Detection of AIS Messages Falsifications and Spoofing by Checking Messages Compliance with TDMA Protocol

Maelic Louart, Jean-Jacques Szkolnik, Abdel-Ouahab Boudraa,
Jean-Christophe Le Lann, Frédéric Le Roy

Detection of AIS Messages Falsifications and Spoofing by Checking Messages Compliance with TDMA Protocol

Maelic Louart[1,2], Jean-Jacques Szkolnik[1], Abdel-Ouahab Boudraa[1], Jean-Christophe Le Lann[2] and Frédéric Le Roy[2]

[1] *Ecole Navale/Arts et Metiers Institute of Technology, IRENav, BCRM Brest, CC 600, 29240 BREST Cedex 9, France.*

(maelic.louart,jj.szkolnik,boudraa)@ecole-navale.fr

[2] *ENSTA Bretagne, Lab-STICC, 2 Rue François Verny, 29200 BREST, France.*

(jean-christophe.le_lann,frederic.le_roy)@ensta-bretagne.fr

Abstract

Automatic identification system is an navigation aid system that allows vessels to exange automatically positions, identity and other information. It improves the safety and of the maritime traffic and help to monitor it. However, this system can be manipulated to send falsified information and mask illicit activities. While previous research has proposed strategies to detect these threats, none of them suggest a solution that considers the time-division multiple access (TDMA) communication protocol. In this work, the compliance of the sent messages with this protocol, specified by the system's standard, is checked for every ship to detect message falsifications. Furthermore, because the ships velocity affects TDMA protocol, a strategy based on the use of a Kalman filter is applied to track every ship and assesses the consistency of their velocity data sent. The proposed strategy was validated on real data, is computationally cheap and can be run in real time. Source codes of the method are open-source to foster research activities from both industry and academia in this field.

Keywords: Automatic Identification System (AIS), TDMA protocol, falsification detection, spoofing detection, Kalman filtering.

1. Introduction

Automatic identification system (AIS) is an electronic tracking system introduced to enhance the safety of vessels traffic by automatically exchanging up-to-date information [1]. Since 2002, AIS has been a mandatory installation to vessels above 300 gross tons or for all ships carrying passengers in international water. Currently, AIS use has also been extended to the pleasure boating sector. Nowadays, about 2 million ships use AIS for regular operations [2]. The typical coverage range of an onboard transceiver is about 25-40 kilometers (km), depending on many factors such as transceiver altitude/type or weather conditions. The messages from AIS transceivers are exchanged in the very high frequency (VHF) network using time-division multiple access (TDMA) protocol, which prevents messages interferences for a share medium network. Data exchanged between AIS transceivers, can be divided into two classes:

1. Static data (e.g., vessel name, the dimensions of the vessel, voyage-related data, etc.);
2. Dynamic data (e.g., vessel position, velocity, course over ground, etc.);

Combined with geographic maps, Radar images and depth charts, these data provide a maritime vessel with a complete view of its surrounding environment. Also, these data are used to characterize marine traffic patterns [3],[4], to avoid collisions [5], and to detect anomalous vessel movements behaviour [6], [7]. However, main limitations and weaknesses of the AIS are its reliability and susceptibility to manipulation. Recent works have highlighted and proven the vulnerability of the AIS [8, 9, 10, 11, 12, 13]. Examples of AIS attacks are reported in [9, 10]. An overview on AIS threats and their classification as software and radio attacks has been provided by Balduzzi et al. [8]. Recent real AIS data reported by NATO show that there is compelling evidence that the AIS tracks of ships can be faked [14]. Overall, AIS is not secure because the data received by the transceivers are not subject to any verification of their integrity. Only a cyclic redundancy check is applied to detect transmission errors.

Thus, the transmitted data may contain errors [15] whose possible causes are classified in three categories [16]: unintentional errors, falsification and spoofing. Unintentional errors which represent most of the errors are caused by transceiver deficiency, incorrect input of manual data or poor environmental conditions. Data can then be false, incomplete, impossible according to the norm or the physics (e.g a latitude field value superior to 90°). Lists of these kinds of errors are presented in [17]. Falsification is a voluntary alteration to data of messages to deliberately mislead the outer world. It can concern the emitted identity [18], the dynamic data [19, 8] and the static data [20]. AIS systems can be also turned off to stop broadcast messages [21]. Spoofing is done by creating ex nihilo false messages, from an external actor, and by broadcasting them on the AIS frequencies [8]. These spoofing activities are carried out to mislead both the outer world and the crews at sea, e.g by creating ghost vessels, by sending false closest point of approach triggers or by emitting false emergency message. Also, spoofing can jam communication between AIS transceivers [8]. These falsifications and spoofing of AIS messages, in addition to reducing the reliability of AIS data, can mask illicit activities like piracy, illegal fishing, terrorist attacks. Thus checking the reliability of AIS messages is becoming a necessity to exploit the full potential of this system for safety and security of the maritime traffic. This is why, we present a strategy to detect falsifications or spoofing of AIS messages.

1.1. Related works

To tackle the problem of the AIS weaknesses, two strategies can be considered. On the one hand, the system can apply cryptographic methods enabling encryption of AIS messages [22]. On the other hand, algorithms can be applied to the messages decoded by the AIS to detect falsifications or spoofing. The first strategy needs software update and some changes in the existing AIS service. This is not the case for the second strategy which can be already applied to an AIS transceiver without changes in the the existing AIS service. This is why, this second approach is considered in this work. Concerning this approach,

several methods are proposed in the literature.

First, crowd-sourcing methods, which exploit measurements from sensors to estimate the ships dynamic data (position, speed), and compare these data to those sent by the AIS to assess its reliability [23]. For example, position can be estimated with an accuracy of a few hundred meters, using the time difference of arrivals of AIS messages from several ground stations [24]. In addition, new position measurements can also be obtained using radar signals (coastal radars [25] or space-based synthetic aperture Radar (SAR) [26]). Another way to estimate the position is to use the Doppler effect [27]. A main limitation of crowd-sourcing methods is that, in addition to AIS, they exploit other sensors, which sometimes are placed in locations far away from each other [24]. Moreover, estimation of the positions can be imprecise (a few hundreds meters [24], more than 10 km for [27]) or can take a long time (a few hours to one day for [26]) when using SAR data.

Second class of methods extract characteristics on the raw signal before demodulation process to detect spoofing [28, 29], jam or voluntary system shutdown [30], [31]. For instance, energy evolution over time of the signal can be observed to detect voluntary system shutdown, or radiometric signatures [32] can be extracted to identify every transceiver independently of the transmitted identity and detect identity spoofing [29]. These methods require the building of new AIS receivers to have a direct access to the raw signal. This is a major drawback, because we aim to apply, in this work, our algorithms to the messages decoded by the AIS transceivers available off-the-shelf.

Third class of methods check the consistency of received AIS data. Inconsistency in data may be caused by messages falsifications or spoofing. For instance, dynamic data consistency is checked considering other AIS dynamic data coming from either other ships [33] or the same ship [34, 35, 36, 37, 38, 39, 40, 41, 42]. Unfortunately, in [33], large amount of data are processed, which prevents a real time application. Dynamic data from the same ship are exploited to predict future position and compare it to the received one to detect inconsistencies in positions evolution. However, even if this strategy is interesting, none of the

mentioned papers check the ship velocity, which is necessary because it affects TDMA protocol. An other strategy, such as presented in [23], proposes algorithms that check that the technical standards are consistent with in terms of frequency and order by automatic dependent surveillance-broadcast (ADS-B) messages received [23]. For the moment, these algorithms remain an idea and have not been implemented and verified with real data. Moreover, this strategy concerns only ADS-B application which is the equivalent of AIS for aircraft.

In this work, this last idea is investigated because this approach is efficient to detect message falsifications. Indeed, often when a malicious user creates messages from scratch to transmit false data, these messages do not respect the TDMA protocol. This protocol is complex and it is difficulty to reproduce it. This fact was observed by a proven case of spoofing documented by NATO [14]. Thus, we develop different algorithms to check the messages compliance with this TDMA protocol, specified by the AIS standard [43], to detect messages spoofing and falsifications. In addition, the evolution consistency of position and velocity over time is controlled because velocity intervenes in this protocol. These developed algorithms can be applied to messages decoded by an AIS transceiver available off-the-shelf and have real time performances.

1.2. Contributions

Mains contributions of this work are:

1. We propose a new strategy that detects message falsifications by considering their compliance with the TDMA protocol, which is a first in the literature. This strategy can be applied to position report messages emitted by Class A shipborne mobile AIS stations; These messages represent 80% of transmitted messages [36];
2. The proposed strategy is computationally cheap and allows real time execution. Thus, authorities can detect in real time falsifications and intervene fast to intercept and arrest the malicious user. This represents a novelty in the literature because most of the proposed strategies do not have real time performances;

3. Matlab code of the strategy's algorithms is in open-source with the real data used to test them [44]. It allows other team to use it to compare our performances with their strategies performances and to help research activities from both industry and academia in this field. It is the first time that AIS messages are available on the Internet with a message arrival time accurate to the ms and that the code of a strategy to detect AIS message falsifications is open source.
4. The strategy implements a Kalman filter to detect position falsifications. This filter considers positions in spherical coordinates. This consideration saves computations and is a first in the literature. Usually, when position is tracking from AIS messages, a Cartesian coordinate system is used.

The remainder of this paper is organized as follows. In section II, strategy overview to detect AIS falsifications and spoofing is presented. The algorithm that controls dynamic data consistency with some details of its implementation is introduced in section III. In section IV, we present algorithms that control the compliance with TDMA protocol to detect falsifications and spoofing. Results on real data are presented in section V and discussed in section VI. Finally, some futur works are given in section VII.

2. Detection of AIS messages falsifications and spoofing

In this paper, three algorithms are developed and assembled to form a global strategy that checks the messages compliance with TDMA protocol (Figure 1). The first algorithm (Algorithm 1) checks the reliability of AIS dynamic data (position and velocity), which intervene in TDMA protocol, using a Kalman filter that tracks the ships. The two other algorithms verify the messages compliance with the TDMA protocol, first considering the nominal reporting interval (RI) of AIS messages (Algorithm 2), and after the time-slot (TS) booking process (Algorithm 3). A TS is a small time interval, created by TDMA protocol, during which a message can be emitted.

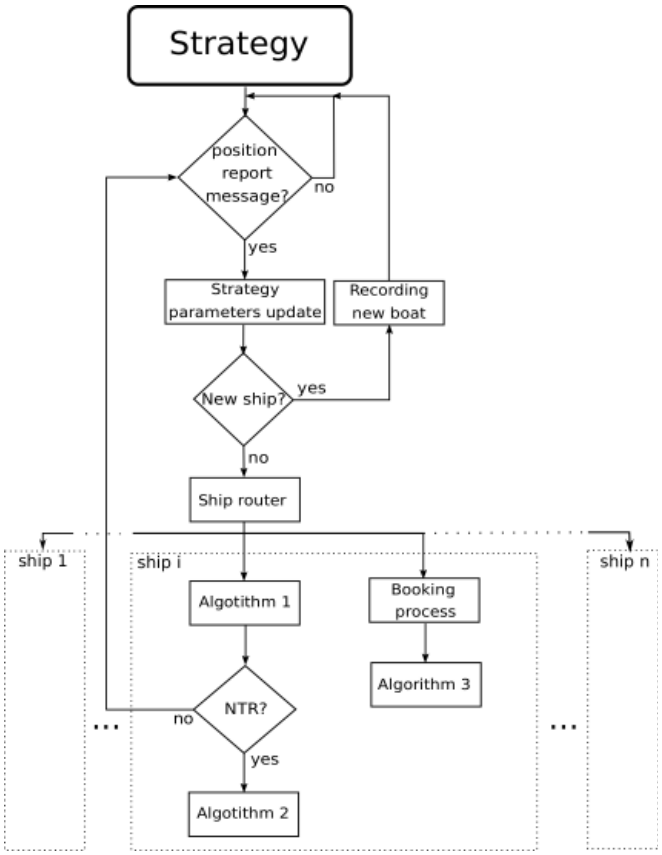


Figure 1: Diagram of the developed strategy to detect AIS position falsifications and messages spoofing.

Algorithm 3 is executed in parallel of the Algorithms 1 and 2. These two algorithms are executed in series because, before checking the RI of messages (Algorithm 2), the reliability of the sent velocity data has to be verified (Algorithm 1). Indeed, RI depends on sent velocity. Thus, if the checks on Algorithm 1 are correct, a nothing to report (NTR) message is returned and allows Algorithm 2 to be executed. Messages from every ship have to be checked, this is why, for each ship, a large block composed of the three algorithms is created. Every large block runs in parallel.

When a position report message is received, the strategy updates its parameters. This update synchronizes the time of message arrival to the minute universal time coordinated (minute UTC), computes the TS, updates the list of tracked ships removing ships that do not send a message for more than 6 minutes, and updates booking process parameters explained in subsection 4.3.4. After, the strategy verifies if the received message comes from a ship already tracked. If it is the case, a router block sends the message to the large block that corresponds to the ship identity. Otherwise, this new ship is recorded by the strategy.

To help user to discern intentional errors (spoofing and falsification) from unintentional errors, every algorithm reports, in addition of alerts, the numbers of controlled messages, the number of detected alerts and the alert percentage computed during the last fifteen minutes. A statistical evaluation is done (Sec. 5) to fix a threshold value for each algorithm, above which, the alert percentage has to be considered as suspect and the errors intentional.

Current version of the proposed strategy is not portable to systems that do not apply the TDMA communication method. However, Algorithm 1 is applicable to systems that receive messages containing the position of the tracked target and the arrival time of the message, which allows to detect position falsifications. Nevertheless, the spoofing detection idea based on communication protocol check is portable to other communication systems that apply other protocols.

3. Checking of dynamic data consistency

As previously mentioned, ship tracking is achieved via a Kalman filter. Under some conditions, this filter provides the best linear state estimates from measured data. It operates by propagating the mean and covariance of the estimated state through time. In this work, this filter tracks latitude and longitude for every ship to detect inconsistency in evolution of dynamic data.

3.1. Related work on methods that predict the dynamics of a ship

Many tracking algorithms have been developed to predict the dynamic behavior of vessels. Most of the time, they are not used to detect falsifications or spoofing, but to resolve a stop in emission causing by poor environmental conditions, and to improve the visibility in the sea area. Some of these algorithms are based on linear filter such as Kalman filters [35] or non-linear filters such as extended Kalman filter [37, 38] and particle filter [39]. One can quote algorithms that do not use filters, but only dynamic equations of a vessel as in [36] and [40]. Also, some algorithms thanks to machine learning methods, predict the next dynamic data from a database collected in a same sea area [41]. Finally, algorithms with particular methods designed especially for AIS data are used in [42]. Due the linear dynamic of the vessel, we implement a linear Kalman filter that is well suited for our study because of the following attractive properties:

- It is the best linear estimator;
- It requires low computation capacity: the Kalman filter could validate the real-time requirements and be implemented in on-board circuits;
- It provides accuracy of predicted positions to assess the reliability of position measurements;
- It allows optimum handling of non periodic measurements: AIS messages are not received at a constant time interval.

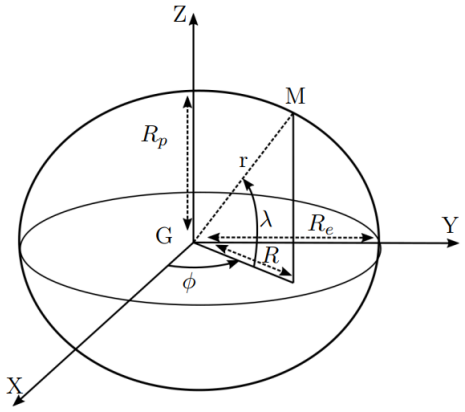


Figure 2: WGS84 geodetic system

3.2. Coordinate system

Several coordinate systems can be used to track vessels. In general, the choice is between the Cartesian coordinate system, in which the target movement is easily described, and the spherical coordinate system, in which the measurements from the sensors (radar or GPS) are expressed. The interest of using the spherical coordinate system is to save important computational costs: the measurements coming from the GPS are directly used and do not require a change of coordinate system as it is done for the Cartesian coordinate system.

Thus, in our application, we use the WGS84 geodetic system which is the spherical coordinate system used by GPS to express the positions of objects. This is the first time in the literature that this coordinate system is applied to track vessels from positions transmitted by AIS messages. Usually the Cartesian coordinate system is used. This coordinate system is represented in Figure 2. In the figure G is the Earth's center of mass, M is the position of the observed object, λ is the latitude, ϕ is the longitude, R_e is the earth equatorial radius, R_p is the earth polar radius.

3.3. Kalman filter equations

Equations and hypotheses presented in this part were found in [45] and [46]. We apply the constant velocity (CV) model to both latitude and longitude be-

cause most of the time, vessel has a uniform rectilinear motion. Maneuvering actions are rare events and we will explain below (3.5) how we consider them with our CV model. So, speed is considered as constant (**H1**). However, because we use the spherical coordinate system, it appears pseudo accelerations on latitude and longitude when the vessel is moving according to an uniform rectilinear motion [47]. These pseudo accelerations' maximum value is, according to [45], equal to :

$$a_{max} = \frac{v_{max}^2}{R_{min}} \tag{1}$$

with v_{max} the maximum velocity of the target and R_{min} the minimum distance between the target and the origin of the chosen coordinate system. Because the maximum velocity for vessel is 40kt and the earth radius is 6356km, the pseudo accelerations can be neglected except at the poles for longitude.

So a second order model is applied and the dynamic model assumes that the state of our system at time $n+1$ evolved from the prior state at time $n \in \mathbb{N}$ according to the following equation:

$$X_{n+1} = F_{n+1}X_n + \Gamma_{n+1}v_n \tag{2}$$

$$X_n = \begin{pmatrix} x_n \\ \dot{x}_n \end{pmatrix}, F_n = \begin{pmatrix} 1 & \Delta T_n \\ 0 & 1 \end{pmatrix}, \Gamma_n = \begin{pmatrix} \frac{\Delta T_n^2}{2} \\ \Delta T_n \end{pmatrix}$$

where

(a) X_n is the state vector containing the position x_n (latitude/longitude) and the first derivative of x_n with respect to time ($\dot{x}_n$).

(b) F_n is the state transition matrix between time of index $n-1$ to time of index n.

(c) Γ_n is the noise gain matrix at time n.

(d) $\Delta T_n = t(n) - t(n-1)$ is the time interval between two consecutive measurements (messages).

(d) v_n is the process noise at time n.

In this model the process noise model used is a discrete white noise acceleration (DWNA) model (**H2**). For this model, the acceleration noise v_n, with standard deviation σ_v, is assumed to be constant over each sampling period and independent between periods. However, $\sigma_v \Delta T_n$ has to be small compared to the actual velocity to validate the hypothesis (**H1**). The model can be considered as nearly constant velocity (NCV) model.

The observation model of our system is:

$$Y_n = CX_n + w_n \tag{3}$$

where Y_n is the measurement at the time n, $C = (1\ 0)$ is the observation matrix and w_n is the observation noise at the time n. Noise w_n is assumed (**H3**) to be zero-mean Gaussian white noise sequences as v_n so:

$$\begin{array}{ll} \mathbb{E}[v_k] = 0 & \mathbb{E}[w_k] = 0 \\ \mathbb{E}[w_k w_l^T] = R_k \delta_{kl} & \mathbb{E}[v_l w_k] = 0 \\ \mathbb{E}[X_0 W_k^T] = 0 & \mathbb{E}[V_k V_l^T] = Q_k \delta_{kl} \quad \mathbb{E}[X_0 V_k^T] = 0 \\ V_k = \begin{pmatrix} \frac{\Delta T_k^2}{2} & \Delta T_k \end{pmatrix}^T v_k & W_k = \begin{pmatrix} w_k & 0 \end{pmatrix}^T \end{array}$$

where $(k, l) \in \mathbb{N}^2$, $\mathbb{E}[.]$ is the expectation operator, δ is the Kronecker symbol, V_k is the process noise vector at time k, X_0 the initial value of state vector and W_k is the observation noise vector at time k.

Kalman filter runs successively prediction and estimation algorithms as presented in Figure 3. Presented variables and equations were taken from [45] and are expressed below:

Predictor equation:

$$\widehat{X}_{n+1|n} = F_{n+1} \widehat{X}_{n|n} \tag{4}$$

Estimator equation:

$$\widehat{X}_{n|n} = \widehat{X}_{n|n-1} + H_n (Y_n - C\widehat{X}_{n|n-1}) \tag{5}$$

Weight equation:

$$H_n = \widehat{P}_{n|n-1} C^T [R + C \widehat{P}_{n|n-1} C^T]^{-1} \tag{6}$$

Predictor covariance matrix equation:

$$\widehat{P}_{n|n-1} = \mathrm{COV}(\widehat{X}_{n|n-1}) = A_n \widehat{P}_{n-1|n-1} A_n^T + Q_n \tag{7}$$

Covariance of process noise vector V_n:

$$Q_n = \mathrm{COV}(V_n) = \mathbb{E}[V_n V_n^T] = \begin{pmatrix} \frac{\Delta T_n^4}{4} & \frac{\Delta T_n^3}{2} \\ \frac{\Delta T_n^3}{2} & \Delta T_n^2 \end{pmatrix} \sigma_v^2; \tag{8}$$

Covariance of measurement vector Y_n:

$$R = \mathrm{COV}(Y_n) = \mathrm{COV}(W_n) = \mathbb{E}[W_n W_n^T] = \sigma_w^2 \tag{9}$$

Estimator covariance matrix :

$$\widehat{P}_{n-1|n-1} = \mathrm{COV}(\widehat{X}_{n-1|n-1}) = (I - H_{n-1} C) \widehat{P}_{n-1|n-2} \tag{10}$$

Initialization is done applying the two-point differencing method [46]:

$$\widehat{X}_{1|1} = \begin{pmatrix} Y_1 \\ \\ \frac{Y_1 - Y_0}{\Delta T_1} \end{pmatrix} \widehat{P}_{1|1} = \begin{pmatrix} R & \frac{R}{\Delta T_1} \\ \\ \frac{R}{\Delta T_1} & \frac{2R}{\Delta T_1^2} \end{pmatrix} \tag{11}$$

Standard deviation of observation noise (σ_w) is fixed considering the standard deviation of GPS position measurements (5 meters [48]). Dynamic model noise (σ_v) is determined as $\sigma_v = 0.5 \times \Delta a$ where Δa is the maximum acceleration increment over a sampling period. The Δa value is fixed in subsection 3.5. Note that in spherical coordinates when a ship goes in a straight line with a constant velocity, it appears accelerations induced by the geometry in latitude and longitude [45]. These induced accelerations called pseudo-accelerations can be neglected outside the poles because, in our application, the radius of the earth is much greater than the ship velocity [45].

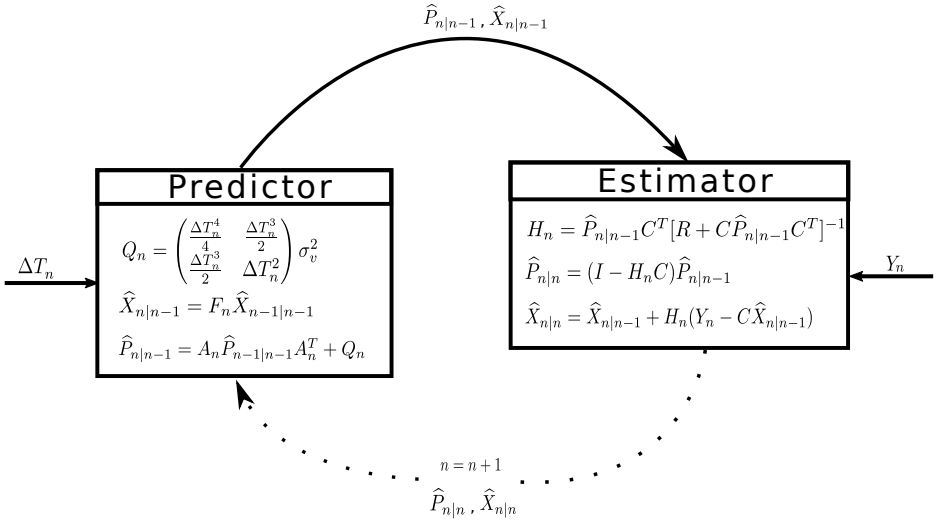


Figure 3: Kalman filter operation diagram

3.4. Speed Over Ground computation

Speed over ground (sog) of the ship, also called velocity in this study, is computed from both latitude state vector $\left(\widehat{X}_{\lambda(n|n)}\right)$ and longitude state vector $\left(\widehat{X}_{\phi(n|n)}\right)$ by application of equation (12). We compare this value with the value transmitted in the messages to assure consistency between position evolution and sog transmitted.

$$sog_c(n) = \sqrt{\widehat{X}^2_{\lambda(n|n)}(2) R_p^2 + \widehat{X}^2_{\phi(n|n)}(2) R_e^2 cos^2(\widehat{X}_{\lambda(n|n)}(1))} \tag{12}$$

To evaluate the accuracy of computed $sog_c(n)$, its standard deviation, $\sigma_{sog_c(n)}$, has to be considered at the same time. However, $\sigma_{sog_c(n)}$, like $sog_c(n)$, is not estimated by Kalman filter, so it has to be computed. To do so, we use the state vectors and covariance matrices estimated by Kalman filter for the latitude and longitude, in addition to the propagation of uncertainty of a non-linear combination $Z = f(X, Y)$ [49]. The computation is simplified, making the hypothesis $\cos(\widehat{X}_{\lambda(n|n)}(1))$ constant over time (**H4**) which renders $\widehat{X}^2_{\lambda(n|n)}(2)$ and $\widehat{X}^2_{\phi(n|n)}(2)$ independent.

Thus, the following equation is derived:

$$\sigma_Z^2 = \left(\frac{\delta f(X,Y)}{\delta X}\right)^2 \sigma_X^2 + \left(\frac{\delta f(X,Y)}{\delta Y}\right)^2 \sigma_Y^2 \tag{13}$$

where

$$\begin{aligned} Z &= sog_c(n) \\ X &= \widehat{X}_{\lambda(n|n)}(2) \\ Y &= \widehat{X}_{\phi(n|n)}(2) \\ \frac{\delta f(X,Y)}{\delta X} &= \frac{R_p^2 \widehat{X}_{\lambda(n|n)}(2)}{sog_c} \\ \frac{\delta f(X,Y)}{\delta Y} &= \frac{R_e^2 cos^2(\widehat{X}_{\lambda(n|n)}(1))\widehat{X}_{\phi(n|n)}(2)}{sog_c} \end{aligned}$$

Standard deviations $\sigma_X = \sigma_{\widehat{X}_{\lambda(n|n)}(2)}$ and $\sigma_Y = \sigma_{\widehat{X}_{\phi(n|n)}(2)}$ are obtained from $\widehat{P}_{\lambda(n|n)}$ and $\widehat{P}_{\phi(n|n)}$ respectively the estimator covariance matrices of latitude and longitude.

3.5. Consideration of the ship's dynamics

Ship behavior can be classified into two states. The first one, when the ship is maneuvering, and the second one, when the ship is not maneuvering. During maneuverers, course and speed change quickly, so the process noise v_n is higher than during non-maneuvering state. Thus, depending on the conditions of navigation, a ship's motion can be described by two dynamic models.

To consider this change in model, Bar Shalom introduced the interacting multiple model (IMM) [46]. This estimator computes, at time n, the state estimate under each possible current model using r Kalman filters. He also proposed, to apply a Kalman filter and fix σ_v to 0.8 of the maximum process noise standard deviation. IMM provides more noise reduction than Kalman filter at a cost of r Kalman filters. The choice between a Kalman filter (single model) and a multiple model approach like IMM estimator depends on the maneuvering index $\lambda = \frac{\sigma_v \Delta T^2}{\sigma_w}$ of the target.

In our application, during the non-maneuvering condition, $\sigma_w \propto 5m$ (angle is converted to distance considering the radius of Earth), $\Delta T = 10s$ and

$\sigma_v \propto 0.05kt.s^{-1}$ ($\Delta a = 0.1kt.s^{-1}$); during the maneuvering condition $\sigma_w \propto 5m$, $\Delta T = 3 + \frac{1}{3}s$ and $\sigma_v \propto 0.5kt.s^{-1}$ ($\Delta a = 1kt.s^{-1}$). λ index is therefore respectively equal to 0.5 and 0.54. ΔT which decreases when the ship is maneuvering, is imposed by AIS standard [43]. Bar Shalom reports that below about $\lambda = 0.5$, Kalman filter and IMM estimator perform equally well [46]. So, we only applied one Kalman filter because the maximum value we obtained for λ is 0.54, which is close to 0.5.

3.6. Algorithm 1: Consistency checking of dynamic data

Kalman filter is applied ship wise to detect inconsistent position and sog measurements. The exact position and sog of each measurement are unknown but their values can be marked out thanks to the vectors and covariance matrices computed by the Kalman filter. To detect falsified measurements, innovations and prediction covariance matrices are considered. Innovation on latitude and longitude are computed using the following equations:

$$\nu_\lambda(n) = Y_\lambda(n) - C\widehat{X}_{\lambda(n|n-1)} \tag{14}$$

$$\nu_\phi(n) = Y_\phi(n) - C\widehat{X}_{\phi(n|n-1)} \tag{15}$$

where $Y_\lambda(n)$ and $Y_\phi(n)$ are respectively the latitude and longitude data encapsulated in AIS message received at discrete time n, and $C\widehat{X}_{\lambda(n|n-1)}$ and $C\widehat{X}_{\phi(n|n-1)}$ are respectively the latitude and longitude predicted by Kalman filter.

Variance of position innovation is computed by Kalman Filter as follows

$$S_\lambda(n) = R + C\widehat{P}_{\lambda(n|n-1)}C^T \tag{16}$$

$$S_\phi(n) = R + C\widehat{P}_{\phi(n|n-1)}C^T \tag{17}$$

where $\widehat{P}_{\lambda(n|n-1)}$ and $\widehat{P}_{\phi(n|n-1)}$ are respectively the prediction covariance matrices for latitude and longitude.

Pseudo velocity innovation is computed using the relation :

$$\nu_{sog}(n) = Y_{sog}(n) - sog_c(n) \tag{18}$$

where $sog_c(n)$ is the velocity computed with equation (12) at discrete time n and $Y_{sog}(n)$ is the velocity measurement sent in AIS messages at discrete time n. We use the term pseudo innovation for the velocity to consider that in equation (18) it is the computed velocity and not the predicted ones that is used.

To compute the variance of pseudo velocity innovation the correlation between $Y_{sog}(n)$ and $sog_c(n)$, both computed from GPS measurements, is neglected (**H5**). The following equation is applied:

$$S_{sog}(n) = \sigma^2_{Y_{sog}}(n) + \sigma^2_{sog_c}(n) \tag{19}$$

where $\sigma_{Y_{sog}}$ is set to 0.3 kt [50].

To verify the consistency of dynamic data, a Chi-squared test of conformity is applied to innovations. This test verifies the hypothesis H_0: *the measurements (Y_n was not falsified.* To verify the hypothesis, it computes the following normalized and squared innovation (20) and applies the conformity test ((21):

$$l(n) = \nu_n^T S_n^{-1} \nu_n \tag{20}$$

$$T(Z_n) = \begin{cases} 1 & \text{si } l_n \leq \gamma \; Y_n \text{ accepted } (H_0 \text{ true}) \\ 0 & \text{sinon} \qquad Y_n \text{ rejected } (H_0 \text{ false}) \end{cases} \tag{21}$$

γ depends on the false alarm probability (α) accepted. For latitude and longitude we fix $\alpha = 0.001$ and for velocity we fix $\alpha = 0.01$.

Innovation on latitude and longitude, computed by the Kalman filter ((14) and (15)), must follow a normal distribution $\nu(n) \sim \mathcal{N}(0, \sqrt{S(n)})$ because of **H2** and **H3**. So, considering a look-up table, α value and because the degree of freedom is 1, $\gamma_\phi = \gamma_\lambda = 10.8$.

Concerning velocity, the threshold γ can not be fixed considering a look-up table. Indeed, velocity innovation does not follow a normal distribution. So, a Monte Carlo is applied to find the γ value that corresponds to a false alarm probability equal to 0.01. For $\alpha = 0.01$ $\gamma_{sog} = 5.76$.

Another quantity to consider is the miss probability that represents the probability to miss a falsification i.e to accept a measurement when it is falsified and has to be rejected. This probability is represented by the variable

β and depends on the probability density function (pdf) of innovation when measurement is falsified, S_n and γ values. This value will be computed during experimentation.

The consistency checking of dynamic data strategy is summarized in Algorithm 1 and presented in steady state at discrete time n. For more clarity, only the messages from the same ship are checked. Kalman algorithm is separated into two classical steps, one step computes the predicted variables (**K_p**) written with the subscript $_{(n|n-1)}$ and the other step computes the estimated variables (**K_e**) written with the subscript $_{(n|n)}$. If no errors are noted in latitude, longitude and sog, a nothing to report (NTR) message is sent. If five errors are detected consecutively in latitude or longitude, their last estimated value is then fixed to their last measured value to readjust the filter. In Algorithm 1 $Toa(n)$ is the time of arrival (TOA) of messages at discrete time n, and nb_err_l and nb_err_L are respectively the number of errors on latitude and longitude.

Algorithm 1 Consistency checking of dynamic data

Data: $Toa(n), Y_l(n), Y_L(n), sog_m(n)$

Result: info

For each timestep n

$\Delta T(n) = Toa(n) - Toa(n-1)$

$\widehat{X}_{\lambda(n|n-1)}, \widehat{P}_{\lambda(n|n-1)} = \mathbf{K\_p}(\Delta T, \widehat{X}_{\lambda(n-1|n-1)}, \widehat{P}_{\lambda(n-1|n-1)})$

$\widehat{X}_{\phi(n|n-1)}, \widehat{P}_{\phi(n|n-1)} = \mathbf{K\_p}(\Delta T, \widehat{X}_{\phi(n-1|n-1)}, \widehat{P}_{\phi(n-1|n-1)})$

Compute $\nu_\lambda(n), \nu_\phi(n), S_\lambda(n), S_\phi(n)$ using (14, 15, 16, 17)

$l_\lambda(n) = \nu_\lambda(n)^T S_\lambda(n)^{-1} \nu_\lambda(n)$

if $l_\lambda(n) < \gamma_\lambda$ **then**

  $\widehat{X}_{\lambda(n|n)}, \widehat{P}_{\lambda(n|n)} = \mathbf{K\_e}(Y_\lambda, \widehat{X}_{\lambda(n|n-1)}, \widehat{P}_{\lambda(n|n-1)})$; $nb\_err_\lambda = 0$

else

  info="Latitude is not consistent"

  $nb\_err_\lambda = nb\_err_\lambda + 1$; $\widehat{X}_{\lambda(n|n)} = \widehat{X}_{\lambda(n|n-1)}$; $\widehat{P}_{\lambda(n|n)} = \widehat{P}_{\lambda(n|n-1)}$

  if $nb\_err_\lambda \geq 5$ **then**

    $\widehat{X}_{\lambda(n|n)}(1) = Y_\lambda(n)$; $nb\_err_\lambda = 0$

  end

end

$l_\phi(n) = \nu_\phi(n)^T S_\phi(n)^{-1} \nu_\phi(n)$

if $l_\phi(n) < \gamma_\phi$ **then**

  $\widehat{X}_{\phi(n|n)}, \widehat{P}_{\phi(n|n)} = \mathbf{K\_e}(Y_L, \widehat{X}_{\phi(n|n-1)}, \widehat{P}_{\phi(n|n-1)})$; $nb\_err_\phi = 0$

else

  info="Longitude is not consistent"

  $nb\_err_\phi = nb\_err_\phi + 1$; $\widehat{X}_{\phi(n|n)} = \widehat{X}_{\phi(n|n-1)}$; $\widehat{P}_{\phi(n|n)} = \widehat{P}_{\phi(n|n-1)}$

  if $nb\_err_\phi \geq 5$ **then**

    $\widehat{X}_{\phi(n|n)}(1) = Y_\phi(n)$; $nb\_err_\phi = 0$

  end

end

Compute $sog_c(n)$, $\sigma_{sog_c}(n)$, $\nu_{sog}(n)$ and $S_{sog}(n)$ using (18, 19)

$l_{sog}(n) = \nu_{sog}(n)^T S_{sog}(n)^{-1} \nu_{sog}(n)$

if $l_{sog}(n) < \gamma_{sog}$ **then**

  info="Velocity is not consistent"

end

3.7. Experiments

Algorithm 1 was tested on AIS messages recorded near Brest (France) during one data acquisition campaign that lasted 9 hours. From these acquisitions, 100000 messages sent by 73 ships are collected. The pre-processing step extracts, from the messages, the AIS data and recorded them on a csv data file with the messages time of arrival given by the GPS. The algorithm is applied on this csv data file.

To show the efficiency of Algorithm 1, a scenario of falsification was simulated starting from collected real data of a ship. In this scenario, inspired by [25], a ship falsified its latitude positions for 6 minutes, from the 4820^{th}s of acquisition, by adding 400 m to the longitude measured. This kind of falsification may be used by fishing boats to fish in protected zones such as Natura 2000 without revealing their true positions.

Algorithm 1 detected the falsification on longitude: innovations were several hundred meters higher than the threshold when the ship started to falsify (4820^{th}s) and when it stopped to falsify (5170^{th}s). The ship's longitude and velocity innovation evolution over time and the threshold evolution are presented respectively in Figure 4 and Figure 5. During this time interval, the longitude and velocity thresholds increased because only the predictor equations (4) and (7) were applied to predict and estimate the states and covariances, as shown in Algorithm 1. Estimator equations (5) and (10) which reduce the estimation noises were not applied. After the first five errors, the estimated longitude is reinitialized to the last measured longitude to readjust the filter.

In addition, four errors on velocity were detected. Two of them were caused by the falsifications and are surrounded by black dashed ellipses and the two other errors are caused because the threshold accepts a false alarm probability equal to 0.01;

The consistency checking of dynamic data of the other ships shows 373 errors for sog and 39 for longitude and 30 for latitude. Even if, we suppose that every alarm encountered is a false alarm, the false alarm percentage is inferior to α value for latitude, longitude and velocity. This is a consequence of the model

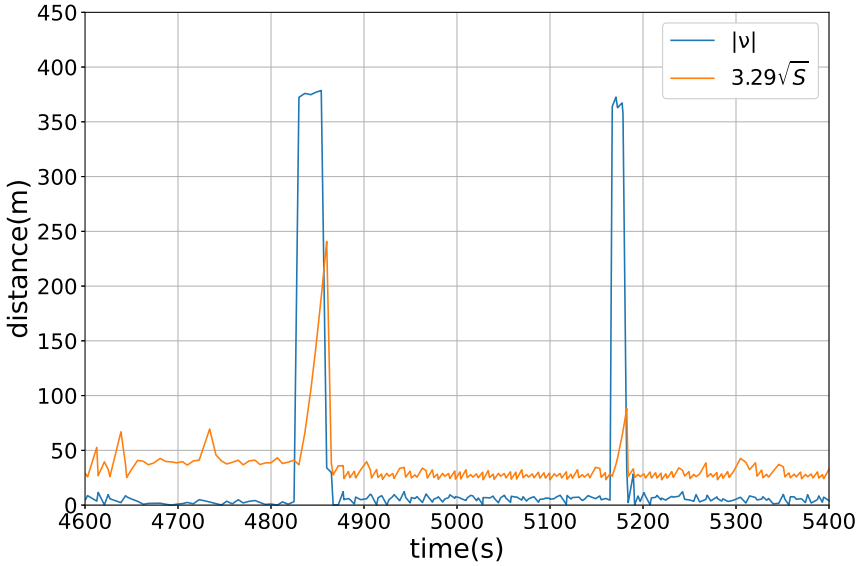


Figure 4: Evolution over time of longitude innovation and the consistency threshold.

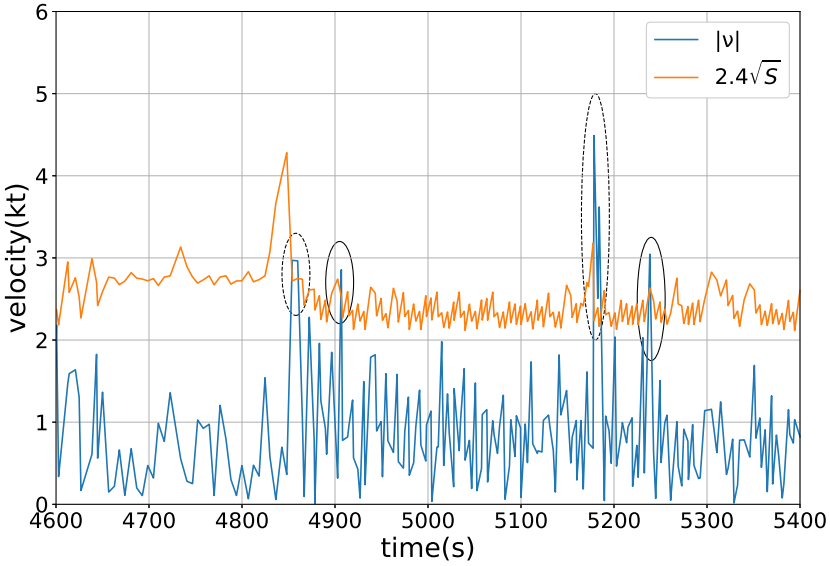


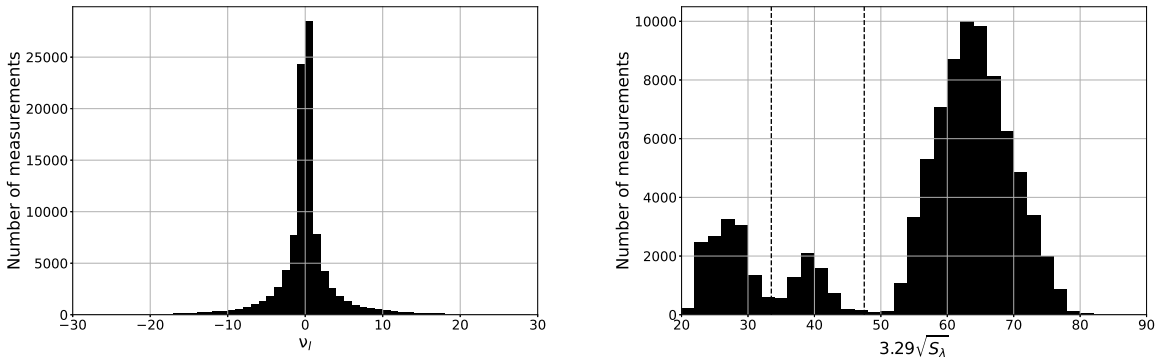
Figure 5: Evolution over time of velocity innovation and the consistency threshold.

noise used by the Kalman filter that has been overestimated to allow tracking of vessels with an acceleration equal to $1kt.s^{-1}$. In reality the tracked boats have a lower acceleration; This is particularly true for container ships.

As explained in the last paragraph, the thresholds depend on the RI which in turn depends on the environmental conditions (weather, geography) that can deteriorate and divert AIS signals, and so generate non-receipt messages. This phenomenon will make the thresholds higher than in normal environmental conditions and Algorithm 1 will become less sensitive to position falsifications. For instance, in Figure 4, at the 1980s the threshold reaches a peak equal to 266m due to non-receipt messages.

To evaluate the performances of Algorithm 1, statistical analysis of the distributions of the thresholds and innovations are computed from the messages. Histograms of the innovations and thresholds values for latitude, longitude and velocity are reported respectively in figures 6, 7 and 8. While computed thresholds (latitude, longitude and velocity) follow multimodal distribution (3 for latitude and longitude and 4 for velocity), the distribution of the computed innovation values (latitude, longitude and velocity) shows a unimodal character. The two first modes for the threshold histogram on velocity are combined for latitude and longitude. In the velocity threshold histogram four RI values can be discerned and are separated by three dotted vertical lines . These RI values (from left to right 2s, 3.3s, 6s and 10s) are presented in the next section and in Table 3.

Moreover, the standard deviations of innovations are 7.13m for latitude, 7.04m for longitude and 0.72kt for velocity. The maximum threshold values are 85m for position and 4.3kt for velocity when no message is missed (maximum RI is 10s). If we consider the threshold is fixed to these values, then only falsifications with a lower value will not be detected. Thus, considering these values and the probability density function of falsifications on position and velocity, we can compute the miss probability (β) presented in part (3.6). We suppose that these densities follow an uniform distribution as in [51] on its domain of definition. Because AIS range is 40km, the β value is insignificant



(a) (b)

Figure 6: Statistical evaluation of Algorithm 1: (a) histogram of the computed innovations on latitude (ν_λ), (b) histogram of the computed threshold on latitude ($3.29\sqrt{S_\lambda}$).

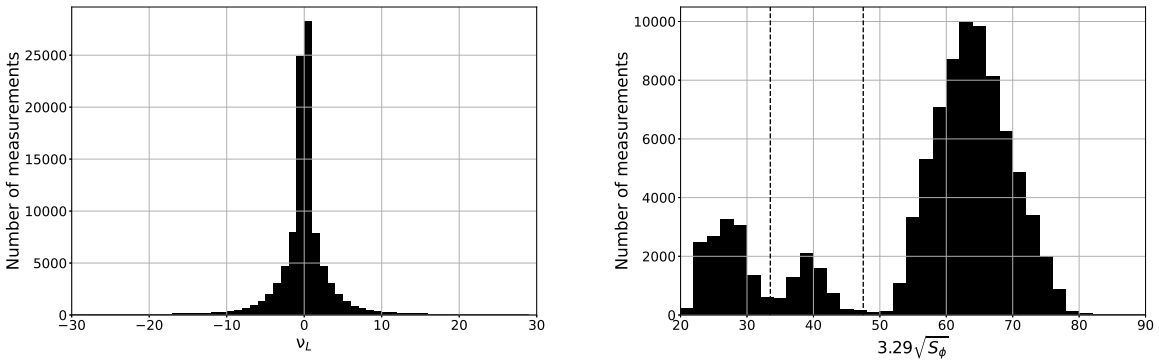
for latitude and longitude. Concerning velocity, its values vary between 0 and 40kt, so $\beta = \frac{4.3}{40} = 0.11$. This is summarized in the following table 1. Note β is majorised because we take the maximum threshold but this gives an idea of the test power. Thus, these tests are selective, particularly for position and can be applied to detect falsifications on dynamic data.

Table 1: H_0 and H_1 testing for sog, latitude and longitude.

	sog		λ ; ϕ	
	H_0 true	H_1 true	H_0 true	H_1 true
H_0 **acc.**	$0.99(1-\alpha)$	$0.11(\beta)$	0.999	≈ 0
H_1 **acc.**	$0.01(\alpha)$	$0.89(1-\beta)$	0.001	≈ 1

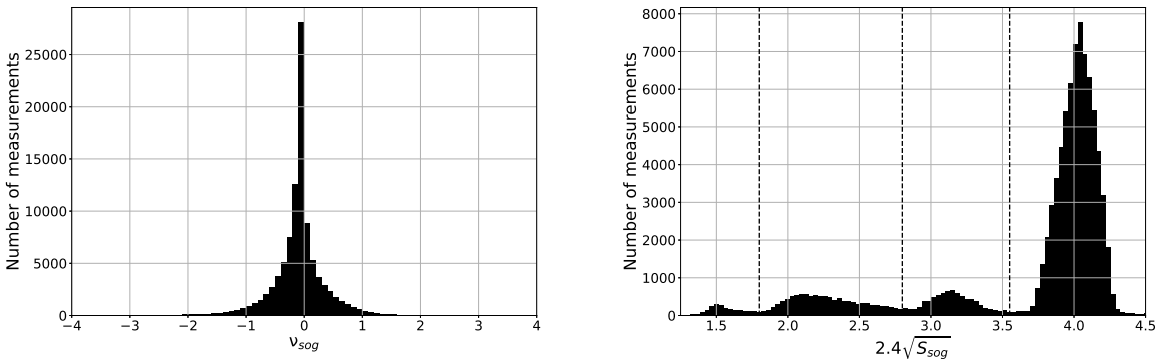
3.8. Comparison of results with other papers

In the literature, there are other works that implements tracking algorithms to detect position falsifications from AIS messages. The most interesting work with the best performances is [38] which implements an IMM filter. The use of this filter allows the conformity test to be more selective than ours. This



(a) (b)

Figure 7: Statistical evaluation of Algorithm 1: (a) histogram of the computed innovations on longitude (ν_ϕ), (b) histogram of the computed threshold on longitude ($3.29\sqrt{S_\phi}$).



(a) (b)

Figure 8: Statistical evaluation of Algorithm 1: (a) histogram of the computed innovations on velocity (ν_{sog}), (b) histogram of the computed threshold on velocity ($2.4\sqrt{S_{sog}}$).

two filters have been compared in this study [52] and the order of magnitude of the gain in precision is few meters. The comparison applied a Monte Carlo simulation and the results are presented in table 2. The table presents the root-mean-square error (RMSE) of the estimated vector on latitude and longitude, and the average of the threshold ($3.29 \times \sqrt{S_n}$) for the conformity test.

Table 2: Comparison between the Kalman (K.) and IMM filters of the RMSE of the estimated vector and the average value of the threshold [52]

	RMSE ($\widehat{X}_{n\|n}$)(m)				$\mu\left(3.29\sqrt{S_n}\right)$ (m)			
	sans man.		acc.		no man.		acc.	
	K.	IMM	K.	IMM	K.	IMM	K.	IMM
λ	4.8	4.1	6.4	6.2	53	40	54	49
ϕ	4.7	4.1	6.3	6.3	66	47	64	56

It appears, our test, presented in part 3.6, remains largely selective for our application. Indeed, position falsifications are superior to one hundred meters because it makes no sense to falsify one's position for a smaller distance. Moreover, the interest of using a Kalman filter instead of an IMM filter is that it requires half as much computation to be executed. Also, in [38], Cartesian coordinates are used to express the positions of the ships while we use here spherical coordinates to save more computation.

3.9. Remark

Systematic tracking of vessels allows to detect falsifications on position and velocity, and so insures the reliability of dynamic data. This is crucial because velocity influences TDMA protocol behavior. So, after dynamic data checking, compliance with TDMA protocol can be verified. To this end, two algorithms referred as Algorithm 2 and Algorithm 3 are developed.

4. Control of the compliance with TDMA protocol by AIS messages

Once dynamic data consistency has been checked, the respect of TDMA protocol by every tracked vessel considering either nominal reporting interval (RI)

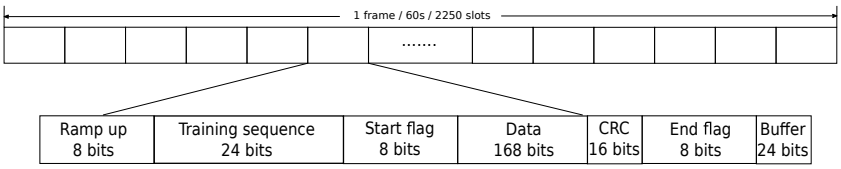


Figure 9: Packet format [43].

(Algorithm 2) or TS booking process (Algorithm 3) is controlled to detect falsifications. This is the first time in the literature that this protocol is considered to detect message falsifications.

4.1. TDMA channel access protocol

TDMA protocol allows several users to share the same frequency channel by dividing the signal into several TS. The users send messages in rapid succession, one after the other, each using its own TS. The standard given in [43] defines this protocol for AIS communications. AIS uses a common time reference, based on UTC, and the frame concept. A frame is one minute long, its start and stop coincide with the UTC minute and is divided into 2250 TS, ranging from 0 to 2249. The default length of a message transmission occupies one TS; the transmitter turns on the radio frequency power at TS start, and turns off after the last bit of the transmission packet. Every packet has an identical structure, compliant with the general high-level data link control one, plus a training sequence, as illustrated in Figure 9. A check of the packet integrity is implemented and uses the cyclic redundancy check 16-bit polynomial to calculate the checksum.

Data embedded in the packets depend on the message type sent (27 types). Position report messages have a type equal to 1, 2 and 3. Packet transmissions are made alternately to channel A (161, 975 MHz) and B (162, 025 MHz). The TDMA protocol is split into four different access schemes to the frequency channels. The ship dynamics and mode of operation determine the access scheme to be used. The access scheme indicates how a station may select slots for transmission of its messages.

The access schemes can be self-organized TDMA (SOTDMA), incremental

TDMA (ITDMA), random access TDMA (RATDMA) and fixed access TDMA (FATDMA). SOTDMA is the basic scheme used for scheduled repetitive transmissions, e.g to transmit position reports, mainly from a ship when it is not maneuvering. ITDMA is used during maneuvering, network entry phase, or for a non-repetitive message. RATDMA has a random access to the AIS communication system. It is used when a ship needs to allocate a slot that has not been pre-announced. This is generally done for the first transmission slot during data link network entry, or when the RI has to be changed. FATDMA only concerns base station communication which will not be considered us in this study.

4.2. Algorithm 2: Control of nominal RI defined by AIS standard

Messages are received following a RI that depends on the velocity of the corresponding vessel and its course, as presented in Table 3 extracted from the AIS standard [43]. When a vessel is not maneuvering, communication state used is SOTDMA and message identity (`id`) is equal to 1 or 2. When it is manoeuvring, communication state is ITDMA and `id` is equal to 3. When the vessel is at anchor or moored the Navigation Status (`Navs`) is equal to 1 or 5. Thus, these data are used to know the expected RI as presented in Table 3 column *Characteristics*. They are explained in more details in the AIS standard.

It should be noted that in order to affirm that a vessel is not maneuvering it is necessary that the identity of the two consecutive messages used to calculate the RI have an identity equal to 1 or 2. In addition, the two consecutive messages used to calculate the RI must have the same Navigation Status. During their navigation sailing boats may switch from sailing to motorized navigation. During this transition phase, messages with the Navigation Status (`Navs`= 0) and (`Navs`= 8) are transmitted successively. The message transmission period is therefore divided by 2 so that the messages associated with each navigation status are transmitted at the correct period.

RI consistency will be checked for every message by Algorithm 2. If RI does not comply with the standard, shown in Table 3, an alert will be sent. RI accuracy is $\pm 20\%$ when the ship is not manoeuvring as explained by the standard

and presented in part (4.3.1). When the ship is manoeuvring experimentations show that RI accuracy is ±50%.

The algorithm is sensitive to poor environmental conditions. Poor environmental conditions increase the probability of non-receipt messages which makes RI different from RI fixed by the standard. This is why, we make a difference between alerts reporting a RI that is a multiple of RI specified by standards (alert 21), which is caused by a non-receipt message, and alerts reporting a RI that is not a multiple of RI specified by standards (alert 22).

Table 3: Shipborne mobile equipment reporting [43]

Ship's dynamic conditions	**RI**	**Characteristics**
Ship at anchor or moored and not moving faster than 3 kt	3 min	*Navs*==1 OR *Navs*==5
Ship at anchor or moored and moving faster than 3 kt	10 s	*Navs*==1 OR *Navs*==5
Ship 0-14 kt	10 s	$id_{n-1} == id_n == 1$ OR 2
Ship 0-14 kt and changing course	3 $\frac{1}{3}$ s	other
Ship 14-23 kt	6 s	$id_{n-1} == id_n == 1$ OR 2
Ship 14-23 kt and changing course	2 s	other
Ship > 23 kt	2 s	$id_{n-1} == id_n == 1$ OR 2
Ship > 23 kt and changing course	2 s	other

4.3. Algorithm 3: control of the respect of TS booking defined by TDMA protcol

Every position report message has a communication state equal to SOTDMA or ITDMA. The communication state incorporates dedicated data (`STO`, `Offset`, `Keep flag` and `Slot Increment`) to pre-announce the TS it will use and avoid messages collisions. Algorithm 3 verifies that each received message has been booked by the communication state data. Before presenting this algorithm, we first introduce SOTDMA access scheme and the data sent with SOTDMA and ITDMA communication state to book next TS.

4.3.1. SOTDMA access scheme

A general view of the TS map access conducted by a ship to transmit AIS messages is shown in Figure 10 where a part of two frames, one for every channel, is splitted into TS. The nominal increment (NI) corresponds to RI (Table 3) but is expressed in TS number (1 TS= 26.7ms). The nominal slots (NS), shown in black in Figure 10, are defined considering NI and nominal start slot (NSS). NSS is, for each channel, the first TS used by a ship to transmit a message on the channel and serves as a starting point to fix NS considering RI. NS are the centers of selection intervals (SI) in which nominal transmission slots (NTS), shown in darker gray in Figure 10, are selected according to a uniform law. Their width are equal to 0.2× NI and are shown in the lightest gray in Figure 10. NTS define the TS during which messages are sent. Parameters NSS, NS, SI, and NI are kept constant as long as the RI keeps constant. However, if RI is changed (not temporary), then these parameters are also changed.

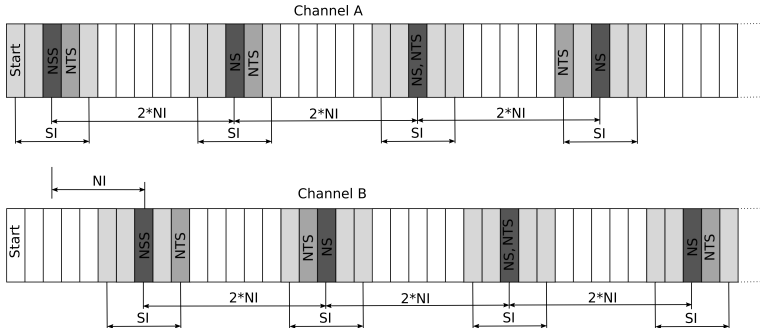


Figure 10: Diagram of TDMA protocol [43].

4.3.2. SOTDMA communication state

For SOTDMA communication state, the following pattern is applied, and data `STO` and `Offset` are sent to book the next NTS:

- When a NTS is determined, a number, called slot time-out (`STO`) between 3 and 7 is randomly generated which specifies the number of remaining frames for which this NTS (slot number) will be used on the same channel;

- The `STO` corresponding to a NTS is decremented at each message transmission ie. at each frame;

- When the `STO` value is 0, a new NTS must be selected. It is selected randomly in the SI with center NS of the next frame in the same channel. The `Offset` from the current NTS to the new NTS should be calculated and assigned, according to the formula: `Offset`= $\text{NTS}_{new} - \text{NTS}_{current} + 2250$, as well as a new `STO`.

When a new NTS is generated (`STO`= 0) it can only be determined from the TS not previously reserved by the other ships.

4.3.3. ITDMA communication state

For ITDMA communication state the following pattern is applied, and data `Keep flag` and `Slot increment` (`Slot incr.`) are sent to book the next NTS:

- `Keep flag` is set to 0 or 1. When it is fixed to 1, it informs that the same NTS remains allocated for one additional frame on the same channel. When it is fixed to 0, it informs that the same NTS will be free for the next frame;

- `Slot Incr.` indicates the increment of TSs from the current NTS to the new NTS, on the same channel, according to the formula: `Slot incr.`$=\text{NTS}_{new} - \text{NTS}_{current}$.

4.3.4. Implementation of the TDMA booking process

We implement the TDMA booking process in Algorithm 3 to know the booked TS, as shown in Figure 11. The process is applied ship wise using the data presented above to determine their booked NTS. The NTS are inserted into a list that is created for every channel (`ListNTS_A` for channel A and `ListNTS_B` for channel B). These lists are updated when a new frame is starting which happens every UTC minute. During the update, 2250TS is subtracted from every NTS value in the two lists, and after, every NTS that has a negative value

is removed from the two lists. This step is done during the step called *strategy parameters update* in Figure 1.

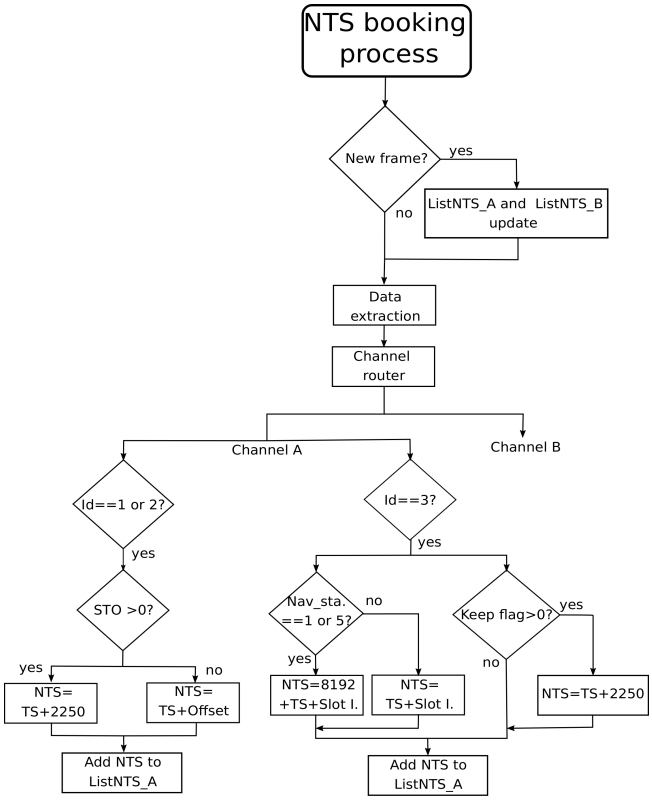


Figure 11: Diagram of the NTS booking process.

In addition, the diagram is shown in the case when a message was received from the channel A. The same process is applied if a message comes from channel B, but, in this case, the NTS is added to the list `ListNTS_B`. It is the router block that sends the messages to their corresponding channel process. The TS number is determined thanks to TOA given by a computer connected to the AIS that receives messages and is given by:

$$\mathrm{TS} = \mathrm{round}\left(\mathrm{mod}\left(\frac{\mathrm{TOA}_s}{60}\right)\frac{2250}{60}\right) \tag{22}$$

where mod is the rest of the division and TOA_s is message TOA in second. Computed TS numbers need to be synchronized to TS numbers of TDMA pro-

tocol. This can be done using `Slot number` data that are encapsulated in every AIS messages using SOTDMA communication state with an even `STO`. Examples that illustrate the TDMA process booking are shown in Tables 4 and 5 from subsection 5.1.

4.3.5. Algorithm

It checks that every TS, during which a message is received, corresponds to an NTS previously reserved by the same ship. If it is incorrect, an alert (alert 3) will indicate that the ship is not compliant with TDMA protocol. The algorithm does not consider messages from RATDMA access scheme because they can not be predicted. These messages can either be the first message sent on every channel during maneuvering actions or during data link network entry, or be characterized by the `repeat_indicator` of the message equal to 1. Note that, like booking process, the algorithm is applied ship and channel wise independently. In addition, it is only applied to a vessel if it has been sending messages for more than one minute. Indeed, the initialization of the booking process takes one minute.

5. Experiments

5.1. Application on real messages generated by one ship

For easy understanding of booking process, the TS used by a ship to send data are shown in Figure 12. The ship uses SOTDMA, ITDMA and RATDMA access schemes to send data. Visually we can discern two RI in Figure 12, one RI is equal to 225 TS and the other is equal to 75 TS. In addition, this figure gives an idea of SI values.

In addition, TDMA data sent during two consecutive frames are reported in Tables 4 and 5. When the `id` is equal to 1, SOTDMA communication state is applied, and when it is equal to 3, ITDMA communication state is applied. `repeat indicator` and `keep_flag` data were not displayed in the tables, because they do not intervene on booking process during these two frames. When

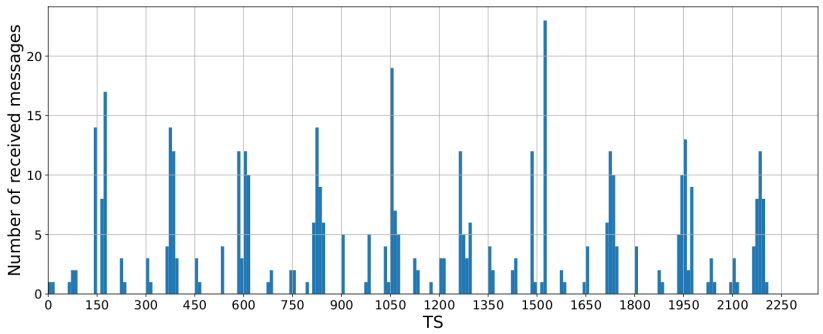


Figure 12: Histogram of the TS used by a ship.

the indicated value is "-1", data was not embedded in the message. RI data reported in Tables 4 and 5 were computed from messages TOA.

Using TS, `STO` and `Offset` received during frame 1 with SOTDMA communication state, we can predict the messages received during frame 2 at the TS 140, 375, 589, 847, 1051, 1290, 1525, 1956 and 2180. Messages received during the TS 1971 and 2044 applied RATDMA access scheme because the ship started maneuvering. RI had to be temporary changed only for the duration of the manoeuvrer. As mentioned above, this access scheme sends messages randomly that could not be reserved before. The `Slot Incr.` (137 and 281) received during these two messages, allow booking process to reserve the next message received during the TS equal to 2108=1971+137 and the TS equal to 75=2044+281-2250. Applying the same rules and using the TS and `Slot I.` data, every message using ITDMA communication state (message with an id equal to 3) was booked before being received during these two frames.

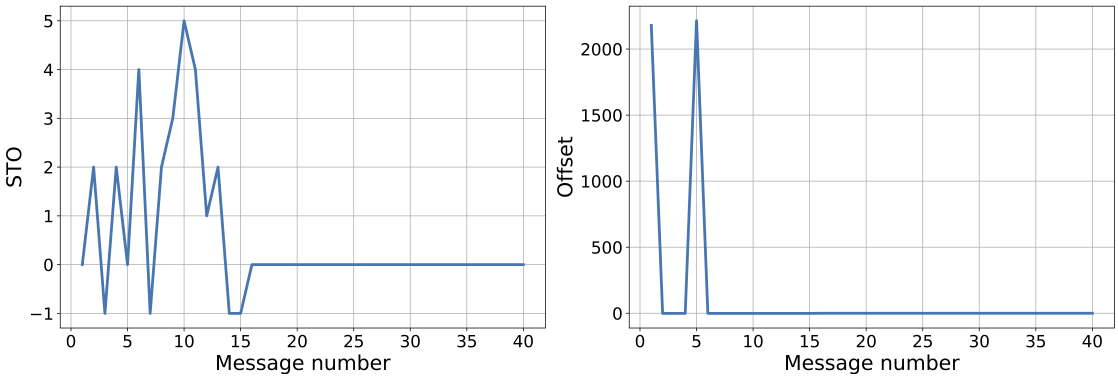
One error is detected during the frame 2. Algorithm 2 detects that the AIS message received at TS 1956 had a RI too high. This error was produced by technical deficiencies (false alert) that caused a non-receipt of the message during the TS equal to 1728.

5.2. Analysis of real falsified AIS messages

We show the effectiveness of our detection strategy on real AIS data for which there is compelling evidence that the positions have been falsified [14]. The falsifications were reported by NATO and concern a warship sailing in the Black Sea [14]. According to the transmitted positions, the ship left Odessa and sailed directly to Sevastopol, approaching within two nautical miles of the port entrance. However, there is clear evidence, using live webcam feeds, that the warship did not leave Odessa.

The AIS messages were collected from a satellite which implies a long delay between each message (generally between 500s and 1500s) and therefore many non-receipts of message. This long time induces a high number of 21, 22 and 3 alerts because the maximum RI value, imposed by the AIS standard, is 10s when the vessel is moving. Therefore, there is no interest to apply our strategy in this case: our strategy is applied to messages received from a transceiver located on a ship or on a coastal base station.

Nevertheless, the observation of SOTDMA communication state data, and particularly the `STO` and `Offset` values, displayed in Figure 13, shows that booking process is not respected. Indeed, from the 16^{th} message, even if the `STO` remains equal to 0, the `Offset` also remains equal to 0. However, this is contrary to the standard, because in this case, no TS is reserved to transmit the next message. In particular, we observe that this is not the case for the `STO` and `offset` data displayed in the Figure 14. In this figure it is represented data sent by another warship moving in the same area and whose positions have not been falsified. Moreover, in the tables 4 and 5, when `STO` is equal to 0, `Offset` has a value greater than 0 to book the TS used to send a message in the next frame. The 16^{th} message corresponds to the departure from Odessa towards Sevastopol and the beginning of the falsification of the AIS data. Thus, if the Algorithm 3 had been applied to messages received from a transceiver located in close proximity to the suspect vessel (< 40km), it would have detected these errors. The conclusions of NATO [14] would have been confirmed. The trajectory of the warship that falsified its positions is displayed in the Figure 15.



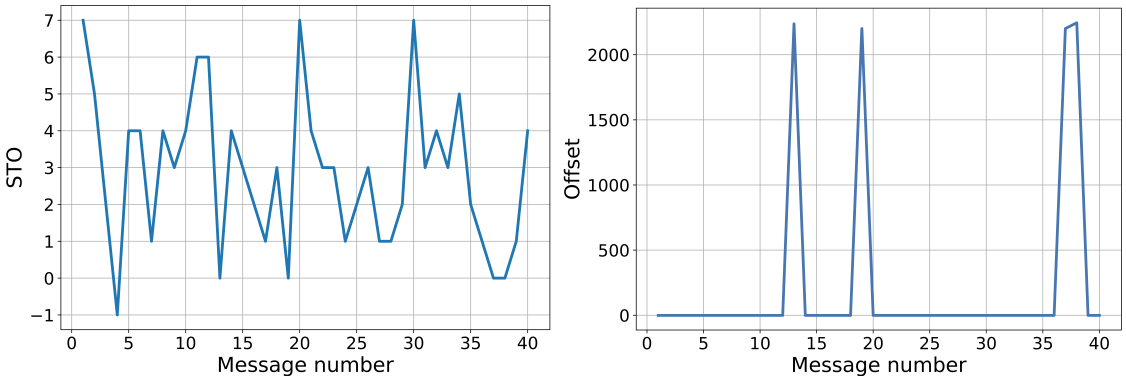
(a) (b)

Figure 13: Trajectory with falsified messages: (a) STO evolution considering message number, (b) Offset evolution considering message number.

Finally, the fact that `STO` and `Offset` remain to 0 during the whole falsified trajectory shows that these AIS data have been fixed without considering the SOTDMA booking process. It is reasonable to think that this is not a particular case and that, often, when a user transmits falsified or spoofed AIS messages, it does not respect the TDMA protocol at all. The alert percentage is then equal to 100%. This fact demonstrates the relevance of our strategy to detect spoofing or falsification by checking the compliance of the messages with TDMA protocol.

5.3. Analysis of real messages generated by a set of ships

We apply the strategy to 100000 messages collected in Brest and used to test the Algorithm 1 (subsection 3.7). We only consider the alerts returned by Algorithm 2 and 3. The detected alerts from Algorithm 1's were already presented in the experiment subsection 3.7. The algorithm provid 7771 alerts 21, 5624 alerts 22 and 6355 alerts 3. Most of the errors come from technical deficiencies and environmental conditions that cause no reception of messages. Nevertheless, the number of alerts is high, this is why we compute, for every vessel, the alerts percentage in relation to the received messages to make the



(a) (b)

Figure 14: Trajectory with messages without falsification: (a) STO evolution considering message number, (b) Offset evolution considering message number.

difference between true and false alerts. The alert percentage is a moving average computed over the last 15 frames when, at least, the number of received messages is higher than the number of messages received during three full frames. This condition is imposed to ensure that we are in a steady state and to have a sufficient number of messages to compute the moving average.

Vessel positions are presented in Figure 16. The ships positions for which an error has been detected by algorithms 2 and 3 are presented in figures 17, 18

Figure 15: Trajectories in the Black Sea of the warship that falsifies its trajectory.

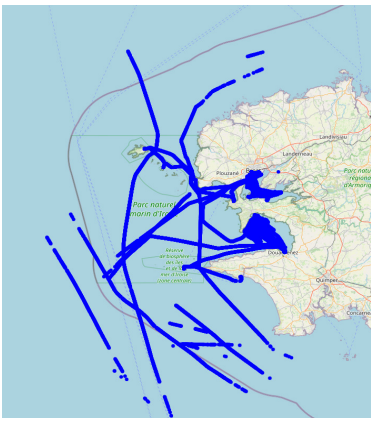


Figure 16: Vessel positions sent in messages

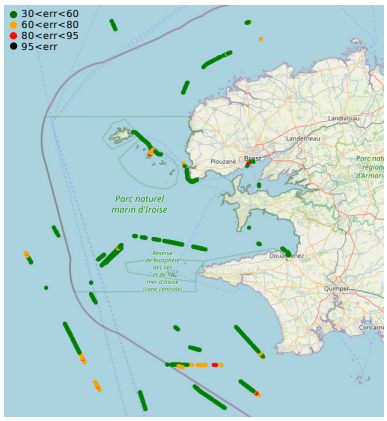


Figure 17: Vessel positions when an alert 21 is detected

and 19. To help the understanding four colors are used to represent the errors percentage. When the error percentage is between 30 and 60% a green color is used, when it is between 60 and 80% a yellow color is used, when it is between 80 and 95% a red color is used and when it is superior to 95 a black color is used.

Rarely, the error percentage exceeds 80%, and when it happens, it lasts for a short period. Thus, if for several minutes this percentage is exceeded, as it was the case for the example of falsified messages in the Black Sea, the vessel must be checked. Alerts from Algorithm 1 have to be considered suspect if they concern five consecutive messages from a same ship. This separation between false alerts (technical deficiencies) and true alerts (falsification and spoofing) is simple but efficient, and can be improved, implementing algorithms from the detection theory.

Finally, to check the real time performances of the strategy we compute its execution time to check the 100000 recorded messages. The CPU is a standard Intel Core I5 processor at 1.7GHz with 16Gb RAM. The execution time is 117s: on average, the execution time is 1.5 ms per message. This value respects the real time condition of the algorithm because, in the worst case (maximum occupation rate of the channels' TS), two messages are received every 26.7 ms.

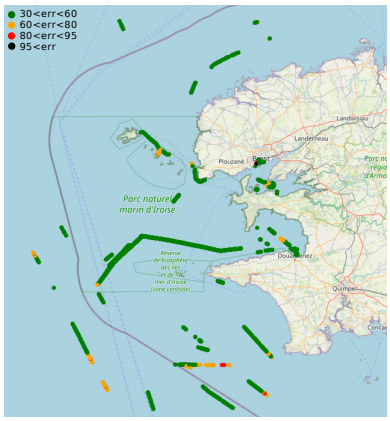


Figure 18: Vessel positions when an alert 22 is detected

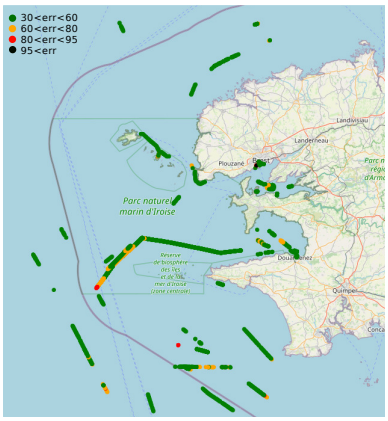


Figure 19: Vessel positions when an alert 3 is detected

Table 4: TDMA scheme data used to book TS during the frame 1.

id	1	1	1	1	1	1	1	1	1	3	3	3	1
TS	140	375	589	847	1051	1290	1525	1728	1956	1971	2044	2108	2185
STO	7	1	3	5	4	4	7	1	3	-1	-1	-1	0
Offset	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	2245
Slot Incr.	-1	-1	-1	-1	-1	-1	-1	-1	-1	137	281	148	-1
Sog (kt)	18.4	18.3	18.3	18.3	18.3	18.4	18.5	18.5	18.5	18.5	18.6	18.5	18.4
RI	205	235	214	258	203	239	124	204	228	15	73	64	77
channel	A	B	A	B	A	B	A	B	A	A	B	A	B

Table 5: TDMA scheme data used to book TS during the frame 2.

id	3	3	1	3	3	1	3	3	1	3	3	1	3	1	1	1	1	1
TS	6	75	140	226	307	375	456	535	589	681	749	847	983	1051	1290	1525	1956	2180
STO	-1	-1	6	-1	-1	0	-1	-1	2	-1	-1	4	-1	3	3	6	2	3
Offset	-1	-1	-1	-1	-1	2247	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
Slot Incr.	301	151	-1	309	149	-1	293	146	-1	302	0	-1	0	-1	-1	-1	-1	-1
Sog (kt)	18.6	18.4	18.4	18.5	18.5	18.5	18.6	18.6	18.6	18.7	18.7	18.7	18.7	18.8	18.7	18.8	18.6	18.6
RI	71	69	65	86	81	68	81	79	54	92	68	98	135	68	239	235	432	224
Channel	A	B	A	B	A	B	A	B	A	B	A	B	B	A	B	A	A	B

6. Discussion

In this work, a detection strategy of falsifications and spoofing of AIS messages has been developed. This strategy is based on the checking of TDMA protocol compliance, which it is a first in the literature to best of our knowledge. The proposed strategy has been validated on real data and has real time performances.

The obtained results highlight that our strategy is well adapted to detect message falsifications. Indeed, on the one hand, the strategy is sensitive to falsifications superior in mean to 80m for position and 4.50kt for velocity. On the other hand, the check of messages compliance with TDMA protocol is appropriated to detect falsified messages. Our experimentation shows that when the alert percentage of messages that do not respect TDMA protocol is above 80% during several minutes, these errors are intentional and the corresponding vessel has to be controlled.

In some conditions, algorithms 2 and 3 can be by-passed. Indeed, if false positions are introduced at GPS sensor input of AIS transceiver or false static data are changing manually, like identity, the emitted AIS messages will comply with TDMA protocol, and so algorithms 2 and 3 will not detect these falsifications. However, in this case, Algorithm 1 will detect jump in position introduced by

these position falsifications. In addition, falsified AIS messages can be emitted from an other system than the AIS transceiver. This can be done, for example, by a software defined radios (SDR) connected to an USRP, as is done in [8]. In this case, the malicious user has to implement TDMA protocol and apply it to its messages not to be detected by algorithms 2 and 3. Note that TDMA protocol implementation requires a significant amount of time and effort.

To finish, this highlighted limitation can be filled by the use of another strategy applied jointly to our strategy. For example, it would be interesting to consider the radiometric signature of the transceiver to detect falsifications of ships identity. In addition, the energy variation of the received signal can be considered to control the distance variation between AIS emitter and receiver, and so detect messages spoofing. To improve the separation between false alerts (technical deficiencies) and true alerts (falsification and spoofing), algorithms from the detection theory could be exploited. To make easy the integration of new methods and algorithms with our strategy, the Matlab code is open source [44].

7. Conclusions and future work

In this work, a detection strategy of falsifications and spoofing of AIS messages based on the checking of TDMA protocol compliance has been developed. In addition, this strategy implements a Kalman filter that tracks ships motion. The strategy represents a first in the literature, has been validated on real data and has real time performances. Thanks to it, the reliability of AIS data transmitted increases and malicious users now have to uphold TDMA protocol and impose a consistent position and velocity dynamic evolution in the AIS messages they spoof or falsify. For more robustness against attacks, and particularly for subtle attacks, other verifications should be included. It would be interesting to consider finger printing of transceiver to detect falsifications of ship identity.

References

[1] K. Dogancay, Z. Tu, G. Ibal, Research into vessel behaviour pattern recognition in the maritime domain: Past, present and future, Digital Signal Processing 119 (2021) 1–7.

[2] Vessel Database Search - Discover more than 500000 ships.
URL https://www.fleetmon.com/vessels/

[3] E. Tu, G. Zhang, L. Rachmawati, E. Rajabally, G.-B. Huang, Exploiting AIS data for intelligent maritime navigation: A comprehensive survey from data to methodology, IEEE Trans. Intell. Transp. Syst. 19 (5) (2017) 1559–1582.

[4] P. Silveira, A. Teixeira, C. G. Soares, Use ofAIS data to characterize marine traffic patterns and ship collision risk off the coast of Portugal, J. Navig. 66 (6) (2013) 879.

[5] J. M. Mou, C. Van der Tak, H. Ligteringen, Study on collision avoidance in busy waterways by using AIS data, Ocean Eng. 37 (5-6) (2010) 483–490.

[6] A. Sidibé, G. Shu, Study of automatic anomalous behaviour detection techniques for maritime vessels, J. Navig. 70 (4) (2017) 847–858.

[7] M. Riveiro, G. Pallotta, M. Vespe, Maritime anomaly detection: A review, Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 8 (5) (2018) 1–34.

[8] M. Balduzzi, A. Pasta, K. Wilhoit, A security evaluation of AIS automated identification system, in: Proc. Annual Comput. Sec. Appl. Conf., 2014, pp. 436–445.

[9] Systematic data analysis reveals false vessel tracks (2021).
URL https://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/

[10] A. Androjna, M. Perkovič, I. Pavic, J. Mišković, AIS data vulnerability indicated by a spoofing case-study, Appl. Sc. 11 (11) (2021) 5015.

[11] S. Collin, J.-J. Szkolnik, A. Boudraa, D. Daré-Emzivat, C. Ray, Détection d'anomalies des signaux AIS à partir de la fréquence instantanée, in: Colloque GRETSI, 2017, pp. 1–4.

[12] E. Alincourt, C. Ray, P.-M. Ricordel, D. Dare-Emzivat, A. Boudraa, Methodology for AIS signature identification through magnitude and temporal characterization, in: OCEANS'15 MTS/IEEE, 2016, pp. 1–4.

[13] C. Ray, C. Iphar, A. Napoli, R. Gallen, A. Bouju, DeAIS project: Detection of AIS spoofing and resulting risks, in: OCEANS'15 MTS/IEEE, 2015, pp. 1–6.

[14] Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base - USNI News, https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base.

[15] M. Caprolu, R. Di Pietro, S. Raponi, S. Sciancalepore, P. Tedeschi, Vessels cybersecurity: Issues, challenges, and the road ahead, IEEE Comm. Mag. 58 (6) (2020) 90–96.

[16] C. Iphar, A. Napoli, C. Ray, A method for integrity assessment of information in a worldwide maritime localization system, in: OCEANS'15 MTS/IEEE, 2016, pp. 1–4.

[17] A. Harati-Mokhtari, A. Wall, P. Brookes, J. Wang, Automatic identification system (AIS): a human factors approach, J. Navig. 60 (3) (2007) 373–389.

[18] Iran, Tanzania and Falsifying AIS Signals to Trade with Syria.
URL `https://www.maritime-executive.com/article/iran-tanzania-and-falsifying-ais-signals-to-trade-with-syria`

[19] Systematic GPS Manipulation Occuring at Chinese Oil Terminals and Government Installations (2019).

URL https://skytruth.org/2019/12/systematic-gps-manipulation-occuring-at-chinese-oil-terminals-and-government-installations/

[20] S. Sotirov, C. Alexandrov, Improving AIS data reliability, in: Global perspectives in MET: Towards Sustainable, Green and Integrated Maritime Transport, 2017, pp. 237–244.

[21] Indonesia spots Chinese research vessel with tracking system off - SAFETY4SEA.
URL https://safety4sea.com/indonesia-spots-chinese-research-vessel-with-tracking-system-off/

[22] S. Sciancalepore, P. Tedeschi, A. Aziz, R. Di Pietro, Auth-AIS: Secure, flexible, and backward-compatible authentication of vessels AIS broadcasts, IEEE Trans. Dependable and Secure Computing (2021).

[23] M. Strohmeier, M. Smith, M. Schäfer, V. Lenders, I. Martinovic, Crowdsourcing security for wireless air traffic communications, in: Int. Conf. Cyber Conflict (CyCon), 2017, pp. 1–18.

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

[25] F. Katsilieris, P. Braca, S. Coraluppi, Detection of malicious AIS position spoofing by exploiting radar information, in: Int. Conf. Inf. Fusion, 2013, pp. 1196–1203.

[26] M. Vespe, M. Sciotti, F. Burro, G. Battistello, S. Sorge, Maritime multi-sensor data association based on geographic and navigational knowledge, in: IEEE Radar Conf., 2008, pp. 1–6.

[27] S. Guo, Space-based detection of spoofing AIS signals using doppler frequency, in: Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Appl., Vol. 9121, 2014, pp. 1–6.

[28] E. Alincourt, C. Ray, P.-M. Ricordel, D. Daré-Emzivat, A. Boudraa, Méthodologie d'extraction de signatures issues des signaux AIS, in: Symposium sur la sécurité des technologies de l'information et des communications, 2016.

[29] C. Ray, C. Iphar, A. Napoli, Methodology for real-time detection of ais falsification, in: Maritime Knowledge Discovery and Anomaly Detection Workshop, Michele Vespe and Fabio Mazzarella, Eds., Ispra, Italy, 2016, pp. 74–77.

[30] F. Mazzarella, M. Vespe, A. Alessandrini, D. Tarchi, G. Aulicino, A. Vollero, A novel anomaly detection approach to identify intentional AIS on-off switching, Expert Syst. Appl. 78 (2017) 110–123.

[31] M. Guerriero, S. Coraluppi, C. Carthel, P. Willett, Analysis of AIS intermittency and vessel characterization using a hidden Markov model., in: Gi jahrestagung (2), 2010.

[32] V. Brik, S. Banerjee, M. Gruteser, S. Oh, Wireless device identification with radiometric signatures, in: Proc. ACM Int. Conf. MCN, 2008, pp. 116–127.

[33] B. Ristic, B. La Scala, M. Morelande, N. Gordon, Statistical analysis of motion patterns in AIS data: Anomaly detection and motion prediction, in: Int. Conf. Inf. Fusion, 2008, pp. 1–7.

[34] M. Redoutey, E. Scotti, C. Jensen, C. Ray, C. Claramunt, Efficient vessel tracking with accuracy guarantees, in: Int. Symposium on Web and WGIS, Springer, 2008, pp. 140–151.

[35] K. Jaskólski, Automatic identification system (AIS) dynamic data estimation based on discrete Kalman filter (KF) algorithm, Scientific J. Polish Naval Academy 211 (4) (2017) 71–87.

[36] P. Last, C. Bahlke, M. Hering-Bertram, L. Linsen, Comprehensive analysis of automatic identification system (AIS) data in regard to vessel movement prediction, J. Navig. 67 (5) (2014) 791–809.

[37] S. Fossen, T. I. Fossen, Extended kalman filter design and motion prediction of ships using live automatic identification system (AIS) data, in: European Conf. Elec. Eng. Comput. Sc., 2018, pp. 464–470.

[38] G. Siegert, P. Banys, C. S. Martínez, F. Heymann, Ekf based trajectory tracking and integrity monitoring of ais data, in: Proceedings of IEEE/ION PLANS 2016, 2016, pp. 887–897.

[39] F. Mazzarella, V. F. Arguedas, M. Vespe, Knowledge-based vessel position prediction using historical AIS data, in: Sensor Data Fusion: Trends, Solutions, Appl., 2015, pp. 1–6.

[40] S. Hexeberg, A. L. Flåten, E. F. Brekke, et al., AIS-based vessel trajectory prediction, in: Int. Conf. Inf. Fusion, 2017, pp. 1–8.

[41] S. Mao, E. Tu, G. Zhang, L. Rachmawati, E. Rajabally, G.-B. Huang, An automatic identification system (AIS) database for maritime trajectory prediction and data mining, in: Proc. ELM, 2018, pp. 241–257.

[42] P. Sheng, J. Yin, Extracting shipping route patterns by trajectory clustering model based on automatic identification system data, Sustainability 10 (7) (2018) 1–3.

[43] M. Series, Technical characteristics for an automatic identification system using time-division multiple access in the vhf maritime mobile band, Recommendation ITU: Geneva (2014) 1371–1375.

[44] M. Louart, TDMA method checking, https://github.com/maelic-louart/TDMA-method-checking (2021).

[45] E. Brookner, Tracking and Kalman filtering made easy, Wiley New York, 1998.

[46] Y. Bar-Shalom, X. R. Li, T. Kirubarajan, Estimation with application to tracking and navigation: theory algorithms and software, John Wiley & Sons, 2004.

[47] C.-B. Chang, J. A. Tabaczynski, Application of adaptive estimation to target tracking., Tech. rep., MASSACHUSETTS INST OF TECH LEXINGTON LINCOLN LAB (1982).

[48] E. Kaplan, C. Hegarty, Understanding GPS: Principle and Applications, Artech house, 2005.

[49] H. H. Ku, et al., Notes on the use of propagation of error formulas, J. Res. Nat. Bur. Stand. 70 (4) (1966) 263–273.

[50] T. Witte, A. Wilson, Accuracy of non-differential GPS for the determination of speed over ground, J. Biomechanics 37 (12) (2004) 1891–1898.

[51] M. Yeddanapudi, Y. Bar-Shalom, K. Pattipati, Imm estimation for multitarget-multisensor air traffic surveillance, Proceedings of the IEEE 85 (1) (1997) 80–96.

[52] M. Louart, J.-J. Szkolnik, A.-O. Boudraa, J.-C. Le Lann, F. Le Roy, Stratégie de détection des falsifications des positions des messages ais basée sur l'application du filtre imm, in: Gretsi'22 XXVIIIème Colloque Francophone de Traitement du Signal et des Images, 2022.