Methodology for Real-Time Detection of AIS Falsification

Cyril Ray, Clément Iphar, Aldo Napoli

METHODOLOGY FOR REAL-TIME DETECTION OF AIS FALSIFICATION

C. Ray [(1)], C. Iphar [(2)], A. Napoli [(2)]

[(1)]Naval Academy Research Institute (IRENav), Brest, France
[(2)]MINES ParisTech, PSL Research University, CRC, Sophia Antipolis, France

ABSTRACT

The Automatic Identification System is an electronic system enabling vessels to send localization messages. Those messages are used for several uses such as fleet control, traffic control or boarding prevention. Sent messages contain errors, falsifications and undergo spoofing due to the unsecured channel of transmission, and that weakens the whole system and the safety of navigation. Beyond known errors, recent works have shown that falsification of AIS messages is easy, and therefore could mask or favor illegal actions, lead to disturbance of monitoring systems and new maritime risks. This paper presents the DEAIS project which proposes a methodological approach for modelling, analyzing and detecting such maritime events.

Index Terms— AIS Falsification, data mining, signal processing

1. INTRODUCTION

The Automatic Identification System is an electronic system enabling vessels to send localization messages. Those messages are used for several uses such as fleet control, traffic control or boarding prevention. 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 first 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.

As a first step, a risk analysis study of the Automatic Identification System has been done via EBIOS method. It led to the identification of circa 350 threat scenarios. A typology of anomalies has been also proposed, alongside with a methodology for anomaly detection.

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.

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. Integrity assessment is done within one lone message, between messages sent by the same vessel, and between messages sent by several vessels and include MMSI-based cross verification in order to link information received by different stations.

We also studied physical characteristics of the signal which are intended to be integrated in the mining process. We currently 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.

2. 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) (Ray et al., 2015). 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 (Harati-Mokhtari et al., 2007), 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 (The Maritime Executive, 2012), the disappearances (Windward, 2014), the broadcast of false GNSS coordinates or the statement of a wrong activity (Katsilieris *et al.*, 2013) are types of falsification. According to (Harati-Mokhtari *et al.*, 2007), 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 (Balduzzi, 2014). 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 cape (in the case of a spoofed vessel).

The whole AIS data transmission system is displayed in Figure 1, where (1) is GPS data transmission, (2) is AIS-SAT transmission, (3) and (4) display VHF marine transmission, (5) shows digital transmission and (6) depicts human supervision. All the chain of AIS data transmission can be affected by one of these three problems.

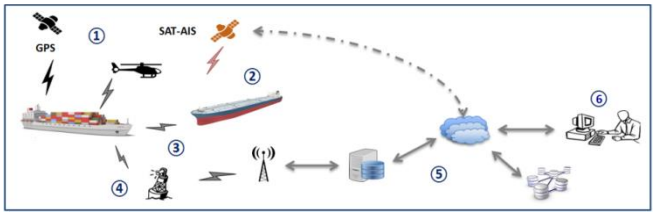

Figure 1 AIS data transmission

As mentioned, problems with the AIS can be understood at the physical and logical levels. DEAIS project considered these two levels for the identification of falsifications. Next sections summarise our risk analysis (section 3) and the methodology proposed for signal analysis (section 4) and message integrity assessment (section 5).

3. AIS EBIOS RISKS ANALYSIS

The EBIOS method (ANSSI, 2010) has been created by the ANSSI (French National Agency for the Security of Information Systems) and is used in both the public and private sectors. It is an approach of risk evaluation which clarifies the entities of the system, their vulnerabilities, the inventoried threats, and contributes in the assessment of the right level of security (compliant with ISO norms 27001, 27005 and 31000).

We conducted an EBIOS analysis of the AIS in which we compiled all known information about the system in order to obtain a complete understanding of it. The application of the EBIOS method on the AIS led to the construction of several tables that enable us to consider several risk levels and the importance to put in place security measures on certain areas which have been found out as particularly vulnerable according to threat scenarios and possible threat sources. These tables describe:

- The essential goods (e.g. dynamic AIS data)
- The essential functions (e.g. transmit AIS data)
- List of support goods (e.g. surveillance centre organisation)
- Identified threat sources (e.g. rival vessel or ship-owner)
- Dread events (e.g. position determination is impossible)
- Threats scenarios (e.g. identity data change on the transponder)

The study led to the identification of more than 350 threat scenarios. Such a study influences the choice of detection algorithms to elaborate first. In particular, it has motivated the study of the AIS signal.

4. SIGNATURE IDENTIFICATION THROUGH MAGNITUDE AND TEMPORAL CHARACTERIZATION

At the physical level, falsification can be identified by signal analysis. For instance, destination masking or disappearances which are also a kind of falsification, as ships turn off their AIS transponder in order to hide some of their activities can be studied by exploiting radar information (Katsilieris *et al.*, 2013). Another approach considers radiolocation of signals to confirm the existence of a real ship and its approximate localization (Papi *et al.*, 2014).

In order to identify a ship's signature or possible falsifications, pertinent features extracted from each frame of the input AIS signals have been studied (Ray *et al.*, 2016). An experimental campaign of reception of frame AIS was conducted in the bay of Brest. Sixteen recordings of five minutes each were collected corresponding to 10 000 usable AIS frames. Each sample is also 5 minutes with a center frequency of 162 MHz and a bandwidth of 100 kHz. It allows recording simultaneously both frequencies of the AIS.

Five features were measured for every AIS frame (Figure 2). The top graph represents the temporal evolution of the frequency modulation of the AIS signal and the down graph represents its power. The first feature is level of the received power, which will allow estimating the broadcast power knowing the distance. The four others temporal parameters are relative to the shape of the signal and are: rise time (Fig. 2-2), fall time (Fig. 2-4), and times before (Fig. 2-1) and after demodulation (Fig. 2-3).

Decoded frames, power of the received signal, and temporal characteristics of the associated signals were then gathered into a geographical database (cf. section 6) to realize a reference database of ships' id and allow statistical studies.

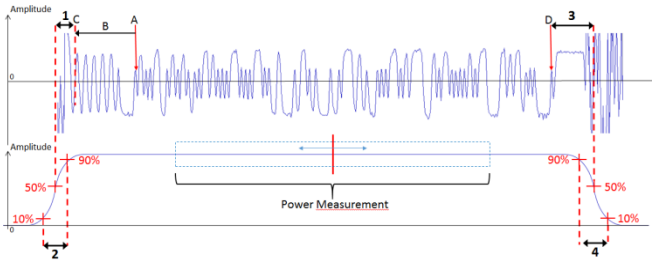

Figure 2 Analysis of a received AIS frame

The study of these different parameters highlights particular values which will allow us to relate with ships' identity signature. For example, Figure 3 proposes a representation of time before modulation in the form of box-plot. The X-Axis corresponds to the MMSI number of ships, the time before modulation being on the Y-Axis. For each ship, the values of "time before modulation" are in a given interval, values that seem different from a ship in the other one.

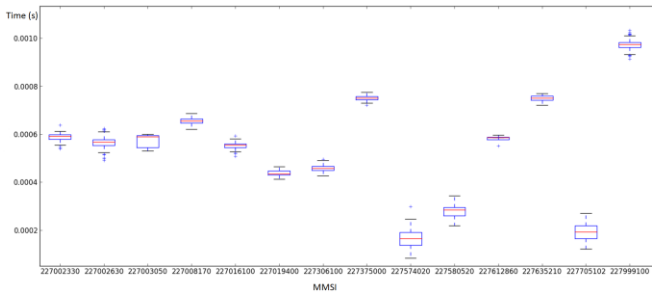

Figure 3 Box plot "Time before modulation" distribution for 'class A' AIS systems

While temporal characterization cannot fully qualify ship's identity, the regularity of these parameters can conversely help to identify inconsistent values. In addition, the study showed that repeaters exhibit specific patterns easily recognizable.

The perspective concerns the improvement of this methodology with the definition of additional signal parameters and the integration of data mining techniques combining signal features with static and dynamic information provided by AIS messages as described in the following section.

5. AIS MESSAGES INTEGRITY ASSESSMENT

At the logical level, fraud and attacks can be identified by message-based data mining methodology to identify abnormal messages and navigational behaviours (Iphar *et al.*, 2015). For instance a ship navigating with a MMSI number which is not the real one, allocated and internationally recognized, can be identified by a correlation with official ships' registry and confirmed by a real-time monitoring of AIS identities at the worldwide level.

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, message of the same type have the same fields and it is thus possible to compare them 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. MMSI-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 item to check is fixed. We established a list of 669 items for the 27 messages, and an ad-hoc nomenclature has been established so that each item can have a clear unique identifier.

An integrity coefficient is assessed by order, i.e. a coefficient is computed for first-order items, another one for second-order, and so on, depending on the type of assessment wanted. Then a global coefficient can be computed, by weighting the order-based coefficients and other results from other methods as desired.

The perspective concerns the implementation of the methodology together with first detection algorithms. Amongst current developments, we are considering black hole detection in AIS transmission in order to identify possible masking. The following section introduces the architecture designed for the detection of AIS falsification.

6. ARCHITECTURE FOR DATA PROCESSING

A synoptic diagram of the proposed architecture can be found in the Figure 4. The signal can be received from various sources, the parser provides messages parameters, the data processing of the signal provides some signal parameters and two different steps of data processing. All this architecture is built around the database in order to fill it and use it for knowledge discovery. Two implementations are currently developed in parallel; one based on a relational database (postgres/postgis) and a second one based on Flink (Salmon et al., 2015) to cope with larger volume of data.

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 NMEA message and decoded AIS frame.

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, needs to request historical data.

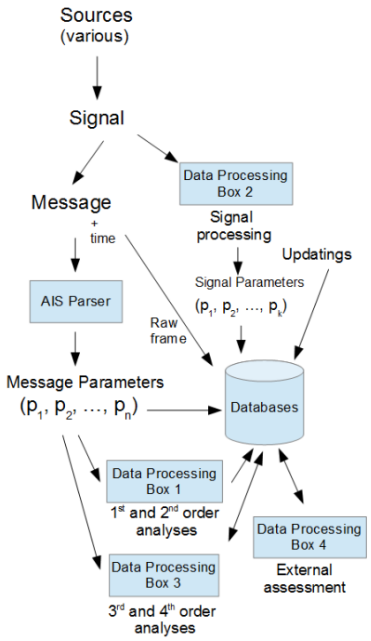

Figure 4 Proposed architecture

In the database itself, each new entry will lead to the creation of a new item (i.e. a new line), with as attributes shall have: a unique identifier, the time of reception, the raw frame, all message field values and the various coefficient obtained through assessments (the four orders and the signal parameters).

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, black hole computations). Of course, the types of processing will vary according to the type of external information available, and it is not possible to have a strictly defined process in this part. A list of assessment items can be created for each new database when its specifications are known (i.e. its fields, their precision, their source and reliability), and two similar databases (i.e. on the same subject) are likely to have two different lists of assessment items as their specifications will differ. Updating of the external databases will, in certain cases, be necessary, as to ensure information is not outdated and data quality assessment is reliable.

7. CONCLUSION

This article proposes a method for analysing AIS data using integrity of information as a key factor, with database storage of information and 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. Such an assessment is the consequence of the defects of this system, transmitting erroneous and possibly falsified data. This method is meant to be implemented and to provide integrity-based confidence coefficient on data that will be useful for the determination of erroneous and falsified data, leading to a risk assessment and alert triggering in a decision-support system and in the end provide an additional tool for the enhancement of maritime security.

8. ACKNOWLEDGEMENT

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

REFERENCES

ANSSI, 2010.*http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.*

Balduzzi, M., Pasta, A. and Wilhoit, K.,A security evaluation of AIS automated identification system. In: *Proceedingsof the 30th annual computer security applications conference.* ACSAC 2014, New Orleans, USA, December 8-12, 2014.

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.

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

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.

Papi, F., Tarchi, D., Vespe, M., Oliveri, F., Borghese, F., Aulicino, G., and Vollero, A., Radiolocation and tracking of automatic identification system signals for maritime situational awareness. Radar, Sonar & Navigation, IET, 9(5):568–580, 2014.

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.

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)

The Maritime Executive, Iran, Tanzania and falsifying AIS signals to trade with Syria. Published in The Maritime Executive, December 7th, 2012.

Windward, *AIS data on the high seas: an analysis of the magnitude and implications of growing data manipulation at sea*, 2014.