Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety

Clément Iphar, Aldo Napoli, Cyril Ray, Erwan Alincourt, David Brosset

Risk Analysis of falsified Automatic Identification System for the improvement of maritime traffic safety

C. Iphar & A. Napoli
CRC, MINES ParisTech, PSL Research University, Sophia Antipolis, France
C. Ray, E. Alincourt & D. Brosset
Naval Academy Research Institute (IRENav), Brest, France

ABSTRACT: On board vessels, the Automatic Identification System sends and receives localization messages and enables vessels to better understand their surroundings. Initiated by the Safety Of Life At Sea convention, this system is used for navigation security and safety, boarding prevention, fleet control or traffic control. Some of the messages broadcasted contain errors, falsification and undergo spoofing that weaken the capacities of the system to achieve its goals. This paper presents a risk analysis study of the Automatic Identification System that leads to the identification of circa 350 threat scenarios. A typology of anomalies is proposed, alongside with a methodology for anomaly detection. The objectives are the determination of the false messages and the improvement of both the effectiveness of the system as a security system and the maritime situational awareness.

1 INTRODUCTION

Crossroads of international issues, the maritime domain is facing growing human activities. The ocean has a central place in some particular domains such as goods transportation and energy transportation where 90% of the global traffic is done by sea. The traffic generated by maritime activities (including fishing, sailing and cruising) is important and still increases. This ever increasing traffic leads to navigation difficulties and risks in coastal and crowded areas where a large amount of vessels exhibit different movement objectives which can be conflicting.

The international traffic is globally dense, but some regions (such as Europe or South-Eastern Asia) and some locations (such as straits or canals) have a particularly dense traffic. For instance Malacca strait and the Suez canal have respectively a yearly traffic of circa 50,000 and 20,000 vessels. Moreover this traffic sometimes takes place in hazardous areas of the world. For the two former examples, as for 2016, the Malacca strait is subject to rampant piracy (The Jakarta Post, 2015) and the Suez canal is located on one side of the Sinai peninsula, which is subjected to an armed conflict (ACLED, 2016).

For the enhancement of the security and safety of navigation, several electronical systems have been designed, such as radar or Long-Range Identification and Tracking system. One of those systems is the Automatic Identification System (AIS), which broadcasts messages from a ship or a coastal base station to all surrounding ships and coastal base station within the radio horizon range.

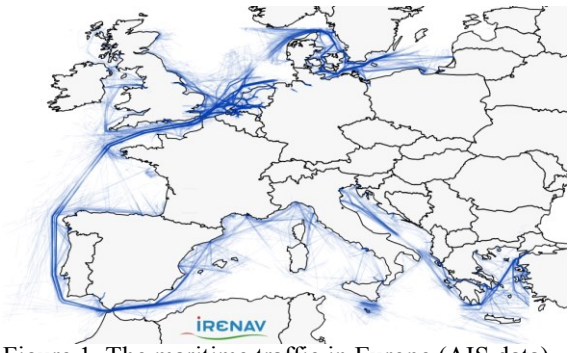

Figure 1. The maritime traffic in Europe (AIS data)

In this paper we present a risk analysis of the AIS system supported by the EBIOS methodology and an anomaly typology. After the introduction, section II presents the Automatic Identification System, principles and weaknesses, then section III details the EBIOS risks analysis conducted on this system. Section IV presents the anomaly typology developed. Section V finally proposes the data processing needed for anomaly discovery and an exemplification of integrity assessment in the case of AIS messages.

2 THE AIS

2.1 *The principles of the system*

The AIS was put in place in 2000 by the International Maritime Organization and its characteristics and

deployment schedule are defined in the Safety of Live at Sea convention (IMO, 2004). This convention, initiated two years after the sinking of the RMS Titanic in 1912, aims at defining the minimal requirements to which every vessel belonging to a signatory country should comply with. The convention deals with a large scope of subjects which range from the construction of vessels to the way radiocommunications shall be done.

One of the themes of the convention is the safety and security of maritime navigation, and it is in this scope that the system was created, as it provides a real-time spatiotemporal positioning of a vessel to every vessels and shore station located in its radio range of action.

Not all the vessels from the signatory countries are concerned with the AIS regulation, as the convention states that "All ships of 300 gross tonnage and upwards engaged on international voyages and cargo ships of 500 gross tonnage and upwards not engaged on international voyages and passenger ships irrespective of size shall be fitted with an automatic identification system" (IMO, 2004).

The system uses transponders to send messages through Very High Frequency marine bandwidth on two worldwide dedicated frequencies: 161.975MHz and 162.025MHz. The transponder is linked with a Global Navigation Satellite System (GNSS) which computed its location as well as external sensors (electronic compass for instance) in order to fill in several data fields within the messages. The AIS can also transmit to satellite the messages (AIS-SAT), that makes possible to keep a track of a vessel even beyond the radio horizon. One kind of message (number 27) is shorter than all other messages and is especially dedicated to satellite reception.

The system, albeit being mainly initially designed for security purposes, the AIS has alternative uses such as the prevention of boarding (alarm triggering when a small closest point of approach is computed), investigation in case of accident, control of fishing fleets, cargo fleets, global traffic, traffic in specific hazardous areas, maritime safety (for a state), aid to navigation or search and rescue operations.

Indeed, some examples of the use of AIS for alternative purposes can be found in studies in several subjects such as accident investigation (Wang et al., 2013), the detection of near miss collision between vessels (Zhang et al., 2015), the behaviour understanding in a waterway through traffic monitoring (Xiao et al., 2015) or the mapping of the fishing effort using AIS data (Natale et al., 2015).

Due to the variety of communications, there are 27 different kinds of messages. Position report messages, information messages and check messages are the three main groups of messages (Tunaley, 2013). All 27 kinds of messages are standardized by the International Telecommunications Union (ITU) and have its particular outline with data fields, each one being allocated a certain number of bits. The information within each field can take several forms: boolean, text, number representing a physical quantity, number representing a choice in a given list. The content of the messages do vary largely from one message to another: in a position report message the data fields are the speed, the position and the cape, amongst others, while an aid to navigation message will display the type of beacon, its name or the location of a hazard.

2.2 *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), circa 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).

3 AIS EBIOS RISKS ANALYSIS

3.1 *The EBIOS*

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, mainly in France but also out of France. 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 needed by the specification the security means which must be put in place. The EBIOS analysis is compliant with ISO norms 27001, 27005 and 31000. The following figure shows the 5-module procedure of the EBIOS analysis.

The first module, "Context Study", is about the identification of the system. The knowledge about the system is gathered, the architecture of the Information System is studied, as well as the technical and regulation constraints, the equipment and software used, and the human organization around the systems and which interacts with it.

The second module is defined as the "study of dread events", and permits to estimate the potential events that could affect an essential good and to clarify the associated risks. The users of the Information System provide their needs in terms of security (confidentiality for instance) with respect to the impacts they consider as inacceptable (people's security or financial cost for instance).

The third module, "Study of the threat scenarios", takes an inventory of the threats according to the technical architecture of the Information System. A list of vulnerabilities and kinds of attacks is set with respect to the materials, the network architecture and the used pieces of software, would it be caused by accident or not, would it be caused by a human factor or not.

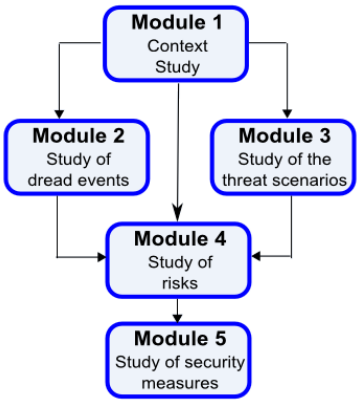

Figure 2. The EBIOS procedure

Then the next module, "Study of risks", evaluates the security needs for the identified threats, in order to highlight the risks against which the Information System shall be protected. Objectives appear and form a bill of specification on security that will convey the level of importance given to the threats in proportion with the required level of security.

The last module, "Study of security measures" specifies the advised security measures, the expected level of demand (which compromise should be chosen: the acceptation, the reduction or the rejection of the risk), the planning of the implementation of the measures and evaluates the benefits in terms of risks of the then applied measures.

3.2 *The analysis outcome*

We conducted an EBIOS analysis of the AIS, in this analysis we compiled all known information about the system in order to obtain a complete analysis of it, with circa 350 threat scenarios identified.

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.

3.2.1 *Context Study*

In this part, essential goods are identified (Tab 1), they are the different kind of information within the AIS. Then, essential functions are identified (Tab 2), which correspond to elementary indispensable functions of the system. Support goods are defined (Tab 3), taking into consideration both the vessels and shore-based stations characteristics.

Table 1. The essential goods

Static AIS data: no evolution over time expected
Dynamic AIS data: positioning and route-based data
Other AIS data: text and binary messages, weather

Table 2. The essential functions

Transmit AIS data
Receive AIS data
Visualize data by table or card
Transponder configuration (possibility to change)
Analyse, treat and store AIS data (for surveillance centre)
Determine its position (whatever the positioning system)

Table 3. List of support goods

INTERNAL	EXTERNAL
AIS chain	GNSS
Surveillance tools	AIS data supplier (incl. AIS SAT)
Vessel Organisation	Public or private IP network (incl. the Internet)
Surveillance Centre Organisation	
Vessel premises	
Surveillance Centre premises	

3.2.2 *Study of dreads events*

A total of 17 threat sources have been identified, and presented in the following table (Tab 4)

Table 4. Identified threat sources

Vessel's crew
Rival vessel or ship-owner
Pirate
Operator of the collecting system
Administrator of the collecting system
Data supplier
Contributor of the data supplier
Manufacturer or installer of the material
Hacker
Hacktivist
Criminal organisation
State organisation
Malicious code from unknown origin
Natural phenomenon
Natural or health disaster
Animal activity
Internal event

The following table (Tab 5) displays the synthesis of dread events, with 20 events, 11 of them being of level 3 for intolerable seriousness, 5 of level 2 for major seriousness and 4 of level 1 for minor seriousness. The levels are defined with both seriousness and plausibility to occur scales, also gratuated with minor, major and intolerable levels. For instance, a major level of risk would be reached by either events of intolerable seriousness with both insignificant and minor plausibilities, or events of major seriousness with minor, major and intolerable plausibility, or events of minor seriousness with intolerable plausibility.

Table 5. Synthesis of dread events

3	Dynamic data are not available
3	Dynamic data are false
3	Other AIS data are false
3	AIS data transmission is not working
3	AIS data transmission is not reliable
3	AIS data reception is not working
3	AIS data reception is not reliable
3	Position determination is impossible
3	Position determination is incorrect
3	Information visualisation is not available
3	Information visualisation is incorrect
2	Static data are accessible to an opponent
2	Dynamic data are accessible to an opponent
2	Other AIS data are accessible to an opponent
2	Data analysis, treatment or storage is corrupted
2	Transponder configuration is corrupted
1	Static data are not available
1	Static data are false
1	Other AIS data are not available
1	Data analysis, treatment or storage is not available

3.2.3 *Study of the threat scenarios*

The following table displays the most plausible threats scenarios. 8 scenarios are presented, all of intolerable seriousness (level 3).

Table 6. Most plausible threats scenarios

Use of the computer for other tasks
Use of the system for sending and receiving short messages (addressed or broadcasted)
Branching of a non-legitimate input
Identity data change on the transponder
Wrong update of route-based and cargo data
Unexpected case according to the norm
Maritime traffic surveillance for villainous ends
Injection of false data hijacking report tools

3.2.4 *Study of risks*

The following table (Tab 7) displays the 11 risks of intolerable level highlighted by the study.

Table 7. Intolerable level risks identified

Risks linked to the dynamic data availability
Risks linked to the dynamic data integrity
Risks linked to the other AIS data integrity
Risks linked to the transmission function availability
Risks linked to the transmission function integrity
Risks linked to the reception function availability
Risks linked to the reception function integrity
Risks linked to the positioning function availability
Risks linked to the positioning function integrity
Risks linked to the visualisation function availability
Risks linked to the visualisation function integrity

This analysis enables us to have a great overview of the risks linked to the use of the AIS, however this analysis must be strenghtened by the discovery of anomalies in actual data. Such a study needs a characterizaion and a classification of the different kinds of possible anomalies in the case of AIS messages, and it is the topic of the following part.

4 TYPOLOGY OF ANOMALIES

In the EBIOS analysis presented in the previous section, a large amount of the identified risks deal with integrity, and more particularly some deal with data integrity issues. Considering integrity as one of the data quality dimensions, the risk assessment through AIS data shall take into consideration the AIS data quality. It is the knowledge of anomalous data and the determination of outliers that will lead us to the data quality assessment. In the case of AIS messages, the anomaly assessment is quite complex as it involves several disjoint concepts. This is the subject of this section.

Anomalies are not all the same of a kind, their spectrum is wide and a classification in families and subfamilies is not trivial. In the scope of the study of AIS messages and according to the research presented in (Roy et Davenport, 2010) and (Roy, 2008), a classification in four main families has been chosen: the behaviour, the content, the lawfulness and the quality. It is presented in figure 3.

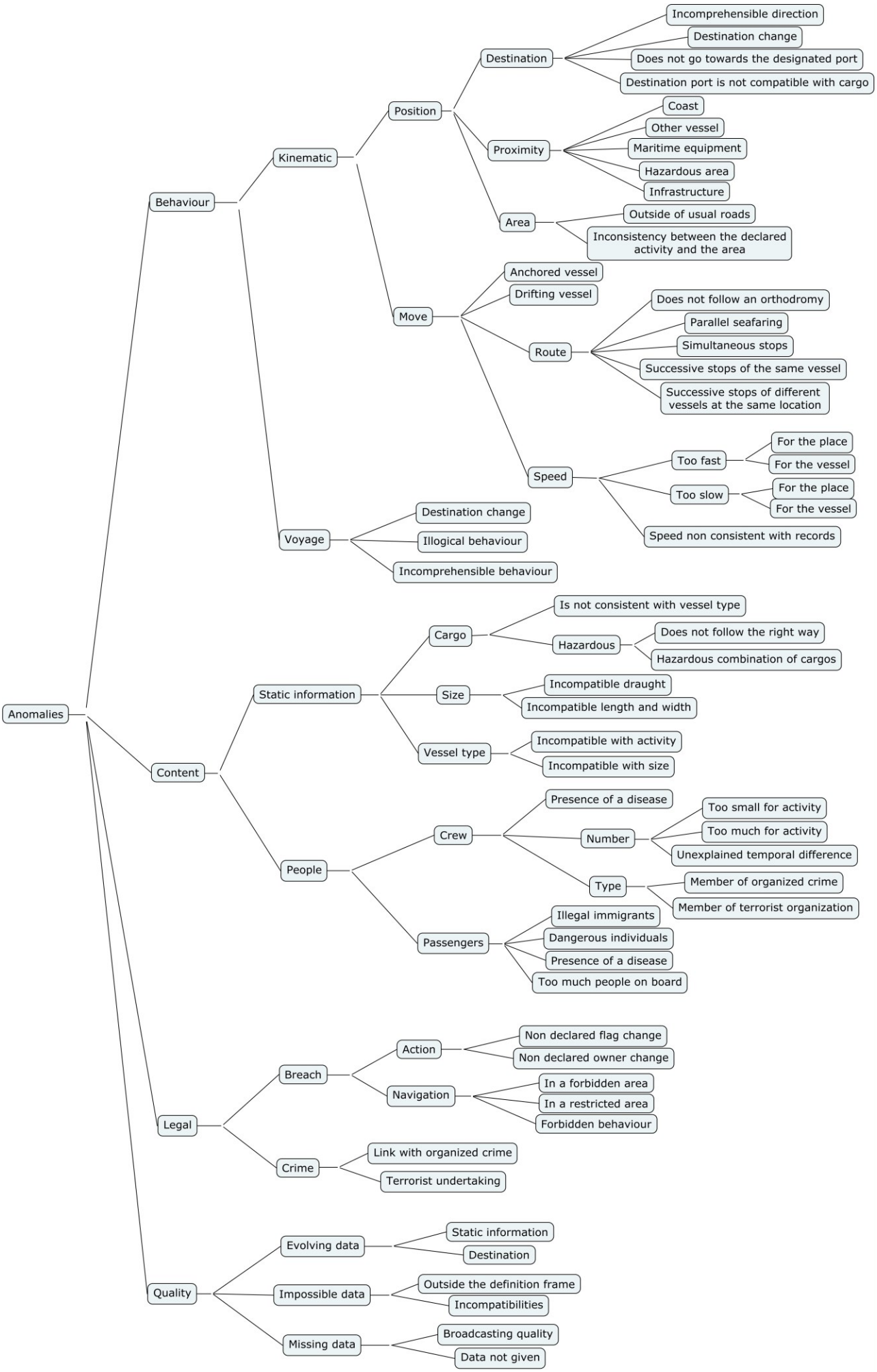

Figure 3. Typology of anomalies in the AIS case

By its size, the behavioural anomalies family is the largest. Kinematic anomalies are the main subfamily, with on the one hand the position-based (about either the destination or the area of location) and on the other hand the movement-based (about either the route or the speed, with or without engine on) anomalies. The other subfamily is route-based anomalies, including unexpected change of destination, illogical or non-understandable behaviour.

As for the content anomalies, two subfamilies are distinguishable: the anomalies in the content of the message itself that do not come under the vessel's behaviour (such as static data, data which usually do not change over time) and anomalies about the people on board (crew or passengers).

The lawfulness anomalies can be split in two subfamilies: criminal issues (terrorism or organised crime) and breach-level issues (such as forbidden behaviour, undeclared change of flag for instance).

About data quality anomalies are distinguished the unexpectedly changing data, the impossible data so as the piece of information is out of the possible scope for it, or impossible with respect to others pieces of information (when a comparison is possible), and missing data due to poor signal reception or voluntary lack of data providing.

5 EXEMPLIFICATION

5.1 *Anomaly detection methods*

Anomaly detection is used in the field of data analysis, with the three elementary steps that are: (1) the identification of the "normality" characteristics by computation and determination of data classical signatures (for instance trajectory clusters in the AIS messages case), (2) the determination of metrics for the computation of the distance of the studied behaviour from the standard behaviour and (3) the determination of threshold criteria for the distance to the standard behaviour, allowing the normality, the abnormality, the magnitude of normality and the magnitude of abnormality for a datum.

The determination of a normal behavioural pattern can be done using diverse methods such as statistical methods, neural networks or machine learning (Martineau et Roy, 2011), that will depend on the nature of the data to study: the created patterns can be a sequence of events, a cluster or a statistical distribution. Statistical methods are fitted with the data in which extreme values are anomalous (the speed for instance), and do not work in the cases where the anomalies are evenly distributed. Neural networks are fitted for the discovery of hidden patterns with complex boundaries but their black box behaviour and their need of a learning phase. The principle of machine learning is to automatically learn complex structures and take data-based decisions. Amongst those methods are genetic algorithms (Shapiro, 2001), Bayesian networks (Friedman et al., 1997) or clustering algorithms (Jain et al., 1999).

The distance determination will depend on the type of data and distances such as Euclidian distance in dimension 1 (in the case of speed), Euclidian distance in dimension 2 (in case of localization coordinates with small distance), orthodromic distance (in case of long distance localization coordinates), mean, Hausdorff or Fréchet distances (in the cases of computation of distance between trajectories), or edition distance (in the case of distance with textual data, for the field "destination" for instance). The choice of the right distance for each field is of major importance in the anomaly detection process.

The third step in this anomaly detection is the thresholding for outlier determination in different cases, among which those aforesaid. This will be the purpose of future work measures.

5.2 *Message correctness assessment*

We conducted a preliminary study between October 2014 and March 2015 with an antenna located in Brest, France. We received and gathered AIS messages and led the first analysis tasks. Over the six months, 20,544,654 messages were received by the antenna (it represents a mean value of more than one message per second), out of which 1,316,689 did not comply with the ITU standardized outline for the particular message. It represents a ratio of 6.41%.

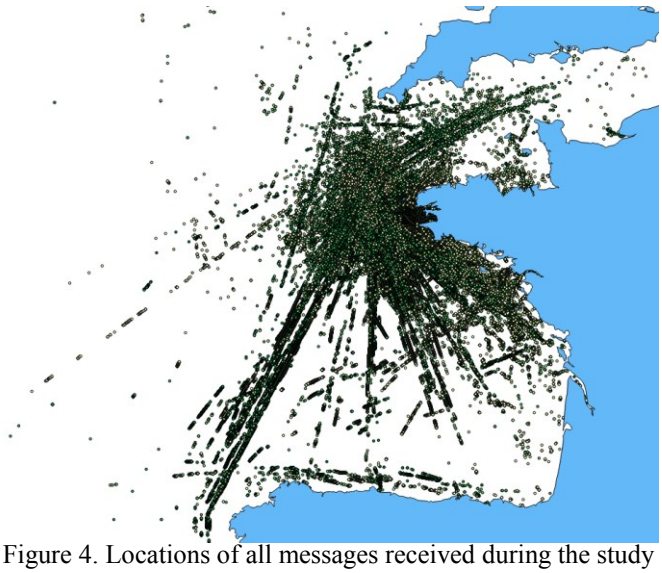

Figure 4. Locations of all messages received during the study

The message number 1 (standard position report for class A vessel) is the more transmitted message, with 62% of all messages, out of which 4.6% are not correct. High rates of not correct current messages (both high rate and current message is considered when prevalence is superior to 1%) are found for message number 9 (standard search and rescue aircraft position report) with 99.8% of not correct messages (2.6% prevalence) and message 21 (Aids-to-

Navigation report) with 39.9% of not correct messages (2.0% prevalence).

Moreover, 13 of the 27 message types have a frequency less than 0.01%, and the relevance of a study on such a little amount of message is weak. 7 message types were received less than 10 times, out of which 2 were never received over the six months span of the study.

5.3 *Message integrity assessments*

The first and the simplest way to assess the integrity of an AIS message is to consider the value of their fields. All 27 messages have an outline defined by the ITU in (ITU, 2014), in which all bit is allocated to a specific field. All fields have a predetermined number of bits assigned, in a predetermined order, and the value within the field has a possible range of possibilities. For instance the field latitude shall refer to a value between -90° and +90°. As the latitude field in the message number 1 gives a value in ten thousandths of minute of arc, and given that negative values (for the southern hemisphere) are given with the 2's complement, the actual value of the field shall be either inferior to 54,000,000 or superior to 80,217,728. Any value between those two numbers (except the default value) is an anomaly.

The very same conduct can be used for every field of every message. We inventoried 183 different field value assessments over the 27 messages.

In addition, it is possible to compare the fields of a single message within themselves, the fields of several messages of the same kind (sent by the same vessel or by several vessels) between themselves and the fields of several messages of the different kinds (sent by the same vessel or by several vessels) between themselves. A total number of respectively 94, 114 and 278 different integrity assessments for the three kinds of comparison have been inventoried. Their study will be the purpose of future work.

6 CONCLUSION

This paper introduces the AIS principles and vulnerabilities that lead to errors and falsifications of the message. These errors and falsifications hamper the view of the maritime traffic, both for the mariners (for their immediate surrounding) and the local authorities (for the understanding of the activity off their coasts), causing a degradation of the maritime navigation safety. An EBIOS risks analysis has been conducted that highlighted the dreads events and the threat scenarios of the AIS when failing to transmit correct data. The concept of anomalies in the maritime environment of the broadcasting of AIS messages have been illustrated by a typology and anomaly detection techniques have been presented. An exemplification of AIS correctness and integrity assessment is proposed, showing the large scope of research that has to be done in order to assess the reliability of AIS, for the improvement of the maritime situation awareness and thus the improvement of the safety of navigation.

ACKNOWLEDGMENTS

Research presented in this paper is supported by The French National Research Agency (ANR) and co-funded by DGA (French Armaments Procurement Agency) under reference ANR-14-CE28-0028. The project is also labelled by French clusters Pôle Mer Bretagne Atlantique and Pôle Mer Méditerranée.

REFERENCES

ACLED. 2016. Real-time Analysis of African Political Violence, January 2016, *Conflict Trends* (NO. 45). Armed Conflict Location & Event Data Project.

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

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

Friedman, N., Geiger, D. & Goldszmidt, M. 1997. Bayesian Metwork Classifiers. In: *Machine Learning, Vol. 29*, (pp. 131-163).

Harati-Mokhari, A., Wall, A., Brooks, P. & Wang J. 2007. Automatic Identification System (AIS): a human factors approach. *J. Navig. Vol 60(3),* Cambridge University Press 11, 2007.

IMO. 2004. *International convention for the safety of life at sea*. International Maritime Organization.

ITU. 2014. *Recommendation ITU-R M.1371-5 (02/2014) – Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band*. International Telecommunication Union.

Jain, A.K., Murty, M.N. & Flynn P.J. 1999. Data Clustering: A Review. In*: ACM Computing Surveys*. *Vol. 31(3)*, september 1999.

Kastilieris, F., Braca, P. & Coraluppi, S. 2013. Detection of malicious AIS position spoofing by exploiting radar information. In: *proceedings of the 16th international conference on information fusion.* Istambul, 2013.

Martineau, E. & Roy, J. 2011. *Maritime Anomaly Detection: Domain Introduction and Review of Selected Literature.* Defence R&D Canada, Valcartier, 2011.

Natale, F., Gibin, M., Alessandrini, A., Vespe, M. & Paulrud, A. 2015. Mapping Fishing Effort through AIS Data. In : *PloS ONE Vol. 10(6)*.

Ray, C., Iphar, C., Napoli, A., Gallen, R. & Bouju, A. 2015. DeAIS project: Detection of AIS Spoofing and Resulting Risks In: *The proceedings of OCEANS'15.* Genova, 2015.

Roy, J. 2008. Anomaly detection in the maritime domain. In C. Halvorson, D. Lehrfeld & T. Saito (eds.), *Optics and Photonics in Global Homeland Security IV*.

Roy, J & Davenport, M. 2010. Exploitation of Maritime Domain Ontologies for Anomaly Detection and Threat Analy-

sis. In: *Proceedings of Waterside Security Conference,* Carrara, Italy, November 3-5. 2010.

Shapiro, J. 2001. Genetic Algorithms in Machine Learning. In: G. Paliouras, V. Karkaletsis, & C. Spyropoulos (Eds.), *ACAI'99*, *LNAI 2049* (pp. 249–257).

The Jakarta Post. 2015. Malacca Strait rampant with pirates. Published in The Jakarta Post, January 2nd, 2015.

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

Tunaley, J.K.E. 2013. Utility of Various AIS Messages for Maritime Awareness. In: *proceedings of the 8th ASAR Workshop*. Longueuil, Canada. 2013.

Wang, Y., Zhang, J., Chen, X., Chu, X. & Yan, X. 2013. A spatial-temporal forensic analysis for inland-water ship collision using AIS data. In: *Safety Science Vol. 57* (pp 187-202).

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

Xiao, F., Ligteringen, H., van Gulijk, C. & Ale, B. 2015. Comparison study on AIS data of ship traffic behavior. In: *Ocean Engineering Vol. 95* (pp. 84-93).

Zhang, W., Goerlandt, F., Montewka, J. & Kujala, P. 2015. A method for detecting possible near miss ship collisions from AIS data. In: *Ocean Engineering Vol. 107* (pp 60-69).