INTERNATIONAL JOURNAL OF SATELLITE COMMUNICATIONS AND NETWORKING
Int. J. Satell. Commun. Network. 0000; **00**:1–21
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/sat

CRC-based detection algorithms for AIS signals received by satellite

Raoul Prévost[1,2], Martial Coulon[1], David Bonacci[2], Julia LeMaitre[3], Jean-Pierre Millerioux[3] and Jean-Yves Tourneret[1]

[1]*University of Toulouse, INP-ENSEEIHT/IRIT, 2 rue Charles Camichel, BP 7122, 31071 Toulouse cedex 7, France, {martial.coulon, jean-yves.tourneret}@enseeiht.fr*
[2]*TéSA, 14-16 Port Saint-Etienne, 31000 Toulouse, France, {raoul.prevost, david.bonacci}@tesa.prd.fr*
[3]*CNES, 18 Avenue Edouard Belin, 31400 Toulouse, France, {julia.lemaitre, jean-pierre.millerioux}@cnes.fr*

SUMMARY

This paper addresses the problem of demodulating signals transmitted in the automatic identification system (AIS). The main characteristics of such signals consist of two points: i) they are modulated using a trellis-coded modulation, more precisely a Gaussian minimum shift keying (GMSK) modulation; ii) they are submitted to a bit-stuffing procedure, which makes more difficult the detection of the transmitted information bits. This paper presents several demodulation algorithms developed in different contexts: mono-user and multi-user transmissions, and known/unknown phase shift. The proposed receiver uses the cyclic redundancy check (CRC) present in the AIS signals for error correction, and not for error detection only. Using this CRC, a particular Viterbi algorithm, based on a so-called extended trellis, is developed. This trellis is defined by extended states composed of a trellis-code state and a CRC state. Moreover, specific conditional transitions are defined in order to take into account the possible presence of stuffing bits. The algorithms proposed in the multi-user scenario present a small increase of computation complexity with respect to the mono-user algorithms. Some performance results are presented for several scenarios in the context of the automatic identification system and compared with those of existing techniques developed in similar scenarios. Copyright © 0000 John Wiley & Sons, Ltd.

Received ...

KEY WORDS: AIS; CRC; trellis codes; error correction; bit-stuffing; Viterbi decoding; multi-user detection; interference cancellation

1. INTRODUCTION

The objective of this paper is to present different demodulation algorithms for AIS signals received by a satellite. The automatic identification system (AIS) is a self-organized time division multiple access (TDMA) communication system, which has been primarily designed in order to avoid collisions between large vessels [1]. This system has not been initially conceived for satellite reception. However, for global supervision of the maritime traffic, it is interesting to investigate the demodulation of AIS signals received by a satellite. Given the high noise and interference levels affecting signals received by satellite, new demodulation techniques have to be developed in order to obtain acceptable packet error rates (PER) at the lowest E_b/N_0. The reception of AIS signals by satellite was investigated in [2, 3], where an enhanced sensitivity receiver was designed. This paper proposes new demodulation strategies based on an error correction method using the

Contract/grant sponsor: DGA, CNES

cyclic redundancy check (CRC) as a source of redundancy. Two different scenarios are considered: Scenario 1 is for mono-user transmission with a perfect phase recovery. This scenario provides a reference to which can be compared suboptimal demodulators. Scenario 2 generalizes scenario 1 and studies another demodulation algorithm for the cases where a phase shift occurs during the transmission, or when the modulation index is unknown and possibly time-varying. The third scenario is proposed for multi-user applications. An interference mitigation method is exploited to mitigate the effects of multiple signals affecting the desired one.

The specificities of the AIS signals considered in this article are: i) the transmitted bit sequence contains a CRC part, and is modulated using a trellis-coded modulation, more precisely the Gaussian minimum shift-keying (GMSK) modulation; ii) this sequence may also contain stuffing bits, inserted after the CRC calculation. The objective of the bit stuffing procedure is either to generate additional transitions, which helps to re-synchronize the receiver clock, or to avoid some specific codewords. Note that the bit stuffing mechanism is present in other systems than AIS, e.g., the universal serial bus (USB), the high level data link control (HDLC) or X.25 systems and the integrated service digital network (ISDN).

The demodulation algorithms proposed in this article all consist of using the CRC not as an error detection tool, but rather as a correction method. While initially conceived for error detection purposes, the CRCs have also been recently proposed for error correction. For instance, the difference between the received CRC and the CRC computed from the received data is used as a syndrome and constitutes the basis of the error correction strategy developed in [4]. This approach, which allows the receiver to correct one single erroneous bit, has been generalized in [5] for the case of two erroneous bits. A strategy suitable for any bit error number has been proposed in [6], where the low confidence bits are corrected in priority. In [7], the error correction is based on the bit error probability, by modifying the high error probability bits until the received and re-computed CRCs are equal. Finally, a strategy using a convolutional code with the CRC has been proposed in [8].

However, these techniques are not appropriate for data containing bit stuffing. New strategies must therefore be investigated. The objective of this paper is to propose CRC-based detection methods for systems involving trellis coding (TC) and bit stuffing. In the mono-user scenario, the first proposed detection method assumes a perfect phase recovery and develops a particular Viterbi algorithm, based on an extended trellis defined by extended states. These extended states are composed of CRC states and TC states. The possible stuffing bits are managed by considering specific conditional transitions in the extended trellis. Note that this approach has recently resulted in the submission of two patents [9, 10].

One next considers the case where the phase shift generated by the channel is unknown by the receiver, and has to be estimated. Phase recovery is a very challenging problem for AIS signals: indeed, the modulation index is subjected to large fluctuations from an AIS equipment to another, due to the electronic of the transmitter, while residual frequency offset and phase noise effects appears to be second order problems. The AIS system is an already operational system, for which non coherent demodulators can be applied, keeping large margins with respect to the link budgets between vessels: in that case, fluctuations of the modulation index is not a major issue. However, considering satellite receptions, where the objective consists of optimizing the received E_b/N_0 using a coherent demodulator, specific methods have to be developed in order to handle the modulation index fluctuations. The approach investigated in this article is based on a Per-Survivor Processing technique [11]. Since the computational complexity must be controlled (because of the large considered trellis [12]), a simple phase estimation is performed, which does not require integration. Hence, the demodulator previously developed, based on the extended trellis and the conditional transitions, is generalized to incorporate the phase recovery procedure. The resulting algorithm, which jointly estimates the phase and demodulates the data, is then compared with an alternative approach using a non data aided (NDA) phase recovery algorithm followed by the demodulation/decoding of [12].

One next studies a multi-user transmission, by considering first perfect phase recovery. In that case, the first mono-user algorithm could theoretically be generalized, by developing an extended trellis involving all extended states of all users. However, this approach would result in

DOI: 10.1002/sat

an exponential increase of the computation complexity, with respect to the mono-user method. Therefore, this generalization is not practically tractable. Instead, the proposed multi-user technique consists of a preliminary step, whose objective is to reduce the multi-user interference. The mono-user algorithm is then applied to the signal obtained after this interference mitigation. Hence, the multi-user signal, after interference reduction, is processed as a mono-user signal, which barely increases the computation complexity with respect to the mono-user scenario. Note that parts of this study have been considered in [12] and [13] for the mono-user scenario with perfect phase recovery, in [14] for the mono-user scenario with joint phase estimation, and in [15] for the multi-user scenario. The present article proposes a more detailed presentation of the different algorithms, deeper result analysis and discussions, along with extended simulation results.

The article is organized as follows. Section 2 recalls some important CRC properties useful for the proposed algorithm, presents the bit stuffing mechanism, as well as the general signal model. Section 3 focuses on the mono-user scenario with perfect phase recovery, for which the specific Viterbi algorithm, based on an extended trellis and conditional transitions, is developed. Section 4 addresses the phase estimation problem, and presents the joint phase estimation/demodulation algorithm. The case of multi-user transmission is considered in section 5, which presents the interference reduction method and the generalization of the mono-user receiver. It also deals with the case of an unknown phase shift for the user of interest, by applying the previous phase estimation. The proposed algorithms are exemplified in section 6, where some simulation results obtained from a realistic AIS simulator (developed by the CNES of Toulouse, France) are reported. The methods developed for the mono-user and the multi-user scenarios are compared with other techniques proposed in the literature. Discussions and conclusion are reported in section 7.

2. TRANSMITTER DESIGN AND CHANNEL MODEL

This paper considers the cases of mono and multi-user transmissions. For both cases, the AIS transmission scheme of a single user is illustrated in Fig. 1. A CRC is computed from the 168 information bits and is concatenated to these bits, yielding a binary sequence on which the bit stuffing mechanism is applied. The resulting bit sequence is then encoded in NRZI (no-return to zero inverted), and modulated in GMSK. The CRC principles and the bit stuffing procedure are described in what follows.

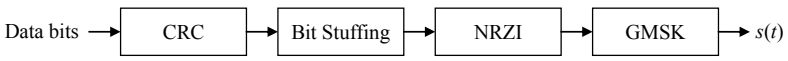


Figure 1. Example of transmitter model used for simulations for each user.

2.1. Cyclic Redundancy Check properties

The CRC is defined as the remainder of the division (modulo 2) of the polynomial formed by the data and a standardized so-called generator polynomial, whose degree equals the length of the CRC plus one. In some cases, some zeros may be inserted before the remainder in order to obtain a fixed-length CRC. At the receiver side, the errors are detected by comparing the CRC computed from the received data with the CRC contained in the data frame. A key CRC property for all algorithms proposed in this article is that the CRC can be computed iteratively, by initializing the CRC to a standard value and by applying the operations to each data bit, as exemplified in Fig. 2. This property allows us to design a specific trellis, which constitutes the basis of the proposed correction methods, as explained in section 3.2.

Moreover, one defines a joint CRC, computed on the bit sequence composed of the information bits and the derived CRC. The definition of this joint CRC is possible since, in the AIS system, the CRC is included juste after the information bits on which it is computed. Given this definition, no

DOI: 10.1002/sat

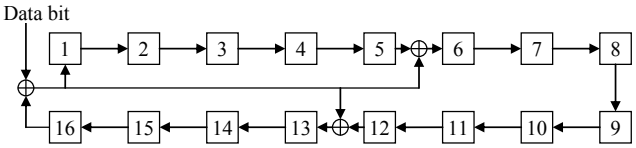


Figure 2. Example of iterative CRC computation with the generator polynomial $G(x) = x^{16} + x^{12} + x^5 + 1$. $\oplus$ represent XOR and are placed according to the generator polynomial. The numbered boxes contain the derived CRC bits.

error is detected at the receiver side when the joint CRC is zero, which can be expressed as

$$\text{CRC}([\text{Data}, \text{CRC}(\text{Data})]) = 0 \tag{1}$$

which is obviously equivalent to compare the CRC computed from the data with the one contained in the data. The expression (1) is also helpful for the proposed detection methods.

2.2. Bit stuffing

In the AIS system, non-informative bits referred to as stuffing bits are potentially added to the bit sequence after the CRC computation, as illustrated in Fig. 3. A first objective is to create additional transitions in the signal by limiting the number of consecutive identical bits, which is useful to re-synchronize the receiver clock. Another objective of the bit stuffing is to avoid specific code words. Note that this particular procedure occurs in various applications (AIS, HDLC data transmission protocol) where the bit stuffing avoids that a data sequence is considered as the end frame flag byte (composed of two bits 0 on each side of six consecutive bits 1). Since the stuffing bits depend on the information sequence, their presence and their location are random, which creates a supplementary issue at the receiver side: indeed, the demodulation algorithm must detect and localize the stuffing bits in order to recover the information sequence. This issue constitutes one of the problems addressed in this study. Since the stuffing bits are always 0 for AIS, this article focuses on the case where only bits 0 are inserted.

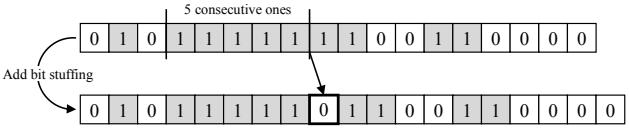


Figure 3. Principle of bit stuffing in AIS: a bit 0 is inserted after each sequence of five consecutive bits 1.

2.3. Gaussian minimum shift keying modulation

The bit sequence obtained after the bit stuffing procedure is encoded using the NRZI coding. The resulting sequence is modulated with GMSK modulation. In the GMSK modulation, the transmitted signal $s(t)$ is a constant-modulus signal defined by

$$s(t) = e^{-j\varphi(t;\mathbf{B})}$$

where the phase $\varphi(t;\mathbf{B})$ contains the information symbols

$$\varphi(t;\mathbf{B}) = 2\pi h \sum_{k=-\infty}^{n} b_k q(t-kT),\ nT \leqslant t \leqslant (n+1)T. \tag{2}$$

In (2), T is the symbol period, $\mathbf{B} = \{b_k\}$ is the bit sequence, h is the modulation index (equal to 0.5 for the AIS system), and $q(t)$ is the waveform defined by

$$q(t) = \int_0^t g(\tau)d\tau. \tag{3}$$

Prepared using satauth.cls
DOI: 10.1002/sat

For GMSK signals, the pulse $g(t)$ is defined by

$$g(t) = Q\left[\frac{2\pi W}{\sqrt{\ln 2}}\left(t - \frac{T}{2}\right)\right] - Q\left[\frac{2\pi W}{\sqrt{\ln 2}}\left(t + \frac{T}{2}\right)\right],$$

where W is the 3 dB cut-off bandwidth, and $Q(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt$ is the complementary Gaussian cumulative distribution function. The pulse $g(t)$ is generally truncated in the interval $[-LT; LT]$ where L is typically equal to 3 in AIS.

2.4. Received signal model

Denote as N_u the number of users, and $s_j(t)$ the signal generated by the jth user at the output of the encoding-plus-modulation block, as depicted in Fig. 1. One considers in this paper frequency-flat channels. Therefore, the multi-user received signal can be expressed as

$$r(t) = \sum_{j=1}^{N_u} a_j s_j(t - \tau_j) e^{-i(2\pi f_j t + \phi_j)} + n(t) \tag{4}$$

where τ_j is the delay, f_j is the Doppler shift, ϕ_j is the phase shift, and a_j is the (real positive value) channel gain corresponding to user #j. Moreover, $n(t)$ is a white additive Gaussian noise, independent of the transmitted signals.

We assume in the first part of this paper that for a given user of interest (denoted by the subscript u), parameters τ_u, f_u, a_u and ϕ_u are known at the receiver side. The case of an unknown possibly varying phase shift ϕ_u will be addressed later in Section 4. The other parameters could for instance be estimated by correlation-based techniques using the headers as pilot symbols. Of course, since the length of the known header (24 bits for the training sequence and 8 bits for the start flag) is quite limited, this estimation method requires the power of the received AIS signal to be sufficient. For the estimation of τ_u, a solution was investigated in [2], where the receiver is applied to all the samples of the AIS message. However, this technique requires to have a receiver with small computational complexity. An alternative is to use several reception antennas and beamforming techniques, at the price of a more complex hardware receiver [16]. However, these estimation issues are beyond the scope of this paper which mainly focuses on the error correction strategy. Note that, in the multi-user scenario, the delays, Doppler shifts, and phase shifts of the users different from the user of interest, need not to be known. After compensating for parameters, the received signal $r(t)$ can be re-written

$$r_u(t) = s_u(t) + \sum_{j \neq u} A_j s_j(t - T_j) e^{-i(2\pi F_j t + \Phi_j)} + n_u(t), \tag{5}$$

where $A_j = \frac{a_j}{a_u}$, $T_j = \tau_j - \tau_u$, $F_j = f_j - f_u$ and $\Phi_j = \phi_j - \phi_u$. The objective is to recover the information data contained in the signal of interest $s_u(t)$ from the received signal $r_u(t)$. To that end, we propose CRC-based detection methods which jointly detect and remove the stuffing bits, and detects the information bits.

3. THE MONO-USER SCENARIO

The mono-user scenario assumes that there is only one transmitted signal, i.e., the multi-user interference term (the second term at the right-hand side of (5)) vanishes. Therefore, for sake of clarity, the subscript u in (5) can be omitted.

3.1. General principle

The received analog signal (4) is first passed through a matched filter (MF) and sampled at the output of the MF with one sample per symbol. Denote r_k as the sample obtained for the kth symbol period and K as the number of received symbols. The standard Viterbi algorithm determines the

Prepared using satauth.cls
DOI: 10.1002/sat

symbol sequence $m_1, \ldots, m_K$ which minimizes the square Euclidean distance defined by

$$\sum_{k=1}^{K} |r_k - m_k|^2 \tag{6}$$

where m_k is the kth estimated symbol obtained after the MF. Given the particular structure of the transmitted signal, the detection method proposed here consists of minimizing the distance (6) subjected to the two following constraints:

(C1) the joint CRC must satisfy the condition (1).

(C2) the number of consecutive bits 1 is upper bounded by a maximum value denoted as $\overline{P}$, specified by the application standard *; this constraint allows bit stuffing to be taken into account.

In order to manage this constrained optimization problem, the proposed detection algorithm is based on a so-called extended trellis, whose states (called extended states) are composed of a CRC state and a TC state. In this extended trellis, all paths ending with a final state give a message whose joint CRC is zero, (hence, paths corresponding to a non zero CRC do not appear in the trellis). Therefore, one ensures that constrained (C1) is satisfied. On the other hand, constraint (C2) is managed by defining specific transitions in the extended trellis. The design of the extended trellis with its transitions is detailed in the next sections. In what follows, the term CRC will always refer to the joint CRC, defined in section 2.1.

3.2. Extended trellis

As mentioned in section 2.1, the CRC can be computed iteratively. Hence, it can be initialized to a particular value, depending on the considered CRC standard, and updated for each received bit. Therefore, a CRC state corresponds to a particular intermediate CRC value. Two consecutive CRC states are connected if the second state can be constructed from the first state by including one bit 0 or one bit 1, as shown in (7).

The proposed algorithm associates a CRC state with a TC state (a state of the trellis code). This association constitutes a so-called extended state. The extended trellis is the trellis composed of theses extended states. For instance, if a TC state α is followed by a TC state β (resp. TC state γ) when the bit 0 (resp. the bit 1) is transmitted, and a CRC state A is followed by the CRC state B (resp. C) when the bit 0 (resp. the bit 1) is transmitted, then the extended state $(A;\alpha)$ is followed in the extended trellis by the extended state $(B;\beta)$ in the transmission of the bit 0 (resp. the extended state $(C;\gamma)$ in the transmission of the bit 1). This operation is illustrated in (7), where the integer k refers to as the number of the received symbol.

$$\begin{array}{ccccc} \texttt{CRC state} & & \texttt{TC state} & & \texttt{Extended state} \\ \overset{k}{A} \xrightarrow{0} \overset{k+1}{B} & \& & \overset{k}{\alpha} \xrightarrow{0} \overset{k+1}{\beta} & \Rightarrow & \overset{k}{(A;\alpha)} \xrightarrow{0} \overset{k+1}{(B;\beta)} \\ A \xrightarrow{1} C & & \alpha \xrightarrow{1} \gamma & & (A;\alpha) \xrightarrow{1} (C;\gamma) \end{array} \tag{7}$$

One proposes to apply the Viterbi algorithm to this extended trellis. To that end, one defines, for the received symbol k, the variable $\Gamma[k,(A;\alpha)]$ as the squared Euclidean distance between the received signal and the sequence of k symbols yielding the extended state $(A;\alpha)$ at time k, i.e.,

$$\Gamma[k,(A;\alpha)] = \sum_{i=1}^{k} \left| r_i - m_i^{k,(A;\alpha)} \right|^2 \tag{8}$$

where $\left[m_1^{k,(A;\alpha)}, \ldots, m_k^{k,(A;\alpha)}\right]$ denotes the symbol sequence yielding $(A;\alpha)$ at time k. Moreover, one denotes by $\Gamma_{\text{trans}}[k,(A;\alpha),b]$ the transition variable defined as the sum of $\Gamma[k,(A;\alpha)]$ and

*Recall that one considers here that the stuffing bits are bits 0.

Prepared using satauth.cls
DOI: 10.1002/sat

the squared distance between the received symbol at time $k+1$ and the symbol coming from the extended state $(A;\alpha)$ containing the bit b, denoted by $m_k^{k+1,(A;\alpha),b}$, i.e.,

$$\Gamma_{\text{trans}}[k,(A;\alpha),b] = \Gamma[k,(A;\alpha)] + \Delta[k,(A;\alpha),b], \tag{9}$$

with

$$\Delta[k,(A;\alpha),b] = \left| r_k - m_k^{k+1,(A;\alpha),b} \right|^2. \tag{10}$$

The transition variables $\Gamma_{\text{trans}}[k,(A;\alpha),b]$ are used to choose the best transition yielding a given state, among the different possible transitions leading to this state. More precisely, the selected transition will minimize $\Gamma_{\text{trans}}[k,(A;\alpha),b]$, as detailed in section 3.5 and in appendix A.
After introducing the principles of the extended trellis, we focus on the detection of stuffing bits, as presented below.

3.3. Bit stuffing

The extended trellis presented above allows the CRC to be used as an error correction tool. However, it cannot account for the possible presence of stuffing bits. Thus, we propose to complete the extended trellis by introducing specific transitions, which are only used when a stuffing bit is received. The principle of these specific transitions consists of generating a change in the TC state when a stuffing bit has been detected, while keeping unchanged the CRC state. Indeed, since the CRC is computed at the transmitter side before the bit stuffing procedure, the stuffing bits should not modify the CRC state. The different possible transitions in the extended trellis are illustrated in (11): at a given time k, where one considers the extended state $(A;\alpha)$, one can receive either a non-stuffing bit 0 or 1, or a stuffing bit (***SB***) 0 (recall that stuffing bits equal 0).

$$\begin{array}{ccccc}
\texttt{CRC state} & & \texttt{TC state} & & \texttt{Extended state} \\
{\scriptstyle k} \quad {\scriptstyle k+1} & & {\scriptstyle k} \quad {\scriptstyle k+1} & & {\scriptstyle k} \quad {\scriptstyle k+1} \\
A \xrightarrow{0} B & & \alpha \xrightarrow{0} \beta & & (A;\alpha) \xrightarrow{0} (B;\beta) \\
A \xrightarrow{1} C & \& & \alpha \xrightarrow{1} \gamma & \Rightarrow & (A;\alpha) \xrightarrow{1} (C;\gamma) \\
A \xrightarrow{SB} A & & \alpha \xrightarrow{SB} \beta & & (A;\alpha) \xrightarrow{SB} (A;\beta)
\end{array} \tag{11}$$

Of course, the receiver has to detect whether a received bit is a stuffing bit or not. The detection of stuffing bits requires to define, for each state $(A;\alpha)$, a state variable $P[k,(A;\alpha)]$, which represents the number of consecutive bits 1 received before reaching the state $(A;\alpha)$ at time k. To respect constraint (C2), the received bit will be declared as a stuffing bit if $P[k,(A;\alpha)]$ reaches a given maximum value $\overline{P}$ specified by the application standard ($\overline{P}=5$ for AIS, corresponding to the zero-bit insertion illustrated in Fig. 3). In that case, one performs the transition $(A;\alpha) \xrightarrow{SB} (A;\beta)$. After this transition, $P[k+1,(A;\beta)]$ is reset to 0, since the received bit has been detected as a stuffing bit (equal to 0). This procedure is exemplified in (12), where $\not\longrightarrow$ is an impossible transition corresponding to the fact that an information bit cannot be a stuffing bit, and vice-versa. These impossible transitions are considered in the algorithm by simply assigning them an infinite distance.

$$\begin{array}{cc}
\texttt{Information bit} & \texttt{Stuffing bit} \\
{\scriptstyle k} \quad {\scriptstyle k+1} & {\scriptstyle k} \quad {\scriptstyle k+1} \\
(A;\alpha) \xrightarrow[P=3]{0} (B;\beta) \atop {\scriptstyle P=0} & (A;\alpha) \xrightarrow[P=5]{0} (B;\beta) \\
(A;\alpha) \xrightarrow[P=3]{1} (C;\gamma) \atop {\scriptstyle P=4} & (A;\alpha) \xrightarrow[P=5]{1} (C;\gamma) \\
(A;\alpha) \xrightarrow[P=3]{SB} (A;\beta) & (A;\alpha) \xrightarrow[P=5]{SB} (A;\beta) \atop {\scriptstyle P=0}
\end{array} \tag{12}$$

In addition to the variable $P[k+1,(A;\beta)]$, one also defines for each state $(A;\alpha)$ the variable $S[k,(A;\alpha)]$ as the number of stuffing bits received before reaching the state. This variable allows one to know the number of informative bits in the received frame. Similarly to the definitions of $\Gamma_{\text{trans}}[k,(A;\alpha),b]$ and $\Gamma[k,(A;\alpha)]$, one defines the transition variables $P_{\text{trans}}[k,(A;\alpha),b]$ and $S_{\text{trans}}[k,(A;\alpha),b]$ representing the evolutions of $P[k,(A;\alpha)]$ and $S[k,(A;\alpha)]$ when the bit b has been received (note that b can take the values 0, 1 or ***SB***).

DOI: 10.1002/sat

3.4. Final state decision

Once the extended trellis has been defined, the optimal path in this trellis has to be determined. To this purpose, the final state of the trellis has to be defined. According to (1) the final CRC state must be 0. However, the final TC state (denoted by $\boldsymbol{\sigma}_{TC}^{f}$) and the number of actual received symbols K in the message are unknown because of the possible presence of stuffing bits. In order to estimate these parameters, we propose to find the estimates $\widehat{\boldsymbol{\sigma}}_{TC}^{f}$ and $\widehat{K}$ minimizing the global distance $\Gamma[K,(0;\boldsymbol{\sigma}_{TC}^{f})]$. This optimization problem has to be constrained in order to ensure that the number of information bits and stuffing bits satisfy the system specifications. Denote as $N_{\min}$ and $N_{\max}$ the minimum and maximum numbers of information bits including the CRC, and $S_{\min}$, $S_{\max}$ the minimum and maximum numbers of stuffing bits (note that $N_{\min}=N_{\max}=184$, $S_{\min}=0$ and $S_{\max}=4$ for AIS). Since $S[K,(0;\boldsymbol{\sigma}_{TC}^{f})]$ is the total number of received stuffing bits, one must have: $S_{\min}\leq S[K,(0;\boldsymbol{\sigma}_{TC}^{f})]\leq S_{\max}$. Moreover, since K belongs to the set $\{N_{\min}+S_{\min},\ldots,N_{\max}+S_{\max}\}$, one has

$$N_{\min}+S[K,(0;\boldsymbol{\sigma}_{TC}^{f})]\leq K\leq S[K,(0;\boldsymbol{\sigma}_{TC}^{f})]+N_{\max}. \tag{13}$$

Finally, the proposed constrained minimization problem is defined as

$$\left(\widehat{K},\widehat{\boldsymbol{\sigma}}_{TC}^{f}\right)=\underset{K,\boldsymbol{\sigma}_{TC}^{f}}{\arg\min}\,\Gamma[K,(0;\boldsymbol{\sigma}_{TC}^{f})] \tag{14}$$

subject to the constraints

$$\begin{array}{c} S_{\min}\leq S[K,(0;\boldsymbol{\sigma}_{TC}^{f})]\leq S_{\max} \\ N_{\min}\leq K-S[K,(0;\boldsymbol{\sigma}_{TC}^{f})]\leq N_{\max}. \end{array} \tag{15}$$

3.5. Detection algorithm

This section summarizes the different steps of the proposed algorithm (see appendix A for more details).

- **Initialization** (see A-1): Denote as $(A_0;\alpha_0)$ the initial state of the trellis. A_0 is initialized according to the standard of the considered application. For instance, since AIS uses a CRC-16, A_0 is initialized to $2^{16}-1$. When α_0 is unknown, all values of the distances $\Gamma[0,(A_0;\alpha_0)]$ are set to 0. When $\alpha_0=\alpha_0^*$ is known, one simply sets $\Gamma[0,(A_0;\alpha_0^*)]=0$.
- **Computation of transition variables** (see A-2): When a P state variable equals $\overline{P}$, the next transition can only be an ***SB*** transition. In order to avoid impossible transitions, $\Gamma_{\text{trans}}[k,(A;\alpha),b]$ is set to ∞ for $b=0$ and $b=1$ where k is the current symbol number and $(A;\alpha)$ is the considered state. Moreover, $\Gamma_{\text{trans}}[k,(A;\alpha),\textbf{\textit{SB}}]$ is set to $\Gamma[k,(A;\alpha)]$ plus the distance between the current received symbol and the symbol carrying an ***SB***. Conversely, when the P state variable does not equal $\overline{P}$, $\Gamma_{\text{trans}}[k,(A;\alpha),b]$ is defined as in the classical Viterbi algorithm for $b\in\{0,1\}$ and is set to ∞ for $b=\textbf{\textit{SB}}$. Moreover, $P_{\text{trans}}[k,(A;\alpha),b]$ is set to 0 for $b\in\{0,\textbf{\textit{SB}}\}$, and is set to $P[k,(A;\alpha)]+1$ for $b=1$. Finally, $S_{\text{trans}}[k,(A;\alpha),b]$ is set to $S[k,(A;\alpha)]$ for $b\in\{0,1\}$, and to $S[k,(A;\alpha)]+1$ for $b=\textbf{\textit{SB}}$.
- **Computation of state variables** (see A-3): The selected transition leading to a given state is the one with minimal Γ_{trans} among those who can precede this state. Let $R[k,(A;\alpha)]$ denote as the last received bit leading to the state $(A;\alpha)$. The state variables Γ, P and S are set to the values of the variables Γ_{trans}, P_{trans} and S_{trans} of the selected transition whereas the state variable R is set to the bit carried by the selected transition.
- **Path reading** (see A-4): The resulting sequence is read by following the path through the trellis starting from the final state. The previous states are selected by reading the last received bit in the state variable R of each state.

3.6. Transmission error detection

By construction, the messages decoded by the proposed algorithm have systematically a correct CRC. Thus the CRC can no longer be used for the detection of transmission errors and other

Prepared using satauth.cls
DOI: 10.1002/sat

detection methods need to be investigated for AIS signals. Possible solutions consist of checking data consistency and the following constraints related to the AIS system

- The identifier of the ship in the message must be an existing identifier.
- The spare field of the message must be 0.
- The speed of the ship must be in the correct range.
- The estimated position must be consistent with the position of the receiver in the sense that the transmitter has to be located at a reachable distance from the receiver.

3.7. Complexity

The number of states associated with the proposed extended trellis equals the product between the number of states of the TC trellis (i.e., 4 for the AIS system) and the number of states of the CRC trellis (i.e., 2^{16}). The total number of states per symbol is therefore $2^{18} = 262\,144$. The extended trellis has 3 transitions departing from each extended state yielding $786\,432$ transitions per symbol. The extended trellis must be constructed for the 188 symbols of the AIS message. Thus, the total numbers of extended states and transitions are $49\,283\,072$ and $147\,849\,216$, respectively. Even if these numbers are quite large, the decoding of an AIS message requires about 1 second per message for our simulator programmed in C with a 2.6-GHz processor. It is interesting to note here that the average computation time could be reduced by applying the proposed error correction method only when the CRC of the AIS message resulting from the conventional receiver differs from 0.

4. PHASE TRACKING

The algorithm presented in section 3 has assumed that there was no phase shift $\phi_u(t)$ for the user of interest, or, equivalently, that $\phi_u(t)$ was known and could be compensated. This section considers a scenario where this phase shift is unknown, and can possibly vary from one symbol to another. This approach can also be applied when the modulation index h is significantly different from its nominal value $h = 0.5$ defined in the AIS standard. Indeed, the actual modulation index can present important variations (typically a variation of $\pm 15\%$ can be observed) with respect to its standard value. In that case, a non data aided (NDA) estimation of the modulation index at the receiver seems quite unrealistic on a very short burst with low E_b/N_0. A rough data aided (DA) estimation is possible using the known preamble of AIS signals (32 bits), but it provides inaccurate estimation. Consequently, it appears pragmatic for the receiver design to model the effect of an inaccurate modulation index as a simple random phase fluctuation. In this case, equation (4) can be rewritten in the mono-user case as [†]

$$r(t) = e^{j\phi(t)} s(t) + n(t). \tag{16}$$

The proposed detection algorithm consists of including the unknown phase shift $\phi(t)$ in the distances defined in eq.'s (8)–(10), which are minimized jointly with respect to the phase $\phi(t)$ and the symbols yielding to the extended state. It is assumed that the phase shift is constant during a period symbol. Hence, only one phase value has to be estimated during this window. More precisely, we propose to minimize the cost function

$$\sum_{k=1}^{K} \left| e^{-j\phi_k} r_k - m_k \right|^2 \tag{17}$$

where ϕ_k denotes the phase shift for the kth period symbol. In order to adapt the detection algorithm to the phase tracking problem, one redefines the squared distance (8) as follows

$$\Gamma[k, (A;\alpha)] = \sum_{i=1}^{k} \left| e^{-j\phi_i^{k,(A;\alpha)}} r_i - m_i^{k,(A;\alpha)} \right|^2 \tag{18}$$

[†]Similarly to section 3, the subscript u is omitted here for notation simplicity.

DOI: 10.1002/sat

where $\left(\phi_1^{k,(A;\alpha)},\ldots,\phi_k^{k,(A;\alpha)}\right)$ and $\left(m_1^{k,(A;\alpha)},\ldots,m_k^{k,(A;\alpha)}\right)$ denote the sequences of estimated phase shifts and symbols in the path reaching the state $(A;\alpha)$ at the kth symbol period. Moreover, one must also redefine the transition variable $\Gamma_{\text{trans}}[k,(A;\alpha),b]$ given in (9). To that end, the increment $\Delta[k,(A;\alpha),b]$ defined in (10) has to be modified in order to take into account the phase tracking, i.e., one chooses the minimal increment with respect to the unknown phase shift. More precisely, we define the function

$$\Delta[k,(A;\alpha),b,\phi]=\left|e^{-j\phi}r_k-m_k^{k+1,(A;\alpha),b}\right|^2 \tag{19}$$

which differs from (10) through the introduction of the unknown variable ϕ. The increment $\Delta[k,(A;\alpha),b]$ which transforms $\Gamma[k,(A;\alpha),b]$ into $\Gamma_{\text{trans}}[k,(A;\alpha),b]$ in (9) has to be replaced by the minimum increment $\Delta[k,(A;\alpha),b,\phi]$ with respect to ϕ, which gives

$$\Delta_{\min}[k,(A;\alpha),b]=\min_{\phi\in\mathcal{I}_k^{(A;\alpha)}}\Delta[k,(A;\alpha),b,\phi] \tag{20}$$

and

$$\Gamma_{\text{trans}}[k,(A;\alpha),b]=\Gamma[k,(A;\alpha)]+\Delta_{\min}[k,(A;\alpha),b]. \tag{21}$$

In (20), the minimization is achieved on the set $\mathcal{I}_k^{(A;\alpha)}$ defined by

$$\mathcal{I}_k^{(A;\alpha)}=\left[\phi_k^{k,(A;\alpha)}-\Delta\phi;\phi_k^{k,(A;\alpha)}+\Delta\phi\right] \tag{22}$$

for some positive real-value $\Delta\phi$. This means that the optimal ϕ at time $k+1$ coming from the state $(A;\alpha)$ is searched in a window of length $2\Delta\phi$ centered around the phase $\phi_k^{k,(A;\alpha)}$, which represents the current estimated phase shift in the path reaching this state at time k. The minimization problem (20) leads to a simple analytic solution, which is specified in appendix B.

One denotes by $\phi_{\text{trans}}^{k,(A;\alpha),b}$ the value of the phase which minimizes (20). Similarly to $\Gamma_{\text{trans}}[k,(A;\alpha),b]$, the transition phase $\phi_{\text{trans}}^{k,(A;\alpha),b}$ is used when the algorithm has to choose a transition toward the state $(B;\beta)$. Indeed, the selected phase $\phi_{\text{trans}}^{k,(A;\alpha),b}$, among the different states $(A;\alpha)$ which lead to $(B;\beta)$ at time $k+1$, is the one corresponding to the selected $\Gamma_{\text{trans}}[k,(A;\alpha),b]$. This selected value of $\phi_{\text{trans}}^{k,(A;\alpha),b}$ becomes then the new phase $\phi_{k+1}^{k+1,(B;\beta)}$ at time $k+1$ in the state $(B;\beta)$.

Note that the analytic solution of problem (20) given in appendix B is quite simple. However, the algorithm can be speed up by discretizing the phase estimation problem. This means that one estimates the phase in the finite set $\{0,\delta_\phi,2\delta_\phi,\ldots,2\pi-\delta_\phi\}$, instead of estimating it in the continuous set $[0;2\pi]$. The quantizing step is then defined by $\delta_\phi=2\pi/N_\phi$, where N_ϕ is the number of possible phase values, which tunes the accuracy of the estimation. The research set $\mathcal{I}_k^{(A;\alpha)}$ in (22) has then to be replaced by the finite set $\widetilde{\mathcal{I}}_k^{(A;\alpha)}$ defined by

$$\widetilde{\mathcal{I}}_k^{(A;\alpha)}=\left\{\phi_k^{k,(A;\alpha)}-n_\phi\delta_\phi,\ldots,\phi_k^{k,(A;\alpha)}+n_\phi\delta_\phi\right\} \tag{23}$$

where n_ϕ is the integer part of $\Delta\phi/\delta_\phi$. Note that $\phi_k^{k,(A;\alpha)}$ appearing in (23) is obtained at the previous iteration in a similar way and is itself a multiple of δ_ϕ. Similarly, $\Delta_{\min}[k,(A;\alpha),b]$ is defined by

$$\Delta_{\min}[k,(A;\alpha),b]=\min_{\phi\in\widetilde{\mathcal{I}}_k^{(A;\alpha)}}\Delta[k,(A;\alpha),b,\phi] \tag{24}$$

and $\phi_{\text{trans}}^{k,(A;\alpha),b}$ denotes the value of the phase which minimizes (24). This discrete minimization simply reduces to find the minimum value among the $2n_\phi+1$ values of $\Delta[k,(A;\alpha),b,\phi]$, which significantly speeds up the computation of $\Delta_{\min}[k,(A;\alpha),b]$ (n_ϕ is generally small, for instance equal to 10 in the simulations presented in section 6). Moreover, while the number of states is important, the minimization problem (24) does not need to be computed for each state at a given

Prepared using satauth.cls
DOI: 10.1002/sat

time k. Indeed, there is only a small number, say N_{symb}, of possible symbols $m_k^{k+1,(A;\alpha),b}$: this means that there are $N_{\text{symb}}N_\phi$ possible values of $\Delta[k,(A;\alpha),b,\phi]$ for all states b and ϕ. Thus, for a given time instant k, these $N_{\text{symb}}N_\phi$ values, their minima in the N_ϕ possible sets $\widetilde{\mathcal{I}}_k^{(A;\alpha)}$ and the arguments of these minimas, can be computed once and for all and saved into tables. Hence, for a given state $(A;\alpha)$ and a given b, $\Delta_{\min}[k,(A;\alpha),b]$ and $\phi_{\text{trans}}^{k,(A;\alpha),b}$ are simply obtained by selecting appropriate values in these tables.

As for the problem addressed in section 3, the transition variables of the form $\Gamma_{\text{trans}}[k,(A;\alpha),b]$ are used to choose the optimal transition which leads to a given state, i.e., the transition minimizing $\Gamma_{\text{trans}}[k,(A;\alpha),b]$.

Note that the bit stuffing detection method is not modified by this phase estimation. Hence, the demodulation algorithm is identical to the one presented in section 3.5, where the transition variable $\Gamma_{\text{trans}}[k,(A;\alpha),b]$ is now defined by (21).

5. THE MULTI-USER SCENARIO

This section studies the case where the received signal is a multi-user signal, from which the data transmitted by a single user of interest have to be estimated. In a first part, the adaptation of the mono-user detection algorithm to this new context is studied, still assuming that there is no phase shift. This generalization is achieved by performing a reduction of the multi-user interference. Next, one studies a scenario where there is a possible varying phase shift.

Consider the multi-user signal model defined in (5). The method presented for the mono-user scenario might be directly generalized to the multi-user problem. Indeed, one might define a multi-user extended trellis, whose extended states are composed of the CRC states and the TC states of all users. However, this strategy, which is theoretically optimal, would face two major difficulties: first, it would require the knowledge of the parameters (delays, gains, Doppler and phase shifts) of all users, even if one is interested to recover the data of one single user. On the other hand, the size of this extended trellis would increase exponentially with respect to the number of users, which would make the detection algorithm untractable.

Therefore, we propose a sub-optimal approach, which first applies a reduction of the multi-user interference, and then applies a modified version of the mono-user algorithm to the signal resulting from this interference reduction. One first define a method adapted to the case where only one single interferer is present. This method is next adapted to the multi-interferer case by developing an empirical approach inspired by the one presented in [17]. The approach presented here assumes first that the parameters (delay, gain, Doppler and phase shifts) of the user of interest are known by the receiver, along with the gains of the other users, while the delays, Doppler and phase shifts of the other users are unknown. The case of an unknown phase shift for the user of interest is finally investigated.

5.1. Single interferer

In order to simplify the presentation, we first consider a single interferer. The received signal (5) can be expressed as

$$r_u(t) = s_u(t) + A_I s_I(t-T_I)e^{-i(2\pi F_I t+\Phi_I)} + n_u(t) \tag{25}$$

where the subscript I stands for the interferer. Neglecting the additive noise, and using the fact that the GMSK modulation is a constant modulus modulation, we obtain

$$|r_u(t) - s_u(t)| \approx |A_I s_I(t-T_I)e^{-i(2\pi F_I t+\Phi_I)}| = A_I, \forall t. \tag{26}$$

Therefore, one proposes a least-squares approach, which consists of minimizing the energy of the difference $|r_u(t) - s_u(t)| - A_I$. More precisely, a new cost function replacing (6) is defined as follows

$$\sum_{k=1}^{K} \left| |r_{u,k} - m_{u,k}| - A_I \right|^2 \tag{27}$$

Prepared using satauth.cls
DOI: 10.1002/sat

where $r_{u,k}$ and $m_{u,k}$ denote the sample obtained from $r_u(t)$ in the kth symbol period, and the sample obtained from the kth estimated symbol of the user of interest. With this new definition of the cost function, the detection algorithm presented in section 3 can be used after transforming the transition variable (8) into

$$\Gamma[k,(A;\alpha)] = \sum_{i=1}^{k} \left| |r_i - m_i^{k,(A;\alpha)}| - A_I \right|^2 \tag{28}$$

and

$$\Delta[k,(A;\alpha),b] = \left| |r_k - m_k^{k+1,(A;\alpha),b}| - A_I \right|^2 . \tag{29}$$

5.2. Multiple interferers

When several interferers are present in the received signal, the property (26) does not hold anymore. However, this property allows an empirical approach to be defined, similar to the one proposed in [17]. More precisely, we propose to remove in the cost function used in the Viterbi algorithm the average multi-user interference power of interfering signals, denoted as $\bar{e}_u^2$, from the difference between symbols and the received signal. In this paper, one suggests to define a cost function slightly different from the one proposed in [17], based on the least-squares criterion given in (27). More precisely, this function is given by

$$\sum_{k=1}^{K} \left| |r_{u,k} - m_{u,k}| - \sqrt{\bar{e}_u^2} \right|^2 \tag{30}$$

where $\bar{e}_u^2$ is the average power of interfering signals defined by

$$\bar{e}_u^2 = \sum_{j \neq u} A_j^2 = \frac{1}{a_u^2} \sum_{j \neq u} a_j^2 . \tag{31}$$

It can be observed that the cost function (30) actually reduces to (27) for a single interferer, and to (6) in the mono-user scenario defined by zero gains A_j. Note that the consistency of the cost function for the different scenarios does not hold for the cost function proposed in [17].

With these definitions, the detection algorithm for the user of interest can be obtained from the mono-user detection algorithm developed in section 3, by appropriately modifying the definition of the transition variable $\Gamma[k,(A;\alpha)]$ in view of the cost function (30), which leads to

$$\Gamma[k,(A;\alpha)] = \sum_{i=1}^{k} \left| |r_i - m_i^{k,(A;\alpha)}| - \sqrt{\bar{e}_u^2} \right|^2 \tag{32}$$

and

$$\Delta[k,(A;\alpha),b] = \left| |r_k - m_k^{k+1,(A;\alpha),b}| - \sqrt{\bar{e}_u^2} \right|^2 . \tag{33}$$

The different steps of the multi-user detection algorithm are then identical to those of the mono-user scenario, presented in section 3.5. Note that, concerning complexity considerations, the computational cost of the mono-user and multi-user algorithms are similar: the slight increase in the multi-user algorithm complexity is only due to the introduction of the average power $\bar{e}_u^2$ (which is computed at the initialization of the algorithm) into the squared distances (32) and (33). In particular, this increase does not depend on the number of users, which constitutes a key advantage of this approach.

5.3. Phase tracking

The detection algorithm proposed above is designed for a known phase shift for the user of interest. If this phase shift is unknown, the detection can be simply modified by using the procedure described

Prepared using satauth.cls
DOI: 10.1002/sat

in section 4, i.e., by incorporating a phase term in the cost function (30), leading to

$$\sum_{i=1}^{k} \left| |e^{-j\phi_k} r_i(l) - m_i^{k,(A;\alpha)}| - \sqrt{\bar{e}_u^2} \right|^2 . \tag{34}$$

This procedure requires to define a minimum increment $\Delta_{\min}[k,(A;\alpha),b]$ and a transition variable $\Gamma_{\text{trans}}[k,(A;\alpha),b]$ similar to (20)-(21), where the function $\Delta[k,(A;\alpha),b,\phi]$ is defined by

$$\Delta[k,(A;\alpha),b,\phi] = \left| |e^{-j\phi} r_k - \boldsymbol{m}_k^{k+1,(A;\alpha),b}| - \sqrt{\bar{e}_u^2} \right|^2 . \tag{35}$$

Simple computations show that the minimum of $\Delta[k,(A;\alpha),b,\phi]$ with respect to ϕ cannot be obtained in closed form as for the mono-user case. Thus this minimum $\Delta_{\min}[k,(A;\alpha),b]$ can only be obtained by using a numerical minimization algorithm. For complexity reasons, it is impossible to perform a numerical minimization for each state of the extended trellis. Therefore, one proposes to use the discrete minimization procedure detailed in section 4. Hence, the computationally expensive exact minimization of (35) simply amounts to selecting the minimizer in a table determined once and for all at the beginning of the algorithm. The computational cost of the resulting detection algorithm in the multi-user case with phase tracking is then slightly increased when compared to the mono-user case with perfect phase recovery.

6. SIMULATIONS

This section presents some simulation results associated with the different scenarios considered in this paper (mono/multi-user, with/without phase tracking). The different detection algorithms are evaluated in the context of the AIS system, whose transmitter characteristics are recalled for consistency. Each user sends fixed length data messages composed of 168 bits concatenated with a 16-bit CRC. The stuffing bits are then inserted according to the AIS recommendation, i.e., a bit 0 is inserted after each sequence of five consecutive bits 1. The resulting sequence is next encoded with NRZI, and then modulated using the GMSK scheme with parameters $WT = 0.4$ and $LT = 3$ (note that these parameters are known by the receiver). In this system model, NRZI coding and GMSK modulation constitute the TC defined before. The generator polynomial for CRC computation is $G(x) = x^{16} + x^{12} + x^5 + 1$ (specified by the AIS recommendation).

6.1. Mono-user scenario with known phase shift

A mono-user transmission is first considered with an additive white Gaussian noise (AWGN) channel with known phase shift. The algorithm detailed in Section 3.5 and Appendix A has been evaluated for the AIS system. Note that the proposed method cannot be compared with the methods [4]–[8] mentioned in the introduction since they do not take into account the presence of bit stuffing. Therefore, our receiver is compared to a conventional coherent GMSK demodulator based on the Viterbi algorithm, for which the bit stuffing mechanism is simply managed as follows: any bit following a sequence of five bits 1 is deleted to remove the stuffing bit.

Fig. 4 shows the BER curves for these two methods as a function of the signal to noise ratio E_S/N_0. The proposed receiver clearly outperforms the conventional GMSK receiver. An important performance criterion in AIS is also the PER. Fig. 5 presents the corresponding PER curves versus E_S/N_0. One can notice in this figure that the improvement provided by the proposed method is even more significant, since a gain of more than 3.5 dB can be observed for a target PER of 0.1. Note that this gain increases when the target PER decreases.

6.2. Mono-user scenario with phase tracking

Figure 6 shows some simulation results obtained with the algorithm presented in section 4, with the AIS system characteristics described previously. The performance of the algorithm presented

DOI: 10.1002/sat

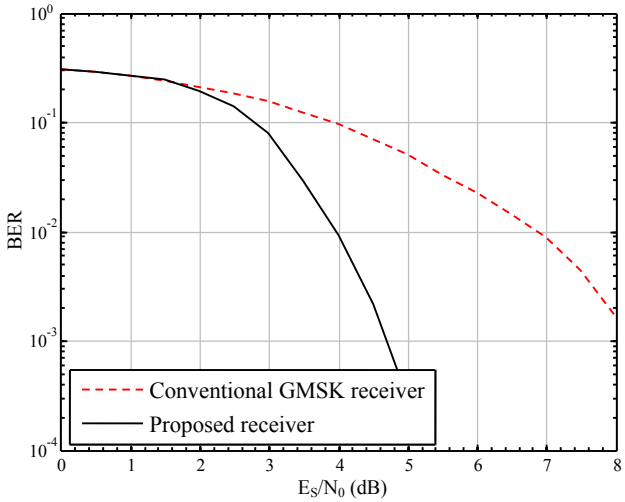


Figure 4. Proposed receiver compared with the conventional GMSK receiver in Bit Error Rate.

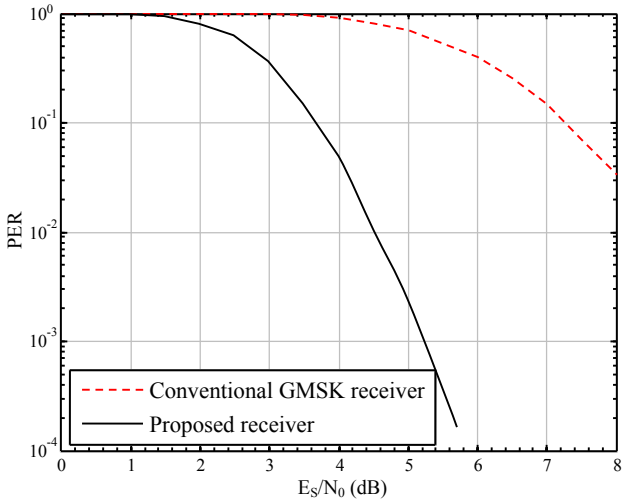


Figure 5. Proposed receiver compared with the conventional GMSK receiver in Packet Error Rate.

in section 3 for known modulation index (denoted h) and phase shift provide a reference to which suboptimal detectors can be compared. The performance of the NDA algorithm is also reported for comparison. In order to simulate an incorrect modulation index in the transmitter, the simulations have been conducted with an actual modulation index $h = 0.45$, whereas the AIS recommendation specifies $h = 0.5$. The proposed algorithm considered the following two cases:

1. h is estimated using the AIS preamble and the parameter $\Delta\phi$ defined in (22) – (23) is set to 4° which covers all possible values of phase shifts;
2. h is not estimated, and the detection algorithm uses the nominal value $h = 0.5$ given by the AIS recommendation. $\Delta\phi$ is then set to 10° (since h is not estimated, the values of phase shifts can be larger than before).

One can note that, with and without estimation of h, the proposed receiver (with unknown h) outperforms the NDA algorithm, with gains equal to 2.5 dB and 1 dB, respectively. One can also observe a performance loss close to 0.5 dB and 2 dB when compared to the case where the modulation index is known. To conclude, by using the proposed receiver, the detection performance

DOI: 10.1002/sat

is not severely degraded when the modulation index is estimated using the AIS preamble and the phase is tracked using an appropriate least square criterion.

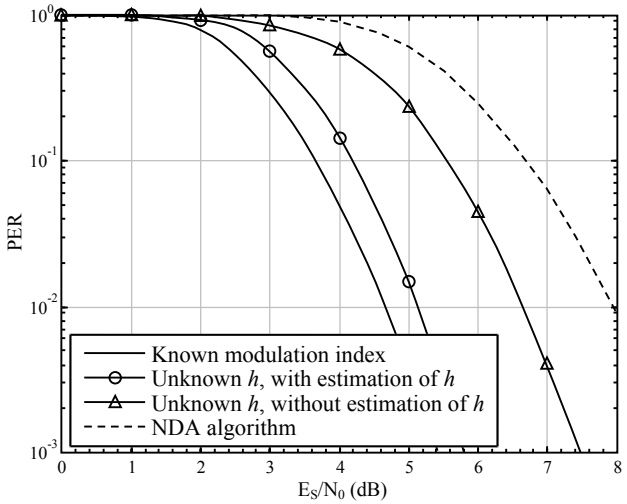


Figure 6. Proposed receiver compared with the algorithm presented in section 3 when the modulation index is known and the NDA algorithm in Packet Error Rate.

6.3. Multi-user scenario without phase shift

For a multi-user transmission without phase-shift, the receivers proposed in sections 5.1 and 5.2 are compared with the method presented in [2], which uses a non-coherent GMSK demodulator and an error correction mechanism based on the CRC presence. Fig. 7 shows the performance of the proposed detector in terms of packet error rates (PER) with 4 interfering signals. Since the error correction technique proposed in [2] is not adapted to bit stuffing, the PER curves presented in Fig. 7 for this technique have been obtained without introducing bit stuffing, contrary to the PER curves for the proposed receiver, where bit stuffing is actually present and is taken into account. The proposed method provides a gain of at least 3 dB when the interference level is low and more than 6 dB when the interference level is high. These results show that the proposed receiver is more resistant to interferences than the receiver of [2] (in addition, the receiver allows bit stuffing to be considered, contrary to the algorithm of [2]). This is due jointly to the interference mitigation and to the efficiency of the proposed error correction strategy.

Fig. 8(a) shows the algorithm performance for different numbers of interfering signals, for a carrier-to-interference ratio (C/I) fixed to 5 dB. The algorithm presented in section 5.1 is used for the single interferer case whereas the algorithm of section 5.2 is used for multiple interferers. One can see that, the more concentrated the interference power into one single signal, the better the performance. This result can be explained as follows: when the interference is concentrated into one single interfering user, the mean power $\bar{e}_u^2$ is close to the instantaneous interference power, resulting in good interference reduction. Fig. 8(b) shows that the detector performs similarly for one or multiple interferers for large C/I ratio (C/I $= 7$ dB). Indeed, with higher C/I, the interference power becomes negligible, and thus the interference mitigation technique has minor effect.

6.4. Multi-user scenario with phase tracking

This section considers the case of a multi-user transmission where the phase shift for the user of interest is unknown. Therefore, one resorts to the algorithm proposed in section 5.3. Figures 9(a) and 9(b) present the PER obtained with 1 and 4 interferers, respectively. For these simulations, the actual modulation index is $h = 0.45$, while the estimated modulation index is $\hat{h} = 0.47$. Moreover, C/I is fixed to 7 dB, and the maximum phase shift $\Delta\phi$ considered in the phase tracking procedure is $\Delta\phi = 6°$. For comparison, these figures show the PER obtained without phase shift. The PER

DOI: 10.1002/sat

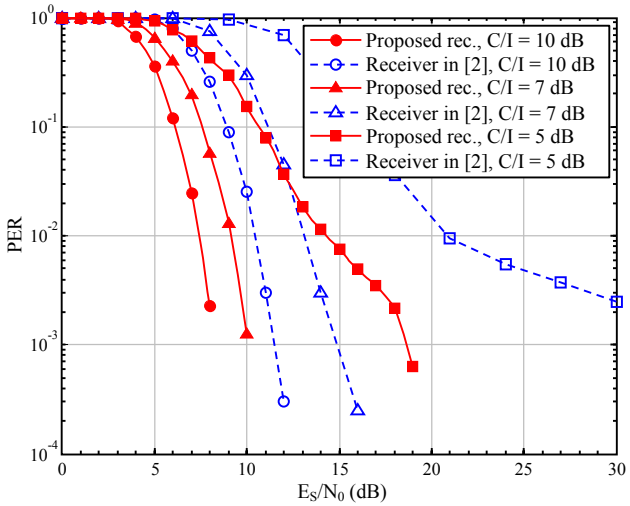
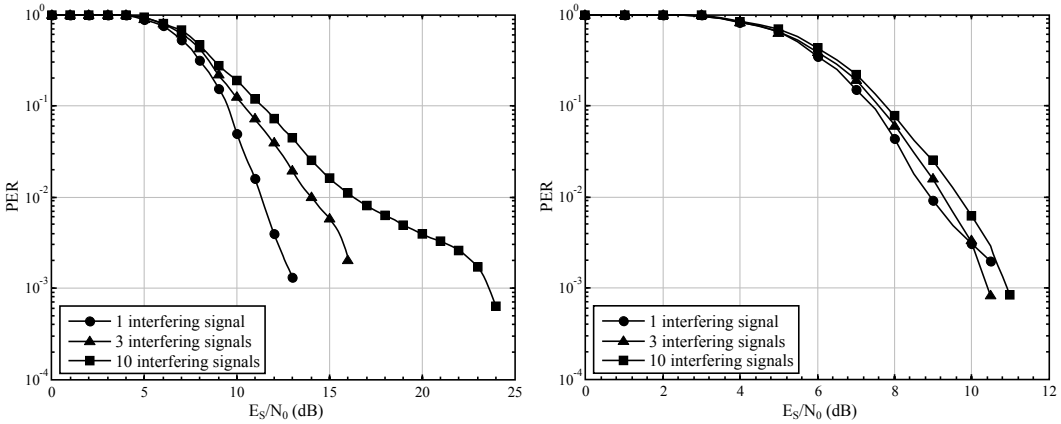


Figure 7. Comparison in Packet Error Rate between the proposed receiver with 4 interfering signals and the strategy introduced in [2] for different C/I ratios.



(a) C/I = 5 dB (b) C/I = 7 dB

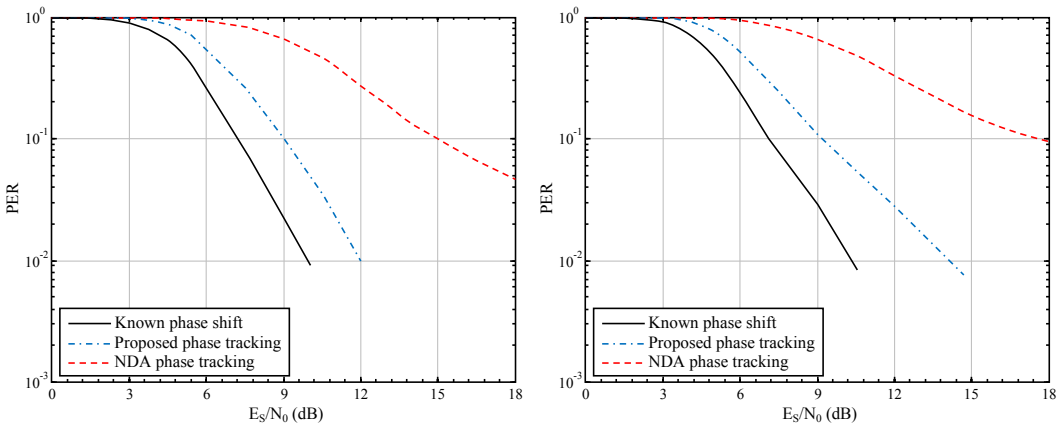
Figure 8. Influence of the number of interfering signals on the receiver performance in PER with C/I = 5 dB (a) and C/I = 7 dB (b).

obtained in the presence of phase shift using the NDA phase estimation is also displayed in the different figures. Obviously, one can note a performance loss when the phase shift is unknown and has to be estimated. This loss (multi-user case) is a bit higher than the one observed in Section 6.2 (mono-user case with phase tracking). However, it also clearly appears from this comparison that the detection algorithm proposed in this paper significantly outperforms the NDA estimation-based detection algorithm.

7. CONCLUSION

This paper proposed different CRC-based receivers for the demodulation of AIS signals for mono-user and multi-user transmissions. These receivers were designed to handle known and unknown phase shift. All receivers developed a particular Viterbi algorithm based on extended states, composed of a CRC-state and a TC-state. The bit-stuffing procedure was managed by defining specific conditional transitions in the extended trellis. The proposed receivers were simulated for

DOI: 10.1002/sat



(a) 1 interferer (b) 4 interferers

Figure 9. PER of different receivers in the presence of 1 interferer (a) and 4 interferers (b).

realistic AIS scenarios, in particular for cases where the actual modulation index is different from the value specified by the AIS recommendation. The proposed algorithms were compared with other techniques proposed in the literature for the demodulation of AIS signals. The comparison showed performance improvement for the proposed receivers in terms of packet error rates. A multi-user strategy with a computational complexity close to the mono-user algorithm was finally investigated. Further work will consider the estimation of the modulation index and its impact on the performance results.

DOI: 10.1002/sat

A. MONO-USER ALGORITHM

This appendix provides more details about the detection algorithm presented in Section 3, for the mono-user scenario with known phase shift. Note that the algorithms designed for phase tracking and multi-user scenario can be seen as a generalization of this algorithm. As mentioned in Section 3.5, this algorithm is composed of 4 steps, described below.

In these algorithms, N_S is the number of symbols, $\mathit{Distance}(x_k, S_s)$ is the cost function of the Viterbi algorithm (actually the distance between the received symbol x_k and the reference symbol S_s), $\mathit{NextS}(\boldsymbol{\sigma}_{TC}, b)$ is the symbol following the TC-state $\boldsymbol{\sigma}_{TC}$ and carrying the bit b. N_{TC} and N_{CRC} are the numbers of TC-states and CRC-states.

Algorithm 1 Initialization

$\Gamma[0,(:;:)] \leftarrow \infty$
$\Gamma[0,(A;\alpha)] \leftarrow 0$
$P[0,(:;:)] \leftarrow 0$
$S[0,(:;:)] \leftarrow 0$
$R[0,(:;:)] \leftarrow 0$

Algorithm 2 Transition variable computation

for $s = 1$ to N_S **do**
  $d[s] \leftarrow \mathit{Distance}(x_k, S_s)$
end for
for $\boldsymbol{\sigma}_{TC} = 0$ to $N_{TC} - 1$ **do**
  $\Gamma_{\text{trans}}[(:;\boldsymbol{\sigma}_{TC}),0] \leftarrow d[\mathit{NextS}(\boldsymbol{\sigma}_{TC},0)]$
  $\Gamma_{\text{trans}}[(:;\boldsymbol{\sigma}_{TC}),1] \leftarrow d[\mathit{NextS}(\boldsymbol{\sigma}_{TC},1)]$
end for
$\Gamma_{\text{trans}}[(:;:),0] \leftarrow \Gamma_{\text{trans}}[(:;:),0] + \Gamma[k-1,(:;:)]$
$\Gamma_{\text{trans}}[(:;:),1] \leftarrow \Gamma_{\text{trans}}[(:;:),1] + \Gamma[k-1,(:;:)]$
$\Gamma_{\text{trans}}[(:;:),\mathit{SB}] \leftarrow \infty$
$P_{\text{trans}}[(:;:),0] \leftarrow 0$
$P_{\text{trans}}[(:;:),1] \leftarrow P[k-1,(:;:)] + 1$
$P_{\text{trans}}[(:;:),\mathit{SB}] \leftarrow 0$
$S_{\text{trans}}[(:;:)] \leftarrow S[k-1,(:;:)]$
for $\boldsymbol{\sigma}_{CRC} = 0$ to $N_{CRC} - 1$ **do**
  for $\boldsymbol{\sigma}_{TC} = 0$ to $N_{TC} - 1$ **do**
    if $P[k-1,(\boldsymbol{\sigma}_{CRC};\boldsymbol{\sigma}_{TC})] = \overline{P}$ **then**
      $\Gamma_{\text{trans}}[(\boldsymbol{\sigma}_{CRC};\boldsymbol{\sigma}_{TC}),\mathit{SB}] \leftarrow \Gamma_{\text{trans}}[(\boldsymbol{\sigma}_{CRC};\boldsymbol{\sigma}_{TC}),0]$
      $\Gamma_{\text{trans}}[(\boldsymbol{\sigma}_{CRC};\boldsymbol{\sigma}_{TC}),0] \leftarrow \infty$
      $\Gamma_{\text{trans}}[(\boldsymbol{\sigma}_{CRC};\boldsymbol{\sigma}_{TC}),1] \leftarrow \infty$
      $S_{\text{trans}}[(\boldsymbol{\sigma}_{CRC};\boldsymbol{\sigma}_{TC})] \leftarrow S_{\text{trans}}[(\boldsymbol{\sigma}_{CRC};\boldsymbol{\sigma}_{TC})] + 1$
    end if
  end for
end for

DOI: 10.1002/sat

Algorithm 3 State variable computation

for $\boldsymbol{\sigma}_{CRC} = 0$ to $N_{CRC} - 1$ **do**
  for $\boldsymbol{\sigma}_{TC} = 0$ to $N_{TC} - 1$ **do**
    $\boldsymbol{T\sigma}_{CRC}(0) \leftarrow \mathit{Prev}\boldsymbol{\sigma}_{CRC}(\boldsymbol{\sigma}_{CRC}, 0)$
    $\boldsymbol{T\sigma}_{CRC}(1) \leftarrow \mathit{Prev}\boldsymbol{\sigma}_{CRC}(\boldsymbol{\sigma}_{CRC}, 1)$
    $\boldsymbol{T\sigma}_{CRC}(SB) \leftarrow \boldsymbol{\sigma}_{CRC}$
    $\boldsymbol{T\sigma}_{TC}(0) \leftarrow \mathit{Prev}\boldsymbol{\sigma}_{TC}(\boldsymbol{\sigma}_{TC}, 0)$
    $\boldsymbol{T\sigma}_{TC}(1) \leftarrow \mathit{Prev}\boldsymbol{\sigma}_{TC}(\boldsymbol{\sigma}_{TC}, 1)$
    $\boldsymbol{T\sigma}_{TC}(SB) \leftarrow \mathit{Prev}\boldsymbol{\sigma}_{TC}(\boldsymbol{\sigma}_{TC}, 0)$
    $b_{\min} \leftarrow \arg\min_b \Gamma_{\text{trans}}[(\boldsymbol{T\sigma}_{CRC}(b); \boldsymbol{T\sigma}_{TC}(b)), b]$
    $\Gamma[k, (\boldsymbol{\sigma}_{CRC}; \boldsymbol{\sigma}_{TC})] \leftarrow \Gamma_{\text{trans}}[(\boldsymbol{T\sigma}_{CRC}(b_{\min}); \boldsymbol{T\sigma}_{TC}(b_{\min})), b_{\min}]$
    $P[k, (\boldsymbol{\sigma}_{CRC}; \boldsymbol{\sigma}_{TC})] \leftarrow P_{\text{trans}}[(\boldsymbol{T\sigma}_{CRC}(b_{\min}); \boldsymbol{T\sigma}_{TC}(b_{\min})), b_{\min}]$
    $S[k, (\boldsymbol{\sigma}_{CRC}; \boldsymbol{\sigma}_{TC})] \leftarrow S_{\text{trans}}[(\boldsymbol{T\sigma}_{CRC}(b_{\min}); \boldsymbol{T\sigma}_{TC}(b_{\min}))]$
    $R[k, (\boldsymbol{\sigma}_{CRC}; \boldsymbol{\sigma}_{TC})] \leftarrow b_{\min}$
  end for
end for

Algorithm 4 Path reading

$\boldsymbol{\sigma}_{CRC} \leftarrow 0$
$\boldsymbol{\sigma}_{TC} \leftarrow \boldsymbol{\sigma}^f_{TC}$
$n \leftarrow K - S[K, (0; \boldsymbol{\sigma}^f_{TC})]$
for $k = K$ to 1 **do**
  $b \leftarrow R[k, (\boldsymbol{\sigma}_{CRC}; \boldsymbol{\sigma}_{TC})]$
  if $b \neq SB$ **then**
    $\boldsymbol{\sigma}_{CRC} \leftarrow \mathit{Prev}\boldsymbol{\sigma}_{CRC}(\boldsymbol{\sigma}_{CRC}, b)$
    $\boldsymbol{\sigma}_{TC} \leftarrow \mathit{Prev}\boldsymbol{\sigma}_{TC}(\boldsymbol{\sigma}_{TC}, b)$
    $U_n \leftarrow b$
    $n \leftarrow n - 1$
  else
    $\boldsymbol{\sigma}_{TC} \leftarrow \mathit{Prev}\boldsymbol{\sigma}_{TC}(\boldsymbol{\sigma}_{TC}, 0)$
  end if
end for

DOI: 10.1002/sat

B. MINIMUM PHASE DERIVATION

Given the definition of $\Delta[k,(A;\alpha),b,\phi]$ in (19), it is straightforward to show that the minimization problem (20) can be re-expressed as the following maximization problem

$$\max_{\phi\in\mathcal{I}_k^{(A;\alpha)}} \Re e\left(e^{-j\phi} r_k \overline{m_k^{k+1,(A;\alpha),b}}\right). \tag{36}$$

Denoting M_k and ψ_k as the modulus and the phase of $r_k\overline{m_k^{k+1,(A;\alpha),b}}$, (36) reduces to

$$\max_{\phi\in\mathcal{I}_k^{(A;\alpha)}} M_k\cos(\phi-\psi_k). \tag{37}$$

Denoting as

$$\begin{aligned}\phi_m^k &= \phi_k^{k,(A;\alpha)} - \psi_k - \Delta\phi\\ \phi_M^k &= \phi_k^{k,(A;\alpha)} - \psi_k + \Delta\phi,\end{aligned}$$

the analytic solution of (20) is defined as follows

- if $0\in[\phi_m^k;\phi_M^k]$ (modulo 2π),

$$\begin{aligned}\Delta_{\min}[k,(A;\alpha),b] &= \left(|r_k|^2+|m_k^{k+1,(A;\alpha),b}|^2\right) - 2M_k\\ \phi_{\text{trans}}^{k,(A;\alpha),b} &= \psi_k\end{aligned}$$

- if $0\notin[\phi_m^k;\phi_M^k]$ (modulo 2π),

$$\begin{aligned}\Delta_{\min}[k,(A;\alpha),t] &= \left(|r_k|^2+|m_k^{k+1,(A;\alpha),b}|^2\right) - 2M_k\max\left(\cos\phi_m^k,\cos\phi_M^k\right)\\ \phi_{\text{trans}}^{k,(A;\alpha),b} &= \psi_k + \underset{\phi=(\phi_m^k,\phi_M^k)}{\arg\max}\ \cos\phi.\end{aligned}$$

DOI: 10.1002/sat

REFERENCES

1. Recommendation ITU-R M1371. Technical characteristics for a universal automatic identification system using time division multiple access in the VHF maritime mobile band. ITU, 2001.
2. Scorzolini A, Perini VD, Razzano E, Colavolpe G, Mendes S, Fiori P, Sorbo A. European enhanced space-based AIS system study. *Adv. Sat. Mul. Sys. Conf.* 2010; **5**:9–16.
3. Burzigotti P, Ginesi A, Colavolpe G. Advanced receiver design for satellite-based automatic identification system signal detection. *Int. Journal of Sat. Comm. and Net.* 2012; **30**(2):52–63.
4. McDaniel B. An algorithm for error correcting cyclic redundance checks. *C/C++ Users Journal* 2003; :6.
5. Babaie S, Zadeh AK, Es-hagi SH, Navimipour NJ. Double bits error correction using CRC method. *Proc. Int. Conf. Semantics, Knowledge and Grid* 2009; **5**:254–257, doi:http://doi.ieeecomputersociety.org/10.1109/SKG.2009.77.
6. Shi-yi C, Yu-bai L. Error correcting cyclic redundancy checks based on confidence declaration. *Proc. ITS Telecommunications* 2006; **6**:511–514.
7. Zhang Y, Yuan Q. A multiple bits error correction method based on cyclic redundancy check codes. *ICSP Signal Processing* 2008; **9**:1808–1810.
8. Wang R, Zhao W, Giannakis GB. CRC-assisted error correction in a convolutionally coded system. *IEEE Trans. Comm.* 2008; **56**(11):1807–1815.
9. Prévost R, Coulon M, Bonacci D, LeMaitre J, Millerioux JP, Tourneret JY. Multi-encodage error correction with extended trellis. Patent Pending.
10. Prévost R, Coulon M, Bonacci D, LeMaitre J, Millerioux JP, Tourneret JY. A Viterbi algorithm with conditional transitions. Patent Pending.
11. Raheli R, Polydoros A, Tzou C. Per-survivor processing: A general approach to MLSE in uncertain environments. *IEEE Trans. Comm.* 1995; **43**(234):354–364.
12. Prévost R, Coulon M, Bonacci D, LeMaitre J, Millerioux JP, Tourneret JY. CRC-Assisted Error Correction in a Trellis Coded System with Bit Stuffing. *IEEE Workshop on Stat. Signal Processing, Nice, France* June 2011; :381–384.
13. Prévost R, Coulon M, Bonacci D, LeMaitre J, Millerioux JP, Tourneret JY. Une technique de correction d'erreurs basée sur le CRC pour des systèmes codés en treillis contenant des bits de bourrage. *GRETSI, Bordeaux, France* Sept 2011; .
14. Prévost R, Coulon M, Bonacci D, LeMaitre J, Millerioux JP, Tourneret JY. Joint phase-recovery and demodulation-decoding of AIS signals received by satellite. *IEEE Int. Conf. Acoust., Speech, and Signal Processing, Vancouver, Canada* 2013; Submitted.
15. Prévost R, Coulon M, Bonacci D, LeMaitre J, Millerioux JP, Tourneret JY. Interference mitigation and error correction method for AIS signals received by satellite. *European Signal and Image Processing Conference*, Bucarest, Roumanie, 2012.
16. Chuang CY, Yu X, Jay Kuo CC. Space-time blind delay and DOA estimation in chip-asynchronous DS-CDMA systems. *Global Telecommu. Conf.*, vol. 4, 2004; 2508–2512.
17. Pukkila M, Mattellini GP, Ranta PA. Constant modulus single antenna interference cancellation for GSM. *IEEE Trans. Veh. Technol.* 2005; **1**(59):584–588.

DOI: 10.1002/sat