European Maritime Safety Agency

12th Mediterranean AIS Expert Working Group | **MAREΣ 12/9/1**

Rome, 22nd October 2014 | **19 September 2014**

Detection AIS spoofing

Submitted by Italy

Executive summary	The paper depicted a method to identify cases of AIS spoofing.
Action to be taken	As per paragraph 6.
Related documents	IEC 62320-1 "*Maritime navigation and radiocommunication equipment and systems – Automatic identification system (AIS) – Part 1: AIS Base Stations*"

1. Introduction

The Automatic Identification System, originally designed for collision avoidance between ships, is becoming a cornerstone of maritime situational awareness. The recent increase of terrestrial networks and satellite constellations of receivers is providing global tracking data that enable a wide spectrum of applications beyond collision avoidance. Nevertheless, AIS suffers the lack of security measures that makes it prone to receiving positions that are unintentionally incorrect, jammed or deliberately falsified.

In Figure 1 is reported a spoof radio signals convinced, an **online ship tracking service**, that this fake craft had travelled on a path near Italy that spelled out the hacker term "**pawned**" which describes a system that has been compromised by an attacker.

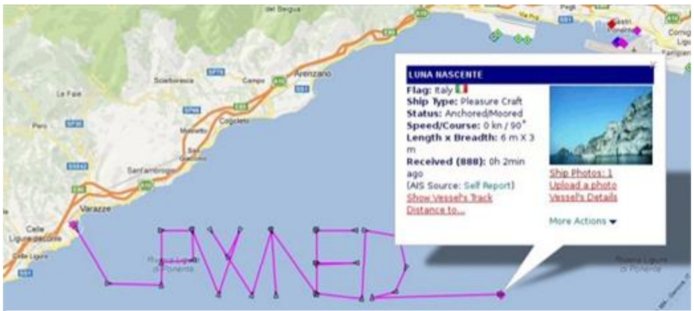

Figure 1: An AIS device transmitting intentionally false position, on a path spelling the term "pawned" (from the web)

So there is a concrete interest for a national competent authority to implement mechanisms to quickly identify cases of spoofing, in order to enhance the quality of the information acquired by both the national and regional AIS network.

European Maritime Safety Agency (EMSA)
Praça Europa 4, Cais Do Sodré 1249-206 Lisbon, Portugal
Tel: +351 21 1209 415, Fax: +351 21 1209 217

At the end of 2013 the Italian Coast Guard started a collaboration with the Joint Research Centre – the Maritime Affaires of the Institute for the Protection and Security of the Citizen - in order to test algorithms able to localize and track a vessel using the radiofrequency of the AIS transmission but without reading the information related to position course and speed broadcasted by the vessel itself through AIS.

The aim of this paper is to provide information about the method used and the outcomes from the experimentation.

2. The VSI sentence

The project is based on the measurement of the Time of Arrival (ToA) of the radiofrequency of the AIS emission transmitted by vessels. The ToA have to be measured for each Base Station that has received the AIS emission.

According to the IEC 62320, the ToA information of a received message is provided by the Base Stations using the VSI sentence to be associated with the corresponding received AIS message. It is output in combination with a VDM sentence.

Below the VSI structure is shown:

$--VSI,c--c,x,HHMMSS.SS,x.x,x.x,x.x*hh<CR><LF>

Signal to noise ratio (dB) (see Note 6)
Receiver input signal strength (dBm) of received message (see Note 5)
First slot number of message (see Note 4)
UTC hour, minute, second, and fractional-second of measurement (see Note 3)
Sequential message identifier (see Note 2)
Unique identifier (see Note 1)

Note: this is the hour, minute, and second of a measurement. The fractional portion of a time of arrival (TOA) measurement can be given with a precision of 1 ns.

Example with a TOA measurement:

```
\1G2:1234,s:r3669961,c:1120959341*2D\!ABVDM,1,1,1,B,100000?0?wJm4:`GMUrf40g604:4,0*hh
\2G2:1234*79\$ABVSI,r3669961,1,013536.96326433,1386,-98,*hh
```

3. Locate a vessel using the radiofrequency emission

The Time of Arrival is used to calculate the distance between the transmitted ship and the received station, as follow:

$$R = ToF * c$$
$$ToF = ToA - T_{slot} - \eta_{tx} - \eta_{rx}$$

Where:

- R, is the distance between the transmitted ship and the received station;
- c, is the speed of light;
- *ToF*, is the Time of Flight (*ToF*) of the electromagnetic wave carrying the AIS message from the transmitted vessel to the received station;
- *ToA*, is the Time of Arrival provided by the received station through the VSI sentence;
- T_{slot}, is the beginning of the time slot during which the message has been transmitted;
- η_{tx} and η_{rx} are the transmitter and receiver timing errors, respectively.

Notice that the information of the number of time slot within the frame of a minute is also contained in the IEC sentence.

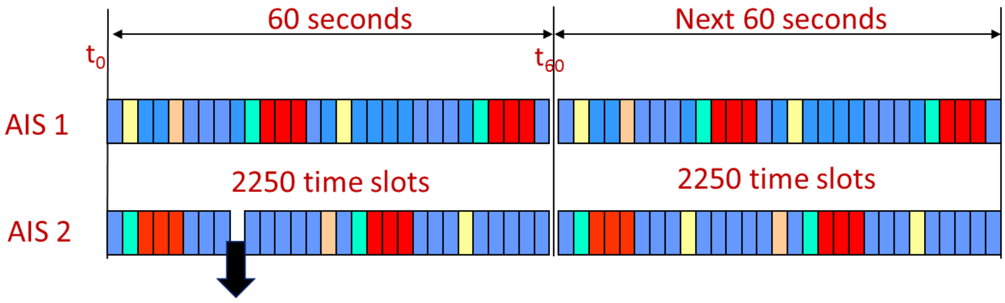

Figure 2: Indication of the Time Slot parameter, that may be calculated considering the indication of the slot used for transmitting the AIS message reported in the VSI sentence.

When it is possible to fully characterise the errors η_{tx} and η_{rx}, an unbiased estimate of the *ToF* could be obtained and used to derive distance R from the considered vessel and the receiving AIS Base Station. Multiple distances from different AIS-BSs could then be used to find an unbiased estimate of the instantaneous vessel position using *ToA* based triangulation (Fig. 3).

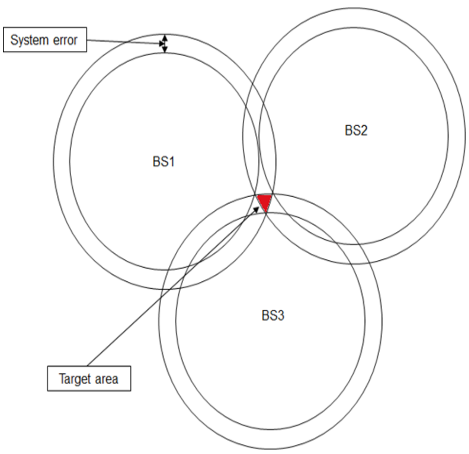

Figure 3: Vessel position obtained using ToA based triangulation

Unfortunately the transmitter timing error η_{tx} is generally unknown and can be in the order of according of tens of μs leading to large ranging uncertainties. Moreover, η_{tx} is vessel-dependent due to differences in the electronics of different transmission equipment. This means that a full characterisation of η_{tx} is not possible and the *ToA* measurements cannot be robustly used to directly solve the vessel localisation problem.

Assuming the vessel under surveillance is within the coverage area of more Base Stations, the simplest idea is to compare the received *ToAs* pairwise and use the Time Difference of Arrivals (*TDoA*), calculated as follows:

$$ToF_1 = ToA_1 - T_{slot} - \eta_{tx} - \eta_{rx1} \qquad ToF_2 = ToA_2 - T_{slot} - \eta_{tx} - \eta_{rx2}$$

Where:

- ToA_1, is the time of arrival at the receiving station rx_1;
- ToA_2, is the time of arrival at the receiving station rx_2.

The difference TDoA:

$$TDoA = ToF_1 - ToF_2 = ToA_1 - ToA_2 - \eta_{rx1} + \eta_{rx2}$$

$TDoA = ToA_1 - ToA_2$ if assuming $\eta_{rx1} \cong \eta_{rx2}$ (the base stations are similar).

Geometry tell us that all the position having the same TDoA are laying on an hyperbola. So if we have different TDOAs we may have different hyperbolas. From the intersection of at least two hyperbolas is possible to obtain the position of the ship (Fig. 4).

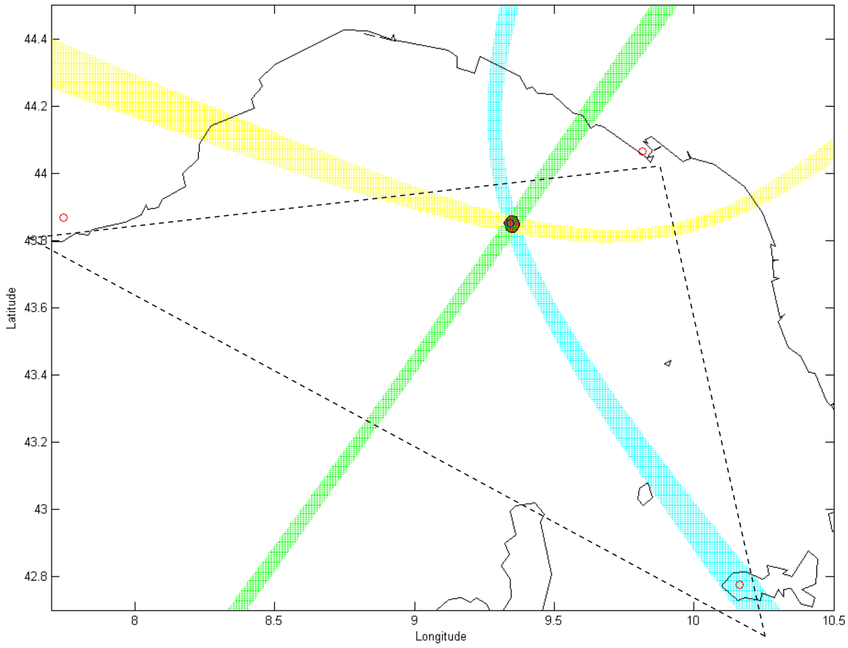

Figure 4: Radiolocation of the AIS emission in the Ligurian Sea as the intersection of the TDoAs hyperbolic functions between three receiving stations (red circles), whose baselines are highlighted by dashed lines. The AIS encoded position (blue circle) falls within the estimated emission area (red).

4. Trials in the Ligurian Sea

First of all it was necessary to modify the Base Stations used for the trial in order to improve the time measurement accuracy, compatibly with the Base Station currently hardware capability. The accuracy has been improved to less than 30 microseconds.

The time of arrival has been added to every message received by the Base Stations, together with the signal strength, using the VSI sentence.

Usually, all the messages acquired by the Base Stations are gathered by a national server which provides also a functionality called "duplication avoidance", operating when the same message is received by two or more Base Stations.

This functionality **has been excluded** because we are just looking for the duplicated messages coming from different Base Stations.

Moreover, the national server has to be able to receive messages from Base Station at full data rate, **without downsampling**.

In the first phase of the project the Italian Coast Guard delivered to JRC the AIS messages acquired in a few days by a limited number (7) of Base Stations located in the Ligurian Sea and in North Tyrrenian Sea.
The project immediately provided very good and enthusiastic results.

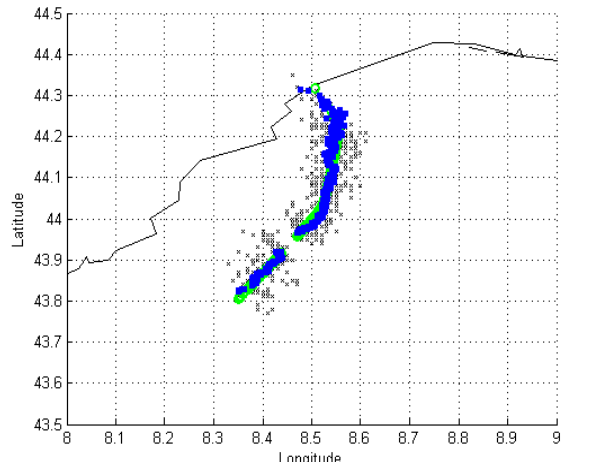

Figure 5: A vessel tracked using the AIS radiofrequency emission

The Figure 5 is showing the track of a vessel obtained considering more positions, acquired in a certain period of time. The track accuracy is improved through time integration by means of an appropriate filter, like the Kalman already used in the radar system. The great experience of JRC in the fields of statistics and radar elaboration provided a very important added value.

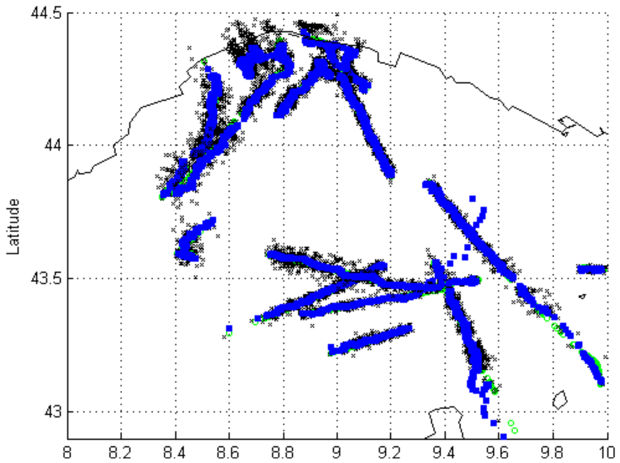

Figure 6: Vessels localization and tracking in the Ligurian Sea

In Fig. 6 is reported the localization and tracking of more vessels sailing in the Ligurian Sea. The average precision of the tracking is less than one kilometre.

In Fig. 7 is reported another screenshot of the results obtained at the end of this project, elaborating off-line information where a vessel radio frequency is received by at least 3 Base Stations in order to achieve sufficient localization accuracy. Using the JRC Blue Hub visualizer is possible to compare the vessel declared position in blue and the position acquired through the radio localization of the emission in green.

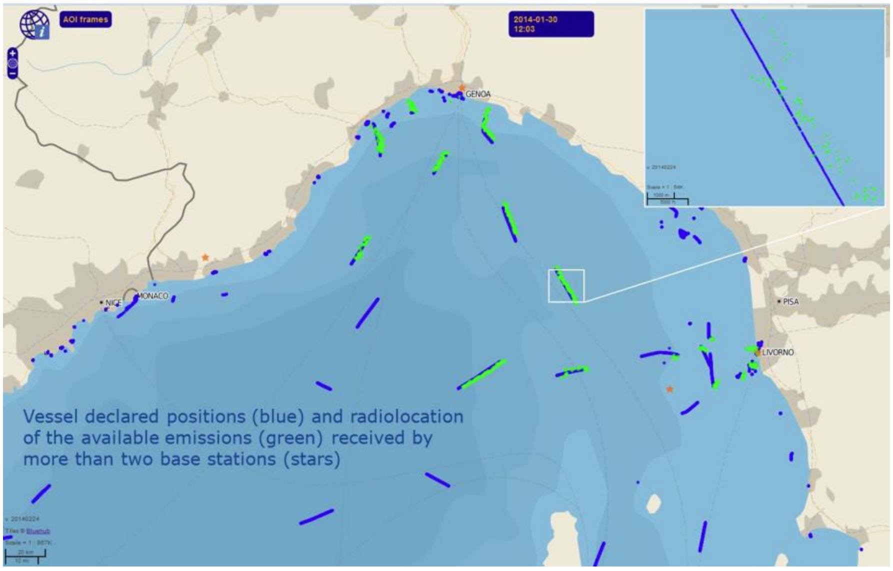

Figure 7: The results obtained

5. Consideration

After the positive results obtained by the trials, it's possible to evaluate the implementation of a permanent service, which runs in parallel to the national network checking the position, course and speed transmitted by the vessel through the AIS in order to detect spoofing.

The number of Base Stations able to receive the radio frequency emission and used to localize and track the vessel is an important factor.

So, for those States that are exchanging AIS information on regional base as the Mediterranean and Black Sea ones, these project may represents a very good opportunity to a establish a more intensive cooperation with the common benefits to enhance the overall confidence of the AIS information exchanged.

Considering the normal VHF coverage of the AIS Base Stations in the Mediterranean Sea and in its western approach there are several areas where is possible to cooperate: in the Gibraltar Strait, in the Sicily Strait, in the Ligurian Sea, in the Corsica channel, in the Bonifacio Strait and in the Adriatic Sea.

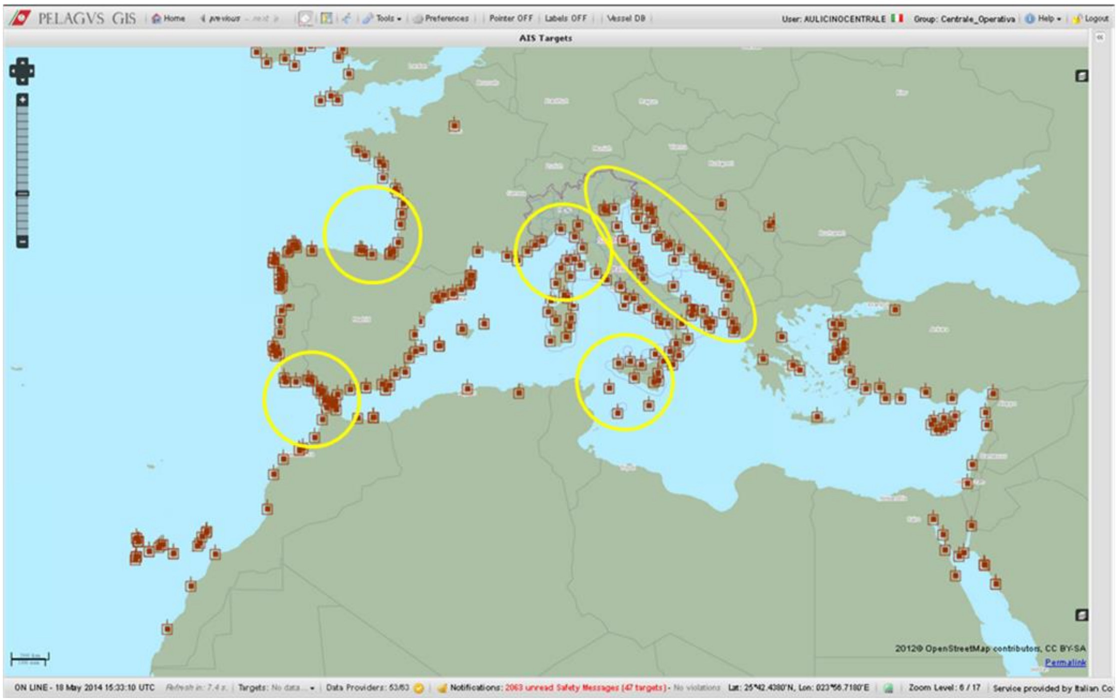

Figure 8: Area of possible cooperation

In these cases the quality of information may be processed by the same system already in place to allow the information exchange among Member States. The regional system may delivers the confidence value of the messages exchanged to all participating Countries and provide a prompt alert when a spoofing is detected.

6. Action required

Participating countries are requested to note the results of the project and to evaluate the feasibility to implement the service in the above mentioned areas.