The Journal of Navigation (2022), **75**:2 333–345
doi:10.1017/S0373463321000837

RESEARCH ARTICLE

Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility

Gareth Wimpenny,* Jan Šafář, Alan Grant, and Martin Bransby

The General Lighthouse Authorities of the United Kingdom and Ireland.
***Corresponding author.** E-mail: gareth.wimpenny@gla-rad.org

Received: 07 May 2021; **Accepted:** 11 October 2021; **First published online:** 14 December 2021

Keywords: AIS; Spoofing; Authentication; VDES

Abstract
The civilian Automatic Identification System (AIS) has no inherent protection against spoofing. Spoofed AIS messages have the potential to interfere with the safe navigation of a vessel by, amongst other approaches, spoofing maritime virtual aids to navigation and/or differential global navigation satellite system (DGNSS) correction data conveyed across it. Acting maliciously, a single transmitter may spoof thousands of AIS messages per minute with the potential to cause considerable nuisance; compromising information provided by AIS intended to enhance the mariner's situational awareness. This work describes an approach to authenticate AIS messages using public key cryptography (PKC) and thus provide unequivocal evidence that AIS messages originate from genuine sources and so can be trusted. Improvements to the proposed AIS authentication scheme are identified which address a security weakness and help avoid false positives to spoofing caused by changes to message syntax. A channel loading investigation concludes that sufficient bandwidth is available to routinely authenticate all AIS messages whilst retaining backwards compatibility by carrying PKC 'digital signatures' in a separate VHF Data Exchange System (VDES) side channel.

1. Introduction

Over recent years, awareness of cyber-threats has been growing within the maritime industry, and groups such as the International Maritime Organization (IMO) and the UK Department for Transport have indicated that the industry may be the target of dedicated, professional cyber-attack (Boyes et al., 2016; IMO, 2016). In an effort to improve maritime cyber-security, the IMO has taken steps requiring vessel operators to address cyber-security through resolution MSC.428(98) (IMO, 2017). Cyber-security guidelines have been published by various maritime industry bodies that are intended to assist compliance with MSC.428(98), including updated guidance from the Baltic and International Maritime Council (BIMCO et al., 2020). Technical standards to address maritime cyber-security have also been published by the International Electrotechnical Commission (IEC, 2021). Whilst it is clear much effort has been directed at improving maritime cyber-security, against this backdrop comparatively little has been done to improve the security of the Automatic Identification System (AIS).

AIS is a compulsory requirement for all SOLAS (IMO Convention on the Safety of Life At Sea) class vessels and it is particularly vulnerable to cyber-attack. This paper describes how spoofing of AIS has the potential to interfere with the safe navigation of a vessel and how such spoofing can be prevented through the use of public key cryptography (PKC). This paper describes a series of improvements to a

PKC authentication system for AIS first described by the authors in 2018 (Wimpenny et al., 2018) and investigates the impact of AIS channel loading due to the use of PKC.

2. Vulnerability of AIS to spoofing attack

AIS makes use of two frequencies in the maritime VHF band, namely 161·975 MHz and 162·025 MHz (VHF channels AIS 1 and AIS 2) (International Telecommunication Union, 2014). The AIS protocol allows the exchange of short messages in certain specified formats with a bit rate of 9·6 kbps. The available AIS bandwidth is shared between its users by way of time division multiple access (TDMA). This divides the bandwidth of each AIS channel into 2,250 time slots established every 60 s. Each time slot can thus represent up to 256 bits of information with the majority of 'ordinary' AIS messages typically taking up one time slot. Transmission time slots are allocated to users through a system of self-organisation (SOTDMA) or, in the case of AIS equipment fitted to non-SOLAS vessels, by carrier sensing (CSTDMA).

AIS is primarily used as a situational awareness tool with vessels, and some maritime aids to navigation (AtoN), conveying their identity and position (usually obtained from a local global navigation satellite systems [GNSS] receiver) via AIS to nearby vessels and shore stations. This data is then typically displayed to the end-user via an electronic chart display and information system (ECDIS), though other display types are also prevalent.

The AIS protocol was developed on the basis that all vessels, shore stations and AtoN need to be able to transmit location (and other) data to each other freely and openly. As such, the civilian AIS protocol was developed with no encryption or authentication mechanism. This makes it possible for a malicious actor to transmit (spoof) any conceivable AIS message and it will be taken at face value; processed by any AIS receiver within range as if the message was genuine.

Such AIS spoofing attacks may be used to spoof the presence of AtoN or vessels on ECDIS and other AIS displays; however, a range of more serious attacks are possible, including:

- Driving a vessel off course or re-routing it by spoofing the presence of virtual aids to navigation (VAtoN) via a spoofed 'AIS Message 21'. VAtoN have no physical presence, but instead provide data via an AIS message which is used to display the presence of AtoN electronically on an ECDIS. Legitimate uses for VAtoN include the marking of new hazards (such as a dangerous wreck) whilst authorities arrange for a physical AtoN, or in instances where a physical AtoN is not appropriate.
- Spoofing a vessel's reported position by providing it with false DGNSS corrections via a spoofed 'AIS Message 17'. Such an attack could interfere with a vessel's ability to navigate safely and has the potential to lead a vessel into harm (depending on how this data is used on the bridge).
- Performing denial of service attacks by misusing AIS channel management broadcasts via spoofing 'AIS Message 22'. Such broadcasts could be used to instruct all AIS transceivers within range to cease operation or switch their AIS broadcasting onto an inappropriate maritime VHF channel, thereby interfering with other maritime communications[1].

The above are all particularly nefarious forms of attack as, unlike spoofing the presence of a physical AtoN or vessel, these spoofing attacks cannot be verified visually or against data from another system, such as radar, and the mariner is reliant solely on AIS data.

By ignoring TDMA allocations, one single transmitter may occupy multiple consecutive AIS transmission time slots and thus spoof thousands of AIS messages per minute. This could allow a malicious actor to spoof the presence of a very large number of vessels (which could be used to hinder vessel traffic services operations) and/or simultaneously spoof very large numbers of AtoN and/or VAtoN using just a single transmitter. Such a 'mass' spoofing attack could mask the presence of a genuine virtual AtoN by surrounding the area with spoofed examples; the mariner would then have no way of identifying which

[1] It is understood that to protect against such attacks there is a plan to remove channel management messages from AIS as part of the ongoing revision of ITU-R M.1371-5. If channel management messages are removed then no protection need be developed for them, though the threat of their spoofing will remain until all legacy AIS transceivers are phased out.

https://doi.org/10.1017/S0373463321000837 Published online by Cambridge University Press

is genuine. Mass spoofing attacks could also spoof the presence of multiple vessels, AtoN or VAtoN at the same coordinates as a legitimate radar return, thereby hindering identification of the return.

AIS spoofing attacks have been observed 'in the wild', a number of which are described by Androjna et al. (2021). These include an incident of mass AIS spoofing identified off the island of Elba in December 2019 where 3,741 vessels were spoofed, all densely packed into a small sea area.

3. Cryptographic authentication of AIS

To guard against spoofing, the direction of arrival of AIS transmissions could be used to indicate if they originate from their reported source of transmission. Direction-finding techniques are, however, useless against those AIS message types which do not state their transmission coordinates and are therefore useless in guarding against the more serious VAtoN, DGNSS and channel management spoofing attacks described above; none of which state their transmission coordinates within the AIS message.

Unlike direction-finding techniques, prior work by the authors has identified a *cryptographic* authentication system, using PKC to 'digitally sign' messages, as capable of providing unequivocal evidence that all AIS message types originate from genuine sources and so can be trusted (Wimpenny et al., 2018). PKC is explained further in earlier work by the authors (Wimpenny et al., 2017); however, a summary of how it is used for authentication is provided here for convenience.

PKC uses two mathematically related keys, a public and a private key, together known as a *key pair*. The public and private key (both stored as computer files) are used to encrypt and decrypt data. The public key is openly distributed to all users, whereas the private key is kept secret and known only to the message sender. To authenticate a message, the sender encrypts the message using their private key. In so doing, the message may only be decrypted with the public key. This does not provide secrecy as the message may be decrypted by any user with the openly available public key, but provides authentication; by decrypting the message with the public key the user knows it can only have been encrypted by the holder of the private key (the message sender) and therefore cannot have been spoofed or otherwise manipulated by a malicious actor.

Rather than encrypt the entire message with the private key (and so prevent a recipient without the public key from reading it), the preferred approach is to broadcast the message unencrypted in plain sight with an accompanying digital signature. To accomplish this, the sender first uses a 'hash function' on the message they wish to sign. This is an algorithm that maps message data of arbitrary size to a separate fixed-size string of characters. This separate string of characters, unique to the message, is known as a digest. The digest (not the message) is then encrypted with the private key to produce a digital signature. This digital signature may be sent separately, alongside the unencrypted message to provide authentication of the message.

When using PKC for authentication, numerous algorithms with varying key sizes are available which provide varying levels of security, speed and subsequent size of digital signature. The PKC algorithms recommended for use in authenticating AIS are the SHA-256 hashing algorithm and the elliptic curve digital signature algorithm (ECDSA) with a key size of 256 bits and using the 'secp256r1' curve (Wimpenny et al., 2018). These algorithms and key sizes were chosen as it was shown that they give relatively small digital signatures, 512 bits in size, which are capable of fitting within a multi-part AIS message. The algorithms and key sizes also provide robust security, as indicated in a report authored by the then European Union Agency for Network and Information Security (ENISA, 2013) and by the US National Institute for Standards and Technology (NIST) (Barker, 2020).

To maintain backwards compatibility with the current use of AIS, authentication is accomplished not by modifying existing AIS data messages, but instead by including the digital signature in a separate 'follow-on' message, in the form of either an AIS binary 'Message 6' or 'Message 8'. This is represented in Figure 1 where a Data Message (Message 21) containing details of a VAtoN is followed by a separate Signature Message (Message 8) containing the digital signature.

For the recipient to link the Data Message with the correct Signature Message, a unique identifier is needed. AIS messages do not contain a unique identifier and backward compatibility would be lost

https://doi.org/10.1017/S0373463321000837 Published online by Cambridge University Press

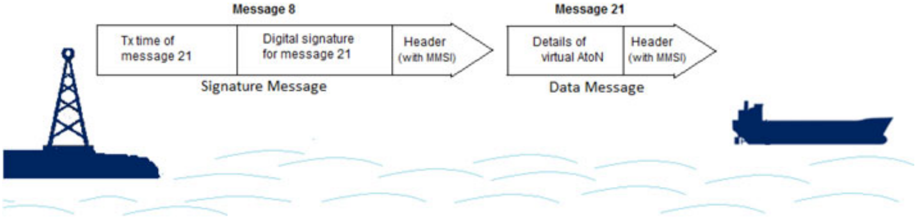

Figure 1. *Representation of a virtual AtoN (Message 21) broadcast, followed by a broadcast containing a digital signature (Message 8) (Wimpenny et al., 2018).*

should the AIS messages be modified to include one; whilst the Maritime Mobile Service Identity Number (MMSI) is routinely included in the headers of all AIS messages, the MMSI alone is unsuited for this task as multiple AIS messages will naturally contain the same MMSI, making it impossible to relate a Signature Message to an individual Data Message.

To overcome this, the approach used by Wimpenny et al. (2018) is to include in the Signature Message a 64-bit timestamp relating to the time of the message being signed i.e. the time of the previous Data Message. It was further reasoned that by using a combination of timestamp and MMSI, the correct Signature Message could be uniquely linked to the correct Data Message and that this approach would retain backwards compatibility with the existing AIS protocol.

It is noted that to timestamp and correctly identify the Data Message, this approach requires both the message sender and recipient to have a local trusted clock synchronised to UTC. For simplicity, this should be the same local UTC clock synchronised to a GNSS time source as used for TDMA message synchronisation by the AIS transceivers.

It is further noted that the proposed technique verifies only the authenticity and integrity of AIS messages and does not prevent position tampering by feeding the AIS transponder with spoofed GNSS data. Addressing GNSS spoofing is beyond the scope of this paper.

4. Comparison of approaches to secure AIS

In recent years, several alternative approaches have been proposed to secure AIS. Of these, Hall et al. (2015) proposed an approach based on the IEEE 1609 standard for wireless access in vehicular environments. Whilst Hall's technique is robust, it is not backwards compatible with the existing AIS protocol, meaning its use would require a new AIS standard to be adopted. Furthermore, Hall takes steps to encrypt (as well as authenticate) some AIS data for privacy. Whilst there are advantages to encryption, such as preventing those engaged in piracy from reading AIS messages, the potential for legitimate users to be prevented from reading them suggests the routine use of encryption is inappropriate.

Stewart et al. (2018) proposed a backwards compatible approach to AIS authentication using a technique similar to that proposed by Wimpenny et al. (2018) (described previously) in which an AIS Data Message is followed by a separate message containing a digital signature. However, Stewart does not address how the Data and Signature Messages can be linked together. Stewart therefore proposes an alternative method in which the follow-on message contains both data (repeated from the first message) and signature combined. A correctly equipped AIS receiver could then simply discard the first (unsigned) Data Message and opt to display only the signed follow-on message.

Whilst this combined message approach is both feasible and backwards compatible, it is considered by the authors as potentially unsuitable for authenticating those AIS messages that may take up more than one time slot, such as AIS Message 21. This is because (noting that Wimpenny et al. [2018] showed a secure digital signature requires four time slots) the combined data-signature message would exceed the five-slot maximum permissible size of AIS Messages 6 and 8. However, the possibility exists that a multi-slot Data Message might be compressed to fit the limited space, albeit this would add complexity. This possibility is not addressed here but could be considered as a future research option.

https://doi.org/10.1017/S0373463321000837 Published online by Cambridge University Press

Goudossis and Katsikas (2019) proposed an approach, further developed in their later work (Goudossis and Katsikas, 2020), that uses 'identity based encryption' (IBC) to both authenticate and/or encrypt AIS messages. Goudossis and Katsikas state that their proposed approach is unsuited to authenticating multi-slot AIS messages due to data-signature message sizes exceeding the five-slot maximum size of Message 6 and 8. IBC also has a potential disadvantage in that this technique requires a trusted third party to be employed to handle private keys. This may cause security and logistical difficulties.

Kessler (2020) proposed an approach in which an AIS Data Message is followed directly by a digital signature as part of the same transmission, thereby avoiding difficulties linking a separate Data Message and Signature Message together. Kessler suggests this method is backwards compatible as a conventional AIS receiver not equipped to verify signatures would simply ignore the appended signature. This assumption is questionable, as receivers may instead reject the entire transmission as corrupt. This approach also violates the existing AIS standard described by ITU-R M.1371-5 (International Telecommunication Union, 2014). In a bid to minimise digital signature sizes, Kessler's approach uses the RSA cryptographic algorithm with 256-bit key sizes. Such small RSA keys are not considered adequately secure by NIST (Barker, 2020).

More recently, Sciancalepore et al. (2021) proposed a technique using the TESLA authentication algorithm. This algorithm reduces data overheads by broadcasting a Signature Message relating to the previous N Data Messages. This approach therefore introduces a delay before Data Messages can be verified and is thus thought less suited for use with infrequent AIS broadcasts; including AIS Message 21 which is normally broadcast at 3 minute intervals. Sciancalepore et al. use small, 80-bit security equivalent key sizes that are not considered adequately secure by NIST (Barker, 2020).

5. Improved approach to AIS authentication

Improvements to the AIS authentication scheme first proposed by Wimpenny et al. (2018), described in section 3, are identified which improve Data Message and Signature Message linking, address a security weakness and help avoid false positives to spoofing caused by changes to message syntax. These are described as follows.

5.1. *Improving linking of Data Messages and Signature Messages*

To link the correct Signature Message to the correct Data Message, the technique proposed by Wimpenny et al. (2018) was to include within the Signature Message a 64-bit UNIX timestamp pertaining to the transmission time of the Data Message. However, this UNIX timestamp alone cannot identify the correct Data Message as UNIX timestamps provide only a 1 second resolution which may pertain to any one of 37·5 AIS time slots within which the Data Message may have been sent. Therefore the recipient will also need to examine the MMSI of every message received within this 1 second period to positively identify the correct Data Message; namely, the message which also has the same MMSI as the Signature Message.

A proposed improvement is instead to use a 64-bit timestamp which precisely identifies the AIS time slot used by the Data Message, a suggested method being to count the number of AIS time slots that have occurred since 00:00:00 UTC, 1 January 2021. Such a precise approach would allow the AIS receiver to more 'elegantly' link the Data Message and Signature Message together rather than using a combination of MMSI and a coarser timestamp. This approach does have a complication in that an AIS transmitter sending a Data Message will need to make available the Data Message's transmission time slot for use as a timestamp in constructing the follow-on Signature Message. Whilst this difficulty can be overcome, work will likely be needed on AIS transmitter design to incorporate this functionality.

5.2. *Preventing vulnerability to a 'replay attack'*

A security weakness was identified with the authentication scheme as the timestamp (shown in Figure 1 as the 'Tx time of message 21') is not signed and therefore cannot be verified (it is noted that the

https://doi.org/10.1017/S0373463321000837 Published online by Cambridge University Press

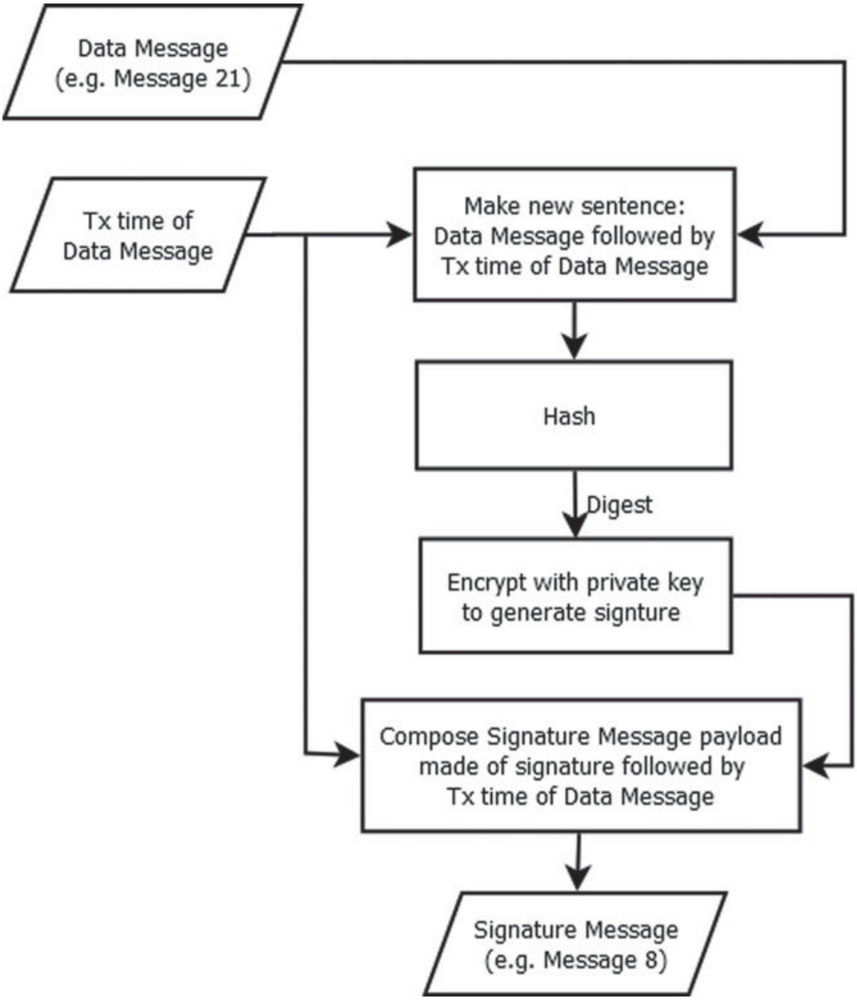

Figure 2. *Modified digital signing procedure to guard against replay attacks.*

authentication scheme proposed by Stewart et al. [2018] suffers from a similar weakness). This makes it possible for a malicious actor to record both the Data Message and Signature Message broadcasts, modify the timestamp to a later time and rebroadcast both messages at the new later time. Such a 'replay attack' would be undetectable as it effectively reuses a genuine digital signature. To protect against such an attack the authentication scheme must be adapted such that both the Data Message and timestamp are signed.

A procedure for accomplishing this is shown in Figure 2 where a Data Message (in this example, an AIS Message 21 broadcast) and timestamp (the transmission time of the AIS Message 21) are first merged into a new sentence. The new combined sentence is then hashed and signed to form the signature. The Signature Message (AIS Message 8) is then composed as previously, from the signature followed by the timestamp. The Data Message and Signature Message may then be broadcast from an AIS transceiver in the ordinary manner.

Upon receiving the Data Message the recipient will be able to read the message as normal without hindrance. The recipient may, if in possession of the sender's public key and having also identified and be in receipt of the Signature Message, then verify the Data Message using the procedure shown in Figure 3. Here it can be seen that the Signature Message is first split into its signature and timestamp components. Two operations then take place:

https://doi.org/10.1017/S0373463321000837 Published online by Cambridge University Press

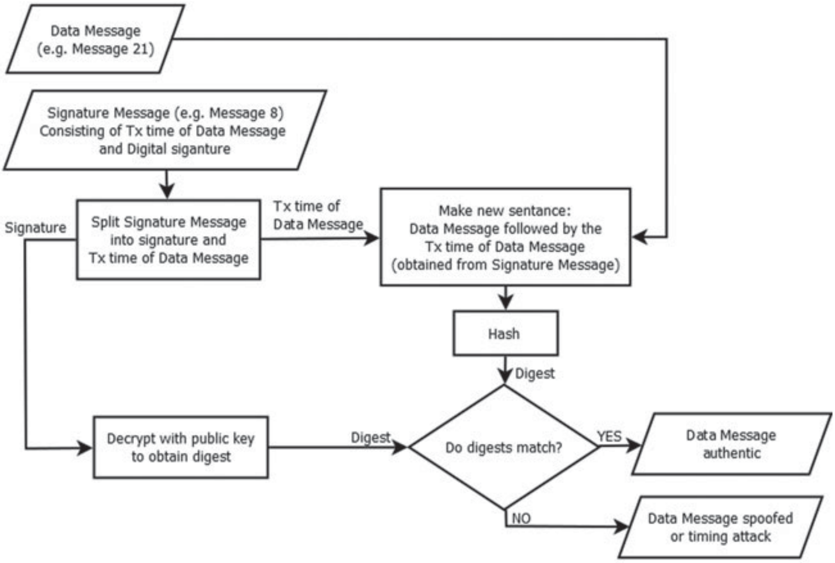

Figure 3. *Verifying the Digital Signature.*

- The Data Message and timestamp component are merged into a new sentence which is then hashed to obtain a digest.
- The Signature component is decrypted with the public key to obtain the digest.

If both digests match then the Data Message is genuine, as only the private key holder could possibly produce a signature (an encrypted digest) that could be correctly decrypted with the public key. Any attempts to alter either the timestamp, Data Message or Signature Message will generate an incorrect digest and cause authentication to fail, alerting the recipient to the possibility of spoofing.

5.3. Preventing verification failures due to varying syntax

The content of AIS messages may be legitimately presented in different formats with differing syntax (e.g. positions may be given in decimal degrees or degrees, minutes and seconds). However, when signing and later verifying a Data Message, it is vital that the Data Message is presented in a consistent format before the signing and the verification processes begin. This is because any variation in message syntax may appear as an attempt to illegally modify (spoof) the Data Message, thus causing verification to fail.

To ensure a consistent syntax for both signing and verification processes, the suggested approach is first to convert the Data Message into a raw AIS bitstream, as defined by ITU-R M.1371-5 (International Telecommunication Union, 2014) before the processes begin. Alternatively, other standard formats (such as IEC 61162-3) may be considered in this role.

6. Impact of signatures on AIS channel loading

A Signature Message has a total payload of 576 bits; this consisting of a 512-bit signature and a 64-bit timestamp. It is shown by Wimpenny et al. (2018) that the 576-bit payload fits into either an AIS Message 6 or Message 8 occupying four consecutive AIS time slots.

The vast majority of 'ordinary' AIS Data Messages occupy a single time slot. It is therefore evident that should each Data Message be followed by a Signature Message four times its size, then a significant impact on AIS channel loading will be seen.

https://doi.org/10.1017/S0373463321000837 Published online by Cambridge University Press

Table 1. AIS channel loading (%) due to the inclusion of four-slot Signature Messages.

Base AIS channel loading (%)	Percentage of AIS messages signed											
	1	5	10	20	30	40	50	60	70	80	90	100
10	10·4	12	14	18	22	26	30	34	38	42	46	50
20	20·8	24	28	36	44	52	60	68	76	84	92	100
30	31·2	36	42	54	66	78	90	102	114	126	138	150
40	41·6	48	56	72	88	104	120	136	152	168	184	200
50	52	60	70	90	**110**	130	150	170	190	210	230	250
60	62·4	72	84	108	132	156	180	204	228	252	276	300
70	72·8	84	98	126	154	182	210	238	266	294	322	350
80	83·2	96	112	144	176	208	240	272	304	336	368	400
90	93·6	108	126	162	198	234	270	306	342	378	414	450
100	104	120	140	180	220	260	300	340	380	420	460	500

This is shown in Table 1 where it can be seen that, unless only a small percentage of AIS messages are signed, the available AIS bandwidth will be quickly swamped by the inclusion of Signature Messages. The highlighted example shows that if AIS bandwidth is currently operating at 50% capacity (the base channel loading), then attempting to sign just 30% of these messages would exceed (110%) the available AIS bandwidth; this disregarding that AIS is unlikely to function optimally before its theoretical bandwidth limits are approached.

It is clear from Table 1 that AIS does not have sufficient bandwidth to routinely support the inclusion of digital signatures for all AIS messages. It is, however, likely that sufficient bandwidth is available to sign a small subset of AIS messages and that if this approach is pursued, consideration is given to signing only 'high risk' messages which have the potential to cause the most harm if spoofed. Consideration should therefore be given to signing only Message 21 (Aids to Navigation Reports), Message 17 (DGNSS Broadcasts) and Message 22 (Channel Management messages) previously identified as high-risk messages. This approach is likely to reduce the burden on available AIS bandwidth but may need to be reconsidered in areas of high AIS traffic where the base channel loading is already high.

7. Using the VDES to carry signatures

As AIS lacks the bandwidth to routinely support the inclusion of digital signatures for all AIS messages, consideration is given to carrying signatures in an alternative 'side channel'. This is a preferred approach as the bandwidth required for the digital signatures will not impinge on the available AIS bandwidth. It also suggests the possibility of routinely signing and authenticating all AIS traffic, rather than only a small subset of high-risk messages.

The VHF Data Exchange System (VDES) allocates several channels in the maritime VHF band for data exchange (IALA, 2019). VDES offers higher bandwidths than AIS along with comparable propagation and thus has potential for use in carrying digital signatures for AIS messages. VDES also provides a benefit in supporting forward error correction (FEC) which will reduce the likelihood of digital signatures being corrupted in transit. Using this approach will require users to be equipped with suitable VDES hardware to send and receive the separate Signature Messages.

Two components of VDES are capable of carrying Signature Messages, namely the Application Specific Message (VDES ASM) component and the VHF Data Exchange (VDE) component. Their potential for use in carrying Signature Messages is described as follows.

https://doi.org/10.1017/S0373463321000837 Published online by Cambridge University Press

***Table 2.** Available data bits for VDES ASM message payloads.*

Number of ASM slots	Maximum payload data bits (no FEC)	Maximum payload data bits (FEC 3/4)
1	384	288
2	896	672
3	1408	1056

***Table 3.** VDES ASM channel loading (%) due to the use of two-slot Signature Messages.*

Base AIS channel loading (%)	Percentage of AIS messages signed											
	1	5	10	20	30	40	50	60	70	80	90	100
10	0·2	1	2	4	6	8	10	12	14	16	18	20
20	0·4	2	4	8	12	16	20	24	28	32	36	40
30	0·6	3	6	12	18	24	30	36	42	48	54	60
40	0·8	4	8	16	24	32	40	48	56	64	72	80
50	1	5	10	20	30	40	50	60	70	80	90	**100**
60	1·2	6	12	24	36	48	60	72	84	96	108	120
70	1·4	7	14	28	42	56	70	84	98	112	126	140
80	1·6	8	16	32	48	64	80	96	112	128	144	160
90	1·8	9	18	36	54	72	90	108	126	144	162	180
100	2	10	20	40	60	80	100	120	140	160	180	200

7.1. Using VDES ASM to carry Signature Messages

Like AIS, there are two VDES ASM channels and the bandwidth of each channel is also divided into 2,250 time slots established every 60 seconds. Each time slot can represent up to 512 bits of information and VDES ASM messages may also be up to three consecutive time slots in length. This allows larger data payloads to be carried than is the case with AIS.

As with AIS, only a portion of each ASM message is available to carry the data payload as several bytes are needed for the message header and other overheads. Table 2 is derived from the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) VDES specification (IALA, 2019) and describes the number of message bits available to carry a data payload for multi-slot VDES ASM messages. Noting that the IALA specification allows the use of FEC at a rate of 3/4, the maximum payloads available are given for when both no FEC is used and for 3/4 FEC.

From Table 2 it can be seen that a two-slot VDES ASM message is needed to carry a 576-bit Signature Message payload (regardless of whether no FEC or 3/4 FEC is used). The impact of VDES ASM channel loading due to carrying a two-slot Signature Message is shown in Table 3. This shows that whilst channel loading is not as severe as when AIS is used to carry Signature Messages, should AIS messages be routinely signed then the VDES ASM bandwidth will be swamped in areas of high AIS traffic. The highlighted example shows that if AIS bandwidth is currently at 50% occupancy, then signing every AIS message will use up the entire VDES ASM bandwidth.

Whilst VDES ASM will struggle to routinely carry digital signatures for all AIS messages, sufficient bandwidth is likely available to sign the smaller subset of ‘high risk’ messages described previously. Carrying digital signatures for these messages within VDES ASM channels is preferable to using AIS channels as this prevents increased channel loading on AIS.

Table 4. *Channel loading (%) on the four VDE 25 kHz channels due to the use of single slot Signature Messages (necessitating using either 8-PSK or 16-QAM modulation schemes).*

Base AIS channel loading (%)	Percentage of AIS messages signed											
	1	5	10	20	30	40	50	60	70	80	90	100
10	0·05	0·25	0·5	1	1·5	2	2·5	3	3·5	4	4·5	5
20	0·1	0·5	1	2	3	4	5	6	7	8	9	10
30	0·15	0·75	1·5	3	4·5	6	7·5	9	10·5	12	13·5	15
40	0·2	1	2	4	6	8	10	12	14	16	18	20
50	0·25	1·25	2·5	5	7·5	10	12·5	15	17·5	20	22·5	25
60	0·3	1·5	3	6	9	12	15	18	21	24	27	30
70	0·35	1·75	3·5	7	10·5	14	17·5	21	24·5	28	31·5	35
80	0·4	2	4	8	12	16	20	24	28	32	36	40
90	0·45	2·25	4·5	9	13·5	18	22·5	27	31·5	36	40·5	45
100	0·5	2·5	5	10	15	20	25	30	35	40	45	**50**

Note: This table shows only channel loading on the VDE physical layer.

7.2. Using VDES VDE to carry Signature Messages

VDE has components intended for terrestrial and satellite use. Here only the terrestrial component is considered for use in authenticating AIS messages.

As with AIS and VDES ASM, the VDE bandwidth is also divided into 2,250 time slots established every 60 seconds. There are four VDE channels available, each 25 kHz wide, thereby giving a total of 9,000 time slots every 60 seconds. (If desired the four channels may be concatenated together into two 50 kHz channels or a single 100 kHz channel, thereby reducing the number of time slots available in each 60 second period to 4500 and 2250 respectively.) VDE also has the option to use the $\pi/4$ QPSK, 8-PSK or 16-QAM modulation schemes, the net result of which is that VDE time slots will have a different data capacity depending on the channel bandwidth and modulation scheme used.

When using VDE, the VDE link layer specification specifies the use of certain pre-defined message types where each message type has differing overheads to which some modest data capacity will be lost (IALA, 2019). For simplicity, when determining the VDE channel loading we therefore consider only channel loading on the physical layer, acknowledging that the overall VDE channel loading will be slightly higher depending on the overheads of the VDE message type(s) chosen to send the Signature Messages.

Considering only the physical layer, it is seen from the IALA VDES specification (IALA, 2019) that by using a single 25 kHz channel with either the 8-PSK or 16-QAM modulation scheme, a single time slot is capable of carrying either a 972-bit or 1296-bit data payload respectively; thus a single time slot is capable of carrying a 576-bit Signature Message, plus any modest overheads. By using either of the above modulation schemes, the impact of VDE channel loading on the physical layer of the four 25 kHz channels due to carrying the Signature Messages in a single time slot is shown in Table 4. The highlighted example shows that if AIS bandwidth is at 100% occupancy, then signing every AIS message will use only 50% of the available VDE bandwidth (this translating to using 4,500 out of an available 9,000 VDE time slots every 60 seconds) and that surplus VDE bandwidth is therefore available for any modest link layer overheads.

Whilst the above table shows it is possible for VDE to routinely carry digital signatures for all AIS messages, it is noted that the burden on the available VDE bandwidth remains significant. It is the case that using a time slot capable of carrying a 972-bit or 1,296-bit message payload to carry a 576-bit Signature Message (plus message overheads) is perhaps wasteful of bandwidth. However, VDE message

https://doi.org/10.1017/S0373463321000837 Published online by Cambridge University Press

payload capacity is not the limiting factor, it is the number of VDE time slots available and this cannot exceed 9,000 every 60 seconds.

8. Public key infrastructure

An advantage of using PKC is that, unlike the case with symmetric cryptography, public keys needed to authenticate messages may be openly published without need for secrecy. This allows public keys to be distributed openly to users either via the internet, or by using a maritime AIS, VDES or NAVDAT[2] radio broadcast (subject to available bandwidth). However to use PKC safely, a user needs to be sure that a public key has not been tampered with, and that it belongs to the entity it says it belongs to and not an imposter (i.e., each public key must be associated with the correct identity, such as an MMSI number).

This may be accomplished by means of a certificate authority (CA), which is a third party universally trusted by all users. The CA carries out checks as to the ownership of public keys and once satisfied that the public key belongs to the entity it reports to belong to, will digitally sign the public key, creating an attached 'security certificate'. Any user would see the CA's security certificate (the CA's trusted digital signature) on a public key and will know that the public key is genuine and unmolested, assuming they have trust in the CA.

An alternative to using a CA to verify public keys is using a 'web of trust' (WoT). This is a decentralised mechanism whereby any user (not just a CA) who has verified that a public key is genuine may sign the public key themselves and so issue their own security certificate. As a public key is verified by more and more users, the public key will have an increasing number of security certificates attached from many different users. A user may then determine their own 'trusted introducers', other users whose security certificates they trust. When the user then encounters a new, unfamiliar public key, the presence of one or more security certificates from a trusted introducer will verify the public key is genuine.

A WoT is useful in that it dispenses with the need for a centralised CA along with any associated administrative and financial overheads, though WoT may typically have difficulty scaling and are therefore a less preferred option.

To establish a maritime CA with the aim of authenticating AIS transmissions, different options are available, though this paper does not seek to make any recommendations. Some suggested options include that proposed by Stewart et al. (2018) whereby those organisations in countries already employed to handle the allocation of MMSIs take on an additional role as CA. Another option is to use the Maritime Identity Registry (MIR) (MCP, 2021). The MIR allows any maritime organisation to set itself up as a CA yet incorporates elements from the WoT in order to maintain a more decentralised approach.

It is suggested that a CA set up to verify AIS public keys may also be used to verify the public keys used by any future PKC system(s) developed for use with VDES, maritime 5G or other maritime communications services.

9. Conclusion

The AIS protocol currently has no authentication mechanism. Therefore, one cannot guarantee that data sent using AIS is from a legitimate source and has not been spoofed. AIS spoofing scenarios are presented by this paper which have the potential to disrupt maritime traffic, interfere with VHF communications and potentially interfere with a vessel's ability to navigate safely.

To prevent such spoofing this paper recommends that a system of cryptographically authenticating AIS messages is adopted, noting that cryptographic authentication is preferable to using radio direction-finding techniques to determine if an AIS message originates from a legitimate source. This is because direction-finding techniques can only confirm a signal is on a correct bearing, whereas cryptographic authentication can provide unequivocal evidence that a message is genuine and 'digitally signed' by its

[2] NAVDAT (Navigational Data) is a system for broadcasting data to ships. NAVDAT is comparable to the existing maritime NAVTEX (Navigational Text) system, though it offers much higher data rates. This makes NAVDAT capable of transmitting images and other data to ships, such as public key files, as well as plain text.

https://doi.org/10.1017/S0373463321000837 Published online by Cambridge University Press

sender. Furthermore, direction-finding techniques are useless in protecting against spoofing those AIS message types which do not state their transmission coordinates and are therefore useless in guarding against the more serious VAtoN, DGNSS and channel management spoofing attacks.

A technique for authenticating AIS messages using PKC, first proposed by the authors, is described along with improvements to prevent 'replay attacks' – recording legitimate AIS traffic and replaying it at a later time to cause confusion. An approach to preventing false verification failures due to changes in message data syntax is also recommended, along with an improved technique for linking messages with their digital signatures.

AIS channel loading due to the use of PKC digital signatures is investigated, with the conclusion that AIS lacks sufficient bandwidth to routinely authenticate all messages using PKC. It is, however, likely that sufficient AIS bandwidth is available to authenticate a small subset of 'high risk' message types that have the potential to cause the most harm if spoofed.

As AIS lacks sufficient bandwidth to routinely authenticate all messages, a preferred approach is to carry PKC digital signatures in a separate side channel so as not to impinge upon AIS bandwidth. This paper concludes that a VDES VDE is capable of this task and is, therefore, a recommended approach.

The proposed approach does not interfere with the existing availability and ordinary use of AIS and backwards compatibility is retained; AIS messages remain broadcast 'in the clear' and unmolested so that if this technique is adopted, mariners will be no worse off than they are today. However, the means of being able to authenticate messages via the outlined approach brings additional benefits, preventing the possibility of spoofing messages and allowing data received via AIS to be reliably trusted. Nonetheless, it is acknowledged that phasing in the proposed solution is likely to be a slow process, both politically and technically.

The PKC approach proposed to authenticate AIS has the potential to authenticate other maritime communications, including VDES (Wimpenny et al., 2018) and future maritime 5G services. The higher bandwidths offered by these services suggest they might carry a wide variety of maritime data, all of which must be authenticated if it is to be safely used. Authenticating these services will be explored in future work.

References

Androjna, A., Perkovič, M., Pavic, I. and Mišković, J. (2021). AIS data vulnerability indicated by a spoofing case-study. *Applied Sciences*, **11**, 5015.

Barker, E. (2020). *Recommendation for Key Management*. Special Publication 800-57, Part 1 Revision 5. National Institute of Standards and Technology, Gaithersburg, MD.

BIMCO, *et al.* (2020) *The Guidelines on Cyber Security Onboard Ships*. Version 4.0. Available at: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Boyes, H., Isbell, R. and Luck, A. (2016). *Code of Practice: Cyber Security for Ports and Port Systems*. Institution of Engineering and Technology, London, UK. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf

ENISA. (2013). *Algorithms, Key Sizes and Parameters Report, Version 1.0*. European Union Agency for Network and Information Security.

Goudossis, A. and Katsikas, S. (2019). Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology* **24**, 410–423.

Goudossis, A. and Katsikas, S. (2020). Secure AIS with identity-based authentication and encryption. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* **14**(2), 287–298.

Hall, J., Lee, J., Benin, J., Armstrong, C. and Owen, H. (2015). IEEE 1609 Influenced Automatic Identification System (AIS). *IEEE 81st Vehicular Technology Conference (VTC Spring)*. Glasgow, UK.

IALA. (2019). *Guideline G1139: The Technical Specification of VDES*. 3rd Edition. Available at: https://www.iala-aism.org/product/g1139-technical-specification-vdes/

IEC. (2021). IEC 63154:2021. Maritime navigation and radiocommunication equipment and systems - Cybersecurity - General requirements, methods of testing and required test results. International Electrotechnical Commission.

IMO. (2016). MSC 96/4/1. Measures to Enhance Maritime Security.

IMO. (2017). Resolution MSC.428(98). Maritime Cyber Risk Management in Safety Management Systems.

International Telecommunication Union. (2014). Recommendation ITU-R M.1371-5. Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band.

https://doi.org/10.1017/S0373463321000837 Published online by Cambridge University Press

Kessler, G. (2020). Protected AIS: a demonstration of capability scheme to provide authentication and message integrity. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*. **14**(2), 279–286.

MCP. (2021). *Maritime Connectivity Platform*. https://maritimeconnectivity.net. Accessed 30 June 2021

Sciancalepore, S., Tedeschi, P., Aziz, A. and Pietro, R. (2021). Auth-AIS: secure, flexible, and backward-compatible authentication of vessels AIS broadcasts. *IEEE Transactions on Dependable and Secure Computing*. DOI:10.1109/TDSC.2021.3069428.

Stewart, A., Rice, E. and Safonov, P. (2018). Digital Authentication Strategies for the Automated Identification System. *Proceedings of the Midwest Instruction and Computing Symposium (MICS)*. 6–7 April 2018, Duluth, MN, USA.

Wimpenny, G., Šafář, J., Grant, A., Bransby, M. and Ward, N. (2017) Cyber-Security and a Potential Role for the Maritime Cloud. *ION GNSS+*. 25–29 September 2017, Portland, OR, USA,.

Wimpenny, G., Šafář, J., Grant, A., Bransby, M. and Ward, N. (2018). Public Key Authentication for AIS and the VHF Data Exchange System (VDES). *Proceedings of the 31st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2018)*. 24–28 September 2018, Miami, FL, USA.

Cite this article: Wimpenny G, Šafář J, Grant A, Bransby M (2022). Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility. *The Journal of Navigation* **75**: 2, 333–345. https://doi.org/10.1017/S0373463321000837