Detection of false AIS messages for the improvement of maritime situational awareness

Clément Iphar, Aldo Napoli, Cyril Ray

Detection of false AIS messages for the improvement of maritime situational awareness

Clément IPHAR, Aldo NAPOLI
MINES ParisTech – PSL Research University
CRC – Centre for research on Risks and Crises
Sophia Antipolis, France
{clement.iphar, aldo.napoli}@mines-paristech.fr

Cyril RAY
Naval Academy Research Institute (IRENav)
Brest, France
cyril.ray@ecole-navale.fr

***Abstract*—The Automatic Identification System (AIS) was initially designed for safety and security of navigation purposes. However it was progressively also used for other objectives, such as surveillance, and thus led to the discovery of behaviors such as the falsification of the AIS messages by people that have been carrying out illegal activities and will to keep their activities up in an hidden way. In addition, the messages contain erroneous data and undergo spoofing attacks. The paper introduces the quality dimensions of data that shall be used in a quality assessment of AIS messages, in order to point out the dubious ones. The principles of a methodological approach for the detection of such data errors and falsifications are introduced.**

Keywords—Automatic Identification System; maritime domain awareness; data falsification; data quality dimensions

I. INTRODUCTION

Besides its primordial role in the development of ecosystems, its wildlife richness and being one of the last places on Earth mainly unknown to humankind, the World Ocean is an important place in the economy of the world, as some activities, such as transportation of goods, fishing, sailing and cruising occur at sea and impact (in a more or less important way) the worldwide economy. For instance, 90% of global goods transportation and energy transportation are done by sea, and millions of people work on sea-related activities (fishermen, aquatic farmers, crews on board, workers on shore). The shipping areas are more and more crowded due to the even increasing traffic [1], leading to risks in coastal areas, harbors, and densely exploited maritime roads, as all vessels try to optimize their journey, creating conflicts in areas where a large amount of vessels are gathered.

Rules of navigation were put in place in order to reduce the number of collisions at sea, that endanger the workers and the passengers and can possibly be dangerous for the environment, the economy and cause important money losses for companies involved in such accidents.

Some states put in place surveillance systems when they had the will to improve the security and safety of the navigation off their coasts, in order to point out some hazardous areas and suspicious ships which could have some illegal interests, and enhance the maritime domain awareness. One of those system is the Automatic Identification System (AIS), which transmits messages to other vessels (that are fitted out) and to shore-based stations, using dedicated radio channels in the VHF band. The messages are broadcasted in a non-secured channel, so it is possible to gather them, as harbors, Vessel Traffic Services (VTSs) and Internet dedicated websites (such as marinetraffic.com) do.

Several systems exist alongside with AIS, such as radar or LRIT (Long-Range Identification and Tracking), and all are meant to be complementary. For instance, AIS has, with respect to radar, a wider range of detection, and enables the user to get rid of masks potentially created by the land in coastal areas. However, the AIS system remains used at the crew's discretion, as the signal is sent by a dedicated device on-board the vessel. Moreover, the messages can be falsified, errors can be committed when the user fills in information and the message can be spoofed. The fact to process the data in a mathematical way could bring some information on the integrity and reliability of data, by the computation of a message-based coefficient, which would rate information. This is done because people, on board the vessels or in VTSs take decision on the basis of the available information they have. So in this scope of decision-making situations, the knowledge of the quality of the information they handle is of paramount importance.

II. THE AIS SYSTEM AND ITS WEAKNESSES

A. The Automatic Identification System

1) Genesis and concerned vessels: The Automatic Identification System (AIS) was put in place by the Safety Of Life At Sea (SOLAS) convention, in its 2002 version [2]. This convention, initiated in 1914 by the sinking of the RMS Titanic two years beforehand, has the purpose of defining the minimal requirements to which every vessel from signatory countries should comply with. The SOLAS convention deals with a lot of subjects, ranging from the construction of vessels to the way radio-communications shall be done.

One of those subjects is the security and safety of maritime navigation, and the AIS system was created in this scope, in order to provide real-time spatiotemporal positioning of a vessel to the other vessels and to shore stations located in its radio range of action (so no further the radio horizon).

Some ships from the signatory countries are concerned by this regulation. Indeed, the SOLAS convention, in its fifth chapter, nineteenth rule, paragraph 2.4, 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" [2]. The deadline for a vessel to be equipped depends on its type and range from 2002 for new ships to the 2008 for non-international travelers vessels.

2) The transmission mode of AIS: The transmission of AIS is done in the Very High Frequency (VHF) bandwidth (which ranges from 30 to 400 MHz), and more precisely in the dedicated Marine VHF bandwidth (consisting in four distinct bandwidth which have a total range of 2.225MHz), as VHF band is split in sub-bands which are used for specific and various applications, such as search and rescue, private or military applications, radio-astronomy, amongst others. Two worldwide dedicated wavelengths are used to transmit AIS data : 161.975MHz and 162.025MHz. In order to transmit and receive AIS signals, some dedicated devices have been put in place since the introduction of the system. Four kinds of devices can be distinguished: class A transponders, class B transponders, multi-channel receivers and radio scanner receivers.

One of those subjects is the security and safety of maritime navigation, and the AIS system was created in this scope, in order to provide real-time spatiotemporal positioning of a vessel to the other vessels and to shore stations located in its radio range of action (so no further the radio horizon).

Class A transponders equip all the ships that are legally required to use the system by the SOLAS convention. They can receive and transmit simultaneously on both channels, and have full capability and options for the users. Class B transponders equip all the ships that are not legally required to use the system but which owners wish to transmit their information and receive information from the others. As their capabilities and options are reduced, their price is lower. Those transponders can receive and transmit on both channels simultaneously. Multi-channel receivers and radio scanner receivers cannot transmit information but they can receive, simultaneously on both channels or only on one channel at a time respectively. Those receivers are used by ships wishing to improve their situational awareness at sea.

The AIS transponders must be linked to a GNSS antenna for positioning reports, and can be linked to an ECDIS (Electronic Charts Display Information System) for the visualization of surrounding traffic and improvement of maritime situation awareness.

Today, two types of transmission are available: terrestrial (i.e. direct reception from emitting device) and by satellite (i.e. the broadcasted signal is received by a dedicated spacecraft). However, at first, the system was only terrestrial, with transmission occurring from one vessel to another, or between a shore station and a vessel, in a range of distance which is limited by the curvature of the Earth (circa 40 nautical miles in optimal conditions [3]). The development of satellites enabled to receive messages even far from the coast line, as it uploads and stores the received messages then download information as soon a coast line and a shore station is reached. The development of Internet gave an even more important step forward in the knowledge of maritime situation as websites display AIS information from all over the world. So where ships previously disappeared beyond the skyline from a terrestrial point of view, they can now be tracked in the whole world by every person who can access the Internet network.

3) The various types of messages: Because of the fact that communications can be various, 27 types of messages were created, each one of them suitable in a particular situation. As stated by [4], the most used messages are the numbers 1, 3 and 5, that are respectively scheduled, special and static position reports for class A transponders. There are standard messages (for class A and B transponders, aircrafts and satellite transmission for spatiotemporal position report), aid-to-navigation messages, safety messages, binary messages, among others. Depending on its type, the message can take from one to five time slots of transmission [4]. Moreover, the position report messages are sent every 2 to 12 seconds, the gap between two messages depending on the speed of the vessel. The outline of the messages is strictly defined and can be found in [5]. According to [3], in a common day, 22 000 vessels send about 400 000 messages.

4) The emission of the signal: The emission is made during time slots, with a length of 26.67ms, each message being sent uses between one and five of those time slots. There are 2250 of those slots in a minute of time. In order to have a scheduled, organized and ordered sending of the messages, several protocols were put in place.

The most of those protocols is the SOTDMA, which stands for Self Organized Time Division Multiple Access. This protocol enables to manage operations in an automatic way, and conceived for sea communication networks. The stations (vessels or shore stations) manage their own time slots reservations for the subsequent messages, and they can modify their own reservations in case of conflict (for instance a meeting with a new station). This protocol is used by class A transponders.

5) The content of the messages: Of course, the content of a message widely varies according to the type of the message, and a position report message will not have the same fields as an aid to navigation message has. A position report (messages 1, 2 and 3) has such data as the user, the navigation status, the rotation rate, the speed, the longitude, the latitude, the course, the true heading, among others. An aid to navigation message (number 21) would display the type of aid, the name of the aid, a longitude, a latitude, a reference point, among others, and a message for satellite transmission (number 27), has simplified data, such as Maritime Mobile Service Identity (MMSI) number, navigation status, speed and course as well as message 1, but have simplified longitude and

latitude, and no other data of interest in order to save place and have a simple transmission.

B. The weaknesses of AIS

1) The limits of the system: While initially designed for security and safety of the navigation purposes through the SOLAS convention, this system is used another way by some people. Indeed, some additional purposes such as investigation in case of accident, traffic in dangerous areas, search and rescue, control of fleets (cargo, fishing) and of global traffic. In the end, several kind of people can use this system, such as coastal authorities for law enforcement, Maritime Rescue Coordination Centers (MMRCs) for search and rescue operations, mariners on board for their own safety of navigation and ship owners for fleet tracking.

2) The errors in the messages: A part of the information contained in AIS messages are entered manually by the crew, both at the initialization of the system for permanent data (such as the name of the vessel for instance) and at every new journey for journey-related data (such as the destination for instance), some of the pieces of information can be erroneous. A study of such erroneous data can be found in [6]. They can be done by underestimating the importance of a correct fulfillment of the system or by ignorance and, as being errors, are not intentional.

Each human-filled field is subject to errors, as well in static data such as identification number of the ship, type of the vessel, name of the vessel, the physical characteristics (length, beam, draft) that in dynamic data such as the position (latitude, longitude), the navigation status, the estimated time of arrival or the destination. According to the study of [6], both static and dynamic data are subject to errors.

Thus, the MMSI number is false is an estimated 2% of the cases [6]. Four numbers appeared in a regular way: “0”, “1”, “999999999” and “1193046”, the latter being guessed as being the initialization number of some kind of transponder. Also, the type of the vessel is often unclear. As 6% do not define a type at all, 3% define their vessel simply as “vessel”. The problem of definition is larger, as it lies on the perception of the person entering information: a case of three ferries, perfectly identical vessels, was shown, were the three given types were “High Speed Craft”, “Passenger” and “Cargo” [6]. The name of the vessel is another issue, as 0.5% does not have a registered name, and some others exceed the allocated space in the field, which is 20 characters.

The position is also subject to problems, as it was noticed that circa 1% of ships had a latitude value (in absolute value) superior to 90° or a longitude value (in absolute value) superior to 180°. The destination is not clearly filled in in almost half of the cases. The use of a vague name, of a country, of an abbreviation, a black space, or jokes is widespread, such as “not available”, “not defined”, “null”, “Atlantic ocean”, “to hell” or “anywhere but here”. Physical characteristics of vessels also suffer from several lacks of consistency [6].

3) The falsifications in the messages: The falsification of AIS messages consists in the fact to modify the message they send, or the fact to stop the transmission of the message, in the particular goal to mislead people that could receive these messages.

Identity theft, destination masking and disappearances are kinds of falsification. Identity thefts occur when a vessel takes the identity (i.e. the MMSi number) of another one. Hundreds of vessels are dissimulated this way [7]. As an exemple, Iran used to falsify the identity of some vessels in order to trade with Syria [8]. Destination masking, when made on purpose, is a falsification [7], as it creates a voluntary lack of information. As for disappearances, the fact to cut off AIS transmission could indicate a will to hide some illegal activities, such as trade illegal goods on coast or with other ships, or fish in unauthorized areas [9]. One vessel out of four cuts off its AIS transponder for at least 10% of the time, taken into account the times of lacking GNSS coverage. The fact to cut off the transmission is also a way to protect oneself from the pirates that could have an Internet access to check the vessels they could attack. Moreover, the fact that cutting off the AIS is very simple and the physical freedom to do so is let to mariners favors this kind of behavior.

4) The spoofing of messages: The fact to spoof messages consists in an action from an actor which is external to the vessel, done in order to mislead both the crew on board and the outside world (MRCCs for instance) on the behavior of a vessel.

Some of those spoofing behaviors are presented by [10], with for instance a false closest point of approach alert. Such an alert occurs when two spatiotemporal trajectories of vessel are crossing, in order to prevent a boarding. A false alert consists of the creation of a ghost vessel that would cross the trajectory of another one, forcing the real one to change its heading, and could hypothetically be guided to hazardous locations. In addition, [10] implemented a program which created a ship having a spatiotemporal trajectory which was displaying a word in the Mediterranean Sea.

Another example of spoofing is presented in [11], in which a pirate GNSS signal is emitted, with a higher power than the genuine one, and covering it. In this case, the system is misled on the positioning aspects, it transmits a false message and forces the pilot to maneuver to return to the believed right cape, but in fact moves away from the initial destination.

III. THE APPROACH

As the purpose is to ascertain the vessels from which the received messages are false, falsified or spoofed, several approaches can be used, such as signal-based or message-based. This research concentrates on a message-based approach, with an interest in inner information that is present

in the messages. Indeed, messages are made of raw data which are, once refined, source of information on all the relevant AIS-linked fields of information. It is therefore important to handle the characteristics (among them their quality dimensions) of data and information in order to assess the quality of messages. The quality dimensions and the methods used for assessment are meant to change depending on the type of message and on the type of study (one message alone or a group of messages for instance).

IV. Information and data in AIS messages

A. Internal and external quality

The qualities of a message can be divided in two parts, the external quality, which is the quality from the point of view of the user and the internal quality, which is the qualities from the point of view of the supplier. External quality covers ease of use, robustness, openness, reliability, accuracy, conformity to the expectations, among others, so external quality can be considered as being the fitness for use. Internal quality lies on concision, cohesion, clarity, generality and simplicity, among others [12].

Internal quality can be described by answering the question: how can I measure the quality of my data and how can I signify it? It is the intrinsic quality of a data set established through rules. It is an absolute technical quality.

External quality can simply be defined as the fitness for use, which worth answering the question: what are the needs of the user on data quality and information quality and how can I give it in order to prevent them from having an abusive use of them? External quality is more difficult to assess because of the multiple and various needs, and the purpose of linking data and their use, data producers' concerns and users' expectations. External quality is the ability to fulfil a particular need, and is a relative use quality.

In case of AIS messages, the assessment of internal quality is important in order to ascertain the genuineness and truthfulness of a message, rather than an external quality assessment, as it depends on the receiver's experience, which is difficult to ascertain as it vastly varies from one to another.

B. Some quality dimensions of data

1) Accuracy: Considering an attribute *a* of an entity *e*, its standard value is *v*. The accuracy of a v' value would be the degree of closeness of (v'-a-e) with respect to (v-a-e). If the value v' = v, the accuracy is maximal and the value is said to be correct. As it is possible to determine accuracy, it is also possible to determine inaccuracy, which would be the degree of difference between the actual value and the correct value. One problem of the determination of accuracy is the notion of correct value. Sometimes, the correct value may not be defined in a unique way, or it can be undefined. Even when a standard value is possible, the calculation of the accuracy may not be obvious, for instance with the words, or the binary values. Sometimes the determination of accuracy with numbers can cause some problems. So the quantification of accuracy or inaccuracy of a value is a nontrivial task [13].

2) Precision: The precision of data does not directly refer to data but to the model in which data is displayed. It is a measurement of the degree of detail of the classification of possible values for data. For instance, when a temperature is measured, is the value rounded at the unit level, or at the one-tenth of degree level; or when a height is measured, it is using feet or inches; or when a color scale is used, does this scale have 16 or 256 possible values.

3) Reliability: The reliability of data in a database is defined in [14] as "a measure of the extent to which a database can be expected to exhibit the externally-observable structural properties specified for a database". It is the process of validation that leads to reliability, i.e. the checking that the values in the base obey to the rules defined in the outline. It is a measure of robustness, which is the assessment of absence of system failures.

4) Currentness: This term is used as defined by [13]. As for the currentness, a datum, by its nature, represents a value at a given time. As most objects evolve with time, the value can evolve as well. A datum true at a given time t is either up-to-date or out-of-date at another time t'. The change over time of a value creates inaccuracy in data, and the notion of currentness can measure the degree of how far out-to-date the datum is [13]. This property can be expended to an entire database for the measurement of its currentness. False data is neither up-to-date nor out-of-date. A distinction must be done between data evolving by nature (such as the speed of the vessel), data likely to evolve (the navigation status), data that may change (such as the usual geographical area of navigation), data unlikely to change (the name of the vessel) and permanent data (the length or draught of a vessel). Given the age of a datum, the probability for it to remain up-to-date after a certain time will depend on which category it belongs, among other parameters.

5) Completeness: The completeness of a database represents the proportion of triplets where a value which is supposed to exist is actually filled in. It can be seen in a binary mode, i.e. yes if every single possible value is filled in and no otherwise; or in a measure of completeness by measuring the fraction of filled in fields with respect to the highest possible number of filled in fields [13]. In databases, a special element called null is used when an attribute in non-applicable (for instance the destination when a ship is docked), when the attribute is of unknown applicability (the relevance of the destination field requires the navigational status field to be filled in), or when the attribute is applicable but the value unknown (for instance the navigational status, always

applicable). Completeness is linked to the fact for a database to contain all the relevant data [15] for a given use. The duplication is the fact, for a database, to have identical triplets, or to have triplet with the same entity and attribute, but different values [13]. Some of those triplets can be irrelevant. The proportion of duplicate values can be measured as a characteristic of the database.

6) Consistency: In a database, the values of the different terms must agree. The consistency is part of this agreement. A consistent database should have consistent values within, as well as unnecessary null values should be avoided. The consistency of the database can be measured in a binary yes/no mode, and the database will be consistent is all the constraints are fulfilled. A measure of the consistency can also be done by the measure of the fraction of consistent triplets in the database. The development of data dictionaries is one part of the consistency improvement, helping to the creation of translation rules between different representations of the same data or of closely linked data [15].

7) Integrity: A measurement of integrity can be done considering all the previous qualities, and empowering the measure of consistency by the use of the temporal dimension, which involves the recording of insertions, deletions and modifications of items.

C. A measure of coherence in information

A common definition of coherence is presented in [16] as "when we gather information from less than fully reliable sources, then the more coherent the story that materializes is, the more confident we may be, ceteris paribus". Some factors can affect the confidence we have in a piece of information. Three can be distinguished: how surprising is the information, how reliable are the sources and how coherent is the information [16]. For instance, if pieces of information are both halfway surprising and halfway coherent, the global confidence will rely on the reliability of the sources: we will be more likely to increase our degree of confidence as the source is more referenced as truth-teller rather than randomizer. Similarly, if the pieces of information are halfway coherent and come from halfway reliable sources, we will rely on the surprise factor in order to assess the degree of confidence, which will be as high as the piece of information is more rather than less expected.

In the case of AIS messages, there are a lot of sources, both vessels and shore-based stations, with a wide spectrum of types of messages, where some message can be of confidence but with a low quality. An ascertainment of the confidence in individuals messages could be done sorting data by MMSI number (i.e. by user).

D. The quality dimensions in the case of AIS messages

In the following table I, comparisons are made between relevant information and data quality dimensions and their application in the case of AIS messages.

TABLE I. APPLICATION OF QUALITY DIMENSIONS

Quality dimension	Application of the dimension
Accuracy	Definition of standard values, for instance in the case of the speed of vessels
Precision	Definition of latitude and longitude, as seen above
Reliability	General coherence of messages with respect to ITU recommendations
Currentness	Use of time stamps of messages
Completeness	Definition of all the fields that should be filled in depending on the message, then computation of their ratio
Consistency	Coherence of information within a message or between messages
Integrity	Enhancement of consistency with temporal recording of actions

V. PROPOSED METHODOLOGY

A. Hypotheses

In this environment, a hypothesis could consist in being able to ascertain the trust in a message by analyzing its data through the scope of the quality of its inner information. At several levels, such an assessment could be done using the data within and by processing it. As the AIS system is not reliable and used by many people for various purposes, the awareness of the users on the proper nature of the system shall be clear.

The integrity of data must be investigated, as some information is clearly impossible (out framed GNSS coordinates for instance) or physically incompatible (two vessels with the same number at the same time, a speed that does not match with the type of the vessel). Such a determination of the reliability of information can be done using a scale of belief, disbelief and uncertainty based on a statistical study [17].

The trust in a user will depend on the past behavior of this user, as the opinion about the source is a key part of trust [18]. This part is mainly made by VTSs and harbors, with the blacklisting of suspicious vessels. The users themselves can be various, with various degree of a priori confidence (between a fisherman and a MRCC member for instance).

B. Exemplification of the methodology on a message

As the purpose is to detect vessels that are undergoing attacks or that are emitting false messages on purpose, a means for the assessment of such vessels must be developed.

As information comes from messages, it is possible to treat and analyze every message independently from the others, a group of messages as a whole, or a single message with respect to a group of messages.

Data contained in AIS message are various, and the messages themselves are numerous. Such an analysis would bring a numerical value on a message, a group of messages or a message with respect to a group of messages.

TABLE II. AN AIS MESSAGE NUMBER 1

Field indicator	N° of bits	Field name
01A	6	Message ID
01B	2	Repeat indicator
01C	30	User ID
01D	4	Navigational status
01E	8	Rate of turn
01F	10	Speed over ground
01G	1	Position accuracy
01H	28	Longitude
01I	27	Latitude
01J	12	Course over ground
01K	9	True heading
01L	6	Time stamp
01M	2	Special maneuver indicator
01N	3	Spare
01O	1	RAIM-flag
01P	19	Communication state

For instance, a message number 1 contains, according to [5], the information contained in table II. Message number 1 is a position report message, sent in a case of scheduled position report by a class A transponder. This message follows the exact same scheme as messages number 2 and 3, used respectively for assigned scheduled position report for class A transponders and special position report as a response to interrogation by a class A transponder.

Several assessments can be done in the only message 1 case. The accuracy can be partly judged by the 01G field, while the precision assessment will concentrate on fields such as 01H and 01I for position, but also 01F, 01E, 01J and 01K for current attitude. The reliability will be assessed by the comparison of the values in the message with reasonably possible values. This will ensure the proper reception of the right message.

The currentness of the message shall be determined using 01L field, while consistency and integrity will be assessed by the studies of the fields independently and with respect to one another, e.g. besides saying that 01H and 01I fields actually correspond to possible coordinates, comparing them in a spatiotemporal way with 01D, 01E, 01F, 01J, 01K and 01L to ensure that the behavior is coherent.

Inspired by the Information Theory developed by Shannon in [19], a mathematical processing of data can be done in order to assess the usefulness of a message, its reliability and its integrity.

The integrity of data is of major importance, and can be assessed for a single message (integrity of the information within), for a group of messages (integrity between the data between the messages) and for a message with respect to a group of messages.

A coefficient for data integrity could then be computed, and with a specified threshold, detect the dubious messages on the basis of data quality, with many parameters taken into account, at several levels: internal to the system, a single message, a group of messages, or external to the system. Such a coefficient would be an indicator for data quality assessment.

The assessment of a single message would be the integrity of the data that can be found in the coherence of its inner information, the coherence of a message from a ship can be assessed by comparison with all the other messages sent beforehand by the same vessel, or by different vessels following the same path. The fact to receive or not to receive an expected message would give additional information on the reliability of the system.

However, such an assessment needs the definition of several metrics for the measure of distances, which would be specific to each field. This will be the purpose of future work.

VI. CONCLUSION

This paper introduces issues on AIS and the way to use information and data quality dimensions to assess the truthfulness and the genuineness in a message, as various problems of errors, falsification and spoofing of the messages actually occur. In this scope, such an assessment of data quality using accuracy, precision, reliability, currentness, completeness, consistency and particularly integrity would bring the detection of erroneous, false or spoofed messages easier, and therefore enhance the maritime situational awareness of maritime actors, and thus security and safety at sea.

Having an importance in the field of geospatial technology, visualization and kinematic studies can lead to kinematic analyses, and thus in behavioral analysis, by comparing several kinds of nominal behaviors. As a

specialization of the information theory in the field of geomatics sciences, future work will concentrate on the use of geographical data, as well as on kinematic considerations (i.e. comparisons between foreseen behavior with respect with broadcasted message data and actual behavior) and behavioral analysis (i.e. use of external databases such as weather information to enlighten and characterize behaviors).

ACKNOWLEDGMENT

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

[1] French ministry of ecology, sustainable development and energy, "Analyse de la conjecture économique : le transport et les services maritimes – 1er semestre 2014", MEDDE, 2014.

[2] International Maritime Organization, "International convention for the safety of life at sea", IMO, 2004.

[3] National Aeronautics and Space Administration, "Space station keeps watch on world's sea traffic", NASA, 2012.

[4] J.K.E. Tunaley, "Utility of Various AIS Messages for Maritime Awareness", presented at the 8th ASAR Workshop, Longueuil, Canada. 2013.

[5] International Telecommunication Union, "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". ITU, 2014.

[6] A. Harati-Mokhtari, A. Wall, P. Brooks and J. Wang, "Automatic Identification System (AIS): a human factors approach", J. Navig. Vol 60(3), Cambridge University Press 11, 2007.

[7] Windward, "AIS data on the high seas: an analysis of the magnitude and implications of growing data manipulation at sea", October 2014.

[8] The Maritime Executive, "Iran, Tanzania and falsifying AIS signals to trade with Syria", 7 December 2012.

[9] F. Katsilieris, P. Braca and S. Coraluppi, "Detection of malicious AIS position spoofing by exploiting radar information", presented at the 16th international conference on information fusion, Istambul, Turkey, 2013.

[10] M. Balduzzi, A. Pasta and K. Wilhoit, "A security evaluation of AIS automated identification system", proceedings of the 30th annual computer security applications conference, ACSAC 2014, New Orleans, LA, USA, December 8-12, 2014.

[11] J. Bhatti and T.E. Humphreys, "Covert control of surface vessels via counterfeit civil GPS signals" University of Texas, unpublished.

[12] R. Devillers, "Conception d'un système multidimensionnel d'information sur la qualité des données géographiques", PhD thesis, Laval University, Canada, 2004.

[13] C. Fox, A. Levitin and T.C. Redman, "The notion of data and its quality dimensions" Information processing & management, vol.30(1), pp.9-19, 1994.

[14] M.L. Brodie, "Data quality in information systems", Information and management, vol.3, pp.245-258, 1980.

[15] Y.U. Huh, F.R. Keller, T.C. Redman and A.R. Watkins, "Data quality", Information and software technology, vol.32(8), pp.559-565, 1990.

[16] S. Hartmann and L. Bovens, "A probabilistic theory of the coherence of an information set", presented at the 4th international congress of the society for analytical philosophy, in proceedings pp.195-206, Bielefeld, Germany, 2001.

[17] D. Ceolin, W.R. van Hage, G. Schreiber and W. Fokkink, "Assessing trust for determining the reliability of information", published in "Situation awareness with systems of systems", pp.209-228, Springer New York, 2013.

[18] M. Hertzum, H.H.K. Andersen, V. Andersen and C.B. Hansen, "Trust in information sources: seeking information from people, documents and virtual agents", Interacting with computers, vol.14(5), pp.575-599, 2002.

[19] C. Shannon, "A mathematical theory of communication" The Bell system technical journal, vol.27, pp.623-656, 1948.