Detection of faked AIS messages and Resulting Risks

Cyril Ray, Aldo Napoli, Alain Bouju, Pierre-Yves Martin

Detection of Faked AIS Messages and Resulting Risks

C. Ray[1], A. Napoli[2], A. Bouju[3], P.Y. Martin[4]

[1]Naval Academy, Brest, France
[2]MINES ParisTech, Paris, France
[3]Université de La Rochelle, 23, avenue Albert Einstein BP 33060, 17031 La Rochelle - France
[4]CEREMA, France

Keywords: Automatic Identification System, AIS, real-time surveillance, analysing and detecting new maritime risks.

Crossroads of international issues, maritime domain is facing growing human activities. This increase of maritime mobilities has favoured the appearance and generalisation of cooperative position report systems such as the Automatic Identification System (AIS). Nowadays these reporting systems provide a real-time situation to ships and Vessel Traffic Services (VTS) in charge of traffic surveillance. Initially designed to ensure maritime security, the AIS system is now used to address this complementary objective – the detection of illegal or suspicious behaviours. Monitoring of coastal maritime areas for various purposes like safety and security, traffic management or protection of strategic areas, is largely based on the identification of positions and trajectories and abnormal behaviour detection [4]. This kind of detection is based on (1) the long-term and large-scale integration of positions from maritime traffic continuously and, (2) spatio-temporal analysis able to determine and classify a given maritime situation [3]. This analysis requires the identification and classification of navigational behaviours, techniques of falsification of position reporting systems and knowledge extraction methods to detect abnormal maritime situations [5].

Beyond irregular behaviours at sea, malfeasance mechanisms and bad navigation practices have inevitably emerged recently to circumvent, alter or exploit such surveillance systems in the interests of offenders [1]. For instance, it is easy to spoof a ship identity by issuing the IMO or MMSI (Maritime Mobile Service Identity) number from another ship (cf. Fig. 1).

Some fishing boats are practicing this offense in order to fish illegally for example by pretending to be a yacht. It is difficult to detect their illegal fishing at distance. Some captains also switch off their

AIS to disappear from monitoring centers screens and electronic chart display and information systems (ECDIS) of neighbouring ships. These acts are committed consciously by people on board. Furthermore, ships can be hijacked without the knowledge of their crew or surveillance centers by injecting false differential GPS information. AIS devices and navigational aids

(ATON) can also be reconfigured (e.g. turn off) at distance. This underlines the urgent need for studies, methodologies and information systems whose objective will be to identify these new risks [2] and contribute to a safer sea by AIS monitoring.

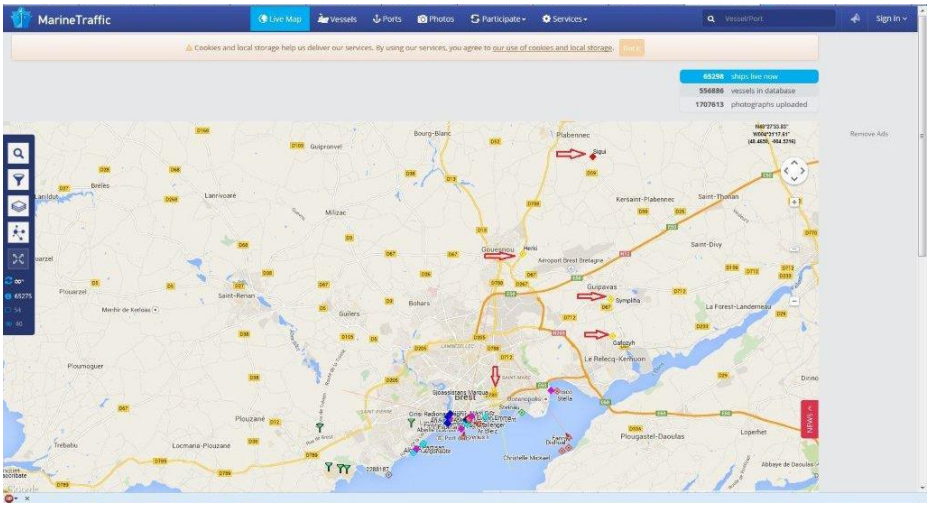

Fig. 1. Spoofing of online provider (MarineTraffic): 5 false ships reported on land.

This poster presents a novel methodological approach for modelling, analysing and detecting these new maritime risks. The objective is to detect when an AIS device is falsified or is undergoing an attack through a message-based analysis. The proposed approach relies on a simple postulate; an attack or a falsification of the AIS has consequences on received messages. An AIS device can broadcast up to 27 different messages in a range of approximately 35 nautical miles. Data exchanged include in particular static information (vessel name, dimensions, etc.) and dynamic information (heading, speed, GPS position, etc.). Positioning information is transmitted at high frequency (2–12 seconds for a moving ship, 3 min for an anchored vessel). The system transmits on less regular basis meta-information related to the ship (international identifier, name, size) and its route (destination, date and time of arrival). Additionally the system broadcast control messages (e.g. management of channels and transceiver modes by a base station is done by a message 22) and aids to navigation messages. This poster describes possible failures of the AIS at the physical, communication, logical levels and will proposes a classification of related risks. Message-based data mining methodology to identify abnormal messages and navigational behaviours is presented.

Acknowledgement.

Research presented in this paper is supported by The French National Research Agency (ANR) under reference ANR−14−CE28−0028.

References:

1. Balduzzi M, Pasta A, Wilhoit K (2014) A Security Evaluation of AIS, Automated Identification System. In: The 30th Annual Computer Security Applications Conference, ACSAC 2014, New Orleans, Louisiana, USA, December 8–12, 2014
2. Idiri B, Napoli A (2012) The automatic identification system of maritime accident risk using rule-based reasoning. In: Proc. of the 7th International Conference on System of Systems Engineering.
3. Ristic B, La Scala B, Morelande M, Gordon N (2008) Statistical Analysis of Motion Patterns in AIS Data: Anomaly Detection and Motion Prediction. In: the 11th International Conference on Information Fusion, pp 40–46.
4. Etienne L, Devogele T, Bouju A (2010) Spatio-temporal trajectory analysis of mobile objects following the same itinerary. In: Proceedings of the International Symposium on Spatial Data Handling.
5. Ray C, Grancher A, Thibaud R, Etienne L (2013) Spatio-Temporal Rule-based Analysis of Maritime Traffic. In: Conference on Ocean & Coastal Observation (OCOSS 2013), pp 171–178, Nice, France, October 28–31, 2013.