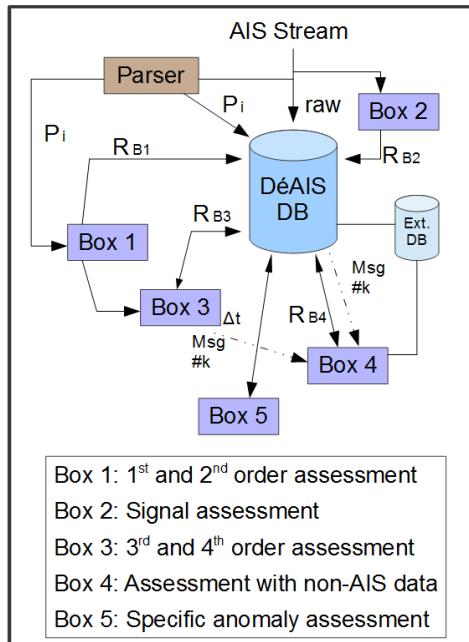


Fig. 1. Processing principles

Additionally, an online processing of the AIS stream has been also designed based on Flink [12] for the computation of black hole. As AIS coverage (and consequently black hole locations) by a receiver evolve continuously, this processing is essential to accurately detect falsified positions.

The data processing box number two corresponds to a signal processing for the determination of aforementioned characteristics. These data are stored in the database with the associated AIS decoded messages.

The data processing box number one is in charge of on-the-fly analysis of first-order and second-order data assessment, in order to have as output coefficients to store in the database. Similarly, the data processing box number three is in charge of the analysis of third-order and fourth-order data assessment, in order to have as output coefficients to be stored in the database. This part of the study, unless the previous, considers time series and needs to request historical data.

The data processing box number four will be in charge of integrity assessments between AIS data and external and aggregated data, (e.g. cartographic information, weather conditions, results of black hole computations). Finally, data processing box number five is in charge of running flags. Of course, the types of processing at this level vary according to the variety of information available and the requested anomaly scenarios.

V. CONLUSION

This article proposes a method for analysing message-based data using integrity of information as a key factor. Considering a variety of data sources, the approach described considers an assessment done on the message itself, on the message with respect to other messages, on the message with respect to external databases and on the signal itself with its physical characteristics. Applied in the context of maritime data, such an assessment is the consequence of the defects of the AIS system, transmitting erroneous and possibly falsified data. This method provides integrity-based predicates on data that are useful for the determination of erroneous and falsified data, leading to a risk assessment and alert triggering of maritime cyber threats. The approach is generic and could be transposed to many sensor-based systems.

ACKNOWLEDGMENT

This research is supported by The French National Research Agency (ANR) and co-funded by Defense procurement and technology agency (DGA) under reference ANR-14-CE28-0028 and labelled by French clusters Pôle Mer Bretagne Atlantique and Pôle Mer Méditerranée.

REFERENCES

- [1] Kalyvas C., Kokkos A., Tzouramanis T., A survey of official online sources of high-quality free-of-charge geospatial data for maritime geographic information systems applications, *Information Systems*, Volume 65, 2017, Pages 36-51
- [2] Ray, C., R. Dréo, E. Camossi, A.-L. Jousselme, and C. Iphar (2018). Heterogeneous integrated dataset for maritime intelligence, surveillance, and reconnaissance. *Data In Brief*, Accepted for publication
- [3] European Maritime Safety Agency. EMSA Facts & Figures 2016. Report. 40p. (2016)
- [4] Balduzzi M., A. Pasta, and K. Wilhoit. A security evaluation of ais automated identification system. In *Proceedings of the 30th Annual Computer Security Applications Conference*, pages 436–445. ACM, 2014.
- [5] Ray, C., Iphar, C., Napoli, A., Gallen, R. and Bouju, A.. DeAIS project: Detection of AIS Spoofing and Resulting Risks In: *The proceedings of OCEANS'15*. Genova, 2015

- [6] Iphar, C., Napoli, A., Ray, C., Data Quality Assessment For Maritime Situation Awareness, 9th ISPRS International Symposium on Spatial Data Quality (ISSDQ 2015), Volume II-3/W5, pages 291-296, La Grande Motte - France, 29-30 September 2015
- [7] Harati-Mokhari, A., Wall, A., Brooks, P. and Wang J., Automatic Identification System (AIS): a human factors approach. *J. Navig.* Vol 60(3), Cambridge University Press, 2007.
- [8] The Maritime Executive, Iran, Tanzania and falsifying AIS signals to trade with Syria. Published in The Maritime Executive, December 7th, 2012.
- [9] Windward, *AIS data on the high seas: an analysis of the magnitude and implications of growing data manipulation at sea*, 2014.
- [10] Kastilieris, F., Braca, P. and Coraluppi, S., Detection of malicious AIS position spoofing by exploiting radar information. In: *proceedings of the 16th international conference on information fusion*. Istambul, 2013.
- [11] Iphar C., Napoli A., Ray C., Alincourt E., Brosset D., Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety, 8 pages, ESREL 2016, Glasgow 25th–29th September 2016
- [12] Salmon, L., Ray, C., Design principles of a stream-based framework for mobility analysis, *Geoinformatica*, Special Issue on GeoStreaming, 25 pages, April 2016 (DOI 10.1007/s10707-016-0256-z)