TRANSNAV
http://www.transnav.eu
the International Journal on Marine Navigation and Safety of Sea Transportation
Volume 14
Number 2
June 2020

DOI: 10.12716/1001.14.02.02

Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity

G.C. Kessler
Embry-Riddle Aeronautical University, Daytona Beach, Florida, USA

ABSTRACT: The Automatic Identification System (AIS) provides situational awareness for vessels at sea. AIS has a number of known security vulnerabilities that can lead to a several types of attacks on AIS, including the ability to create ghost vessels, false warning or meteorological messages, or bogus virtual aids-to-navigation (AtoN). A number of methods, with varying levels of complexity, have been proposed to better secure AIS and, indeed, emerging AIS protocols will implement some of these mechanisms. Nevertheless, little has been done to secure the current standards, which will remain in use for some time. This paper presents Protected AIS (pAIS), a demonstration of capability implementation using public-key cryptography methods to address several AIS security vulnerabilities, maintain backward compatibility, and be able to interoperate with non-pAIS devices.

1 INTRODUCTION

This paper discusses the Automatic Identification System (AIS), some of its security vulnerabilities, and a proof-of-concept software project called Protected AIS (pAIS) that addresses some of the identified vulnerabilities. Sections II and III of this paper provide a high-level overview of AIS and its security exposures, respectively. Section IV describes public key cryptography, the basis for the protections provided by pAIS. Sections V and VI, respectively, provide an overview and detailed example of the operation of pAIS. Section VII offers some of the limitations of pAIS as a solution and suggests further development, followed by Summary and Conclusions in Section VIII.

2 AIS OVERVIEW

AIS is a tracking system that allows vessels at sea to be aware of each other's presence (within 10-20 nautical miles or so), authorities to identify and monitor vessels in their area of responsibility, and ships and shore stations to exchange navigation, meteorological, safety, and other items of information. Following the oil spill caused when the oil tanker *Exxon Valdez* ran aground in Alaska in 1989, AIS was designed as a maritime situational awareness system in the 1990s and adopted internationally in the 2002 International Convention for the Safety of Life at Sea (SOLAS) [3,8].

Chapter V of the SOLAS agreement, titled "Safety of Navigation," mandates that ships of a certain size and/or function carry AIS transceivers as an additional safety measure; this same mandate is found in 33 CFR 164.46 in the United States Code of Federal Regulations. Vessels required to operate AIS are referred to as Class A and include ships of 300 or more gross tons traveling internationally, commercial power vessels of 65 or more feet (19.8 or more meters) in length, and power vessels certified to carry more than 150 passengers; warships are exempted from these requirements although all modern warships have AIS capability [9,20]. Class B refers to those vessels carrying AIS at the option of the captain or that do not have a requirement to carry Class A equipment. AIS devices generally transmit position information messages every 2-180 seconds, depending upon the ship's class, speed, and rate-of-turn [8].

AIS is used today primarily for situational awareness and collision avoidance, vessel traffic management, and coastal surveillance [3,8]. The system is designed so that a ship fitted with appropriate receivers can view the local traffic and quickly determine another ship's name, its International Maritime Organization (IMO) registration number, size (e.g., length, beam, and draft), position (latitude and longitude), course, bearing, destination, status (e.g., anchored, moored, underway under power or sail, etc.), and other information (Figures 1 and 2).

Figure 1. Basic AIS display and control unit provides a radar-like display of nearby targets. (Source: https://commons.wikimedia.org/wiki/File:Ais_dcu_bridge.jpg)[1]

AIS messages are broadcast on maritime very high frequency (VHF) channels 87B (161.975 MHz) and 88B (162.025 MHz). The United Nations' International Telecommunication Union, Radiocommunication sector (ITU-R) describes the radio transmission aspects of AIS, particularly frequency sharing and time slot reservation, in Recommendations M.585-7 and M.1371-5 [10,11]. All AIS transmitters are assigned a Maritime Mobile Service Identity (MMSI) which is their primary identifier.

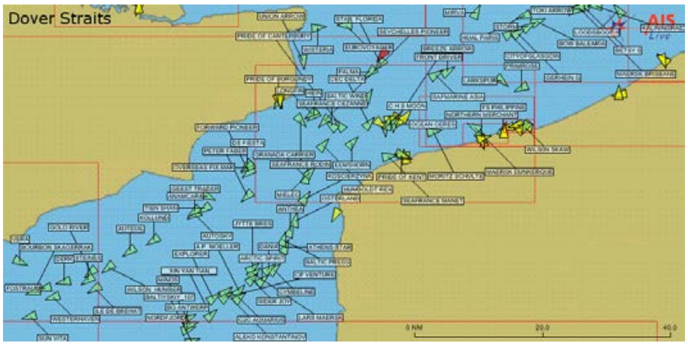


Figure 2. Chartplotter display including AIS data, showing ships in the local area (from https://upload.wikimedia.org/wikipedia/commons/d/d4/AIS_Manche_Est.png).

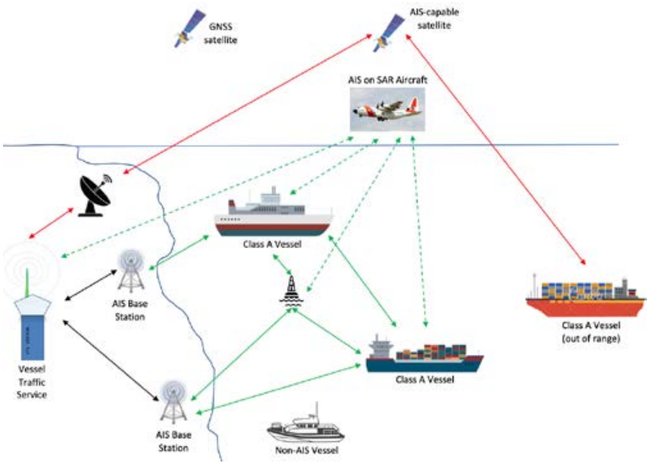


Figure 3. Stations in the AIS network.

The National Marine Electronics Association (NMEA) provides a family of standards describing electrical and serial communications for the interconnection of marine electronics. NMEA 0183 defines character-based AIS messages and low-speed communication over the Controller Area Network (CAN) serial bus [14]. NMEA 2000® describes a higher speed, binary-based AIS message scheme, also running over the CAN bus [15]. The emerging OneNet standard will describe a protocol of high speed, binary messages over the Internet Protocol (IP) and Ethernet; OneNet will also introduce security mechanisms for transmissions [16].

Ships and boats are not the only active components in the AIS network (Figure 3). Mobile stations within the AIS network also include AIS search-and-rescue transponders (AIS-SART), man overboard (MOB) AIS transmitters, Emergency Position Indicating Radio Beacons (EPIRB) AIS devices, AIS-equipped satellites, and AIS-equipped search-and-rescue aircraft. Fixed AIS stations include AIS base stations, repeaters, and specially equipped aids to navigation (AtoNs). Global Navigation Satellite Systems (GNSS) are not a direct component of AIS, but they provide essential geographic positioning information to all of the mobile components [8].

[1] Products or services mentioned in this paper are for informational or example purposes only and should not be construed as a recommendation or reference for such products or services.

3 CYBERSECURITY VULNERABILITIES IN AIS

AIS was designed during an era when security was not the imperative that it is today; indeed, it was designed during the very earliest days of the commercial Internet. Many researchers have discussed security vulnerabilities in AIS, including Balduzzi et al. [1,2], Goudossis and Katsikas [5], Kessler, Craiger, and Haass [13], and Trend Micro [18]. This section will review some of the AIS security issues, particularly those addressed by the pAIS software.

As stated above, AIS broadcasts message on public maritime VHF radio frequencies. Not only can any listener hear all of the traffic, but anyone can transmit messages. In years past, relatively expensive AIS hardware was required in order to transmit; today, there are many ways to build inexpensive systems to both receive and transmit AIS messages [12].

The use of a shared broadcast frequency for AIS is very efficient in terms of communications resource but foreshadows another potential AIS security vulnerability, namely, an attacker usurping the bandwidth in order to block other devices from transmitting, negatively impacting the shared time slot synchronization process, or changing slot reservation/assignment information. Any of these attacks can effectively knock other AIS stations off of the air.

Balduzzi et al. [1,2] originally described many types of attack on AIS due to some specific AIS protocol weaknesses, including:

- Lack of validity checks: AIS messages do not include any geographic validation information meaning that it is possible for a bad actor to send an AIS message from any location while purporting to be in another location.
- Lack of timing checks: AIS messages contain no time stamp verification information meaning that a cyberattacker can replay valid AIS information at a later time of their choosing.
- Lack of authentication: The AIS protocol provides no mechanism to authenticate the sender, thus anyone with the ability to craft or otherwise transmit an AIS packet can impersonate any other AIS device.
- Lack of integrity checks: AIS messages are transmitted in an unencrypted and unsigned form; this makes it simple for an interloper to intercept and/or modify transmissions.

From these vulnerabilities, a bad actor can spoof a non-existent vessel or AtoN, replay past AIS events, trigger false SOS or collision alerts, send bogus weather or other meteorological information, launch a denial-of-service attack on the AIS broadcast system, or modify vessel information being broadcast on the air. Examples of some of these scenarios are discussed below.

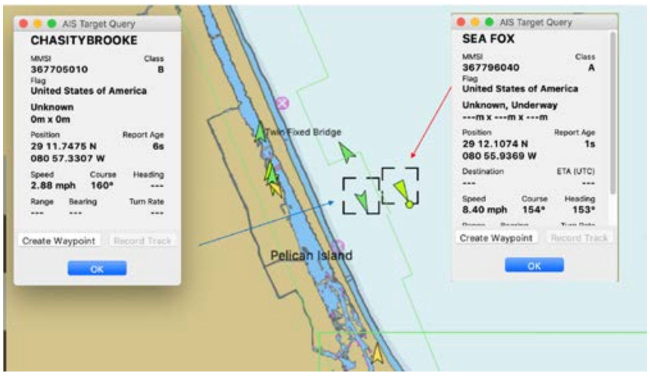


Figure 4. AIS display of real (e.g., Chastity Brooke) and ghost (e.g., Sea Fox) vessels off the coast of Daytona Beach, Florida.

Figure 5. AIS display of real and fake virtual AtoNs in Ponce De Leon Inlet, south of Daytona Beach, Florida.

Figure 4 shows AIS information for nine vessels off the coast of Daytona Beach, Florida, USA, displayed on OpenCPN chartplotter software. Details for each vessel can be found merely by clicking on the target. The Chastity Brooke is a real vessel, as are six of the other targets shown here. The Sea Fox and one other target are also real vessels but had been in the area six months earlier; their data was being replayed and interjected into the AIS data stream. A totally bogus vessel could also be injected into the system. It is impossible to tell from AIS alone which ships are real and which are "ghosts."

Figure 5 shows the detail of Ponce De Leon Inlet, south of the Daytona Beach area. Note the physical AtoNs and, in particular, the deep channel on the north edge of the inlet marked with red and green buoys. The north edge of the inlet is dredged and at least 36 ft (11 meters) deep, while the south side of the inlet can be as shallow as 4 ft (1 m). The chart shows the presence of four virtual AtoNs; the one labelled "Ponce 2nd Channel" is a preferred channel marker directing boaters to the south side of the inlet and the other three virtual AtoNs define a second "channel." These virtual AtoNs appear on the chart based upon spoofed AIS messages. The U.S. Coast Guard has sole authority in the U.S. for transmitting information about virtual AtoNs, but there is no mechanism with which to authenticate the sender of this information.

4 PUBLIC KEY CRYPTOGRAPHY

The primary security element of pAIS -- and, indeed, all methods that provide security to AIS transmissions -- is the use of cryptography. Protected AIS employs public-key cryptography (PKC) methods. The PKC concept was first described in 1976; the first implementation, in 1977, was the Rivest, Shamir, and Adleman (RSA) scheme, which remains the most common PKC algorithm in use [4].

Unlike secret key cryptography that uses a shared secret key for both encryption and decryption, PKC methods use two keys that have the following properties:

- The two keys are mathematically related and derived as a pair
- Knowledge of one key does not yield knowledge of the other key
- Either key can be used to encrypt data; the other key is then used to decrypt the data (for this reason, PKC is also referred to as asymmetric cryptography)

Because of the latter two properties, one of the keys is designated the private key and is kept as a closely held secret by the owner; the other key is designated the public key and can be widely distributed and shared [4].

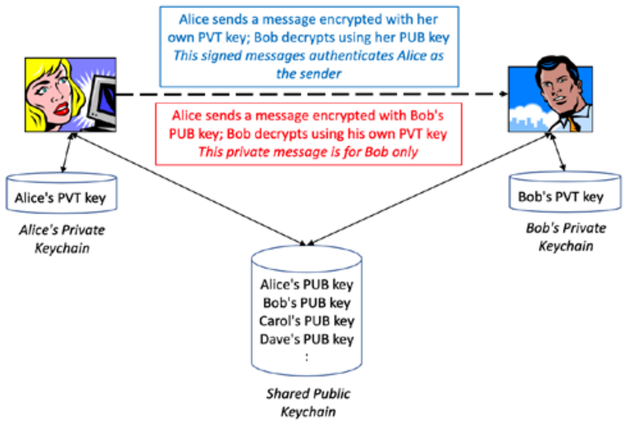


Figure 6. PKC model showing two communicating parties and their respective private key repositories, as well as a shared public key database. Alice authenticates messages by encrypting with her own private key and sends private messages to Bob by encrypting with his public key.

Figure 6 shows how PKC can be used for a variety of applications. In this scenario, the two communicating parties are Alice and Bob. Each has a private (PVT) key file that stores their private key locally (i.e., on their own device). They both also have access to a large number of public (PUB) keys through a shared database which could be on the Internet or corporate network, or could just be shared amongst all of the users. If Alice wishes to send a private message to Bob, she encrypts it with Bob's public key; only he possesses the private key so only he can decrypt the message. If Alice wants to authenticate a message that she sends -- i.e., prove that she is the sender -- she will encrypt the message with her own private key; this message can be read by anyone who can access her public key and successful decryption proves that she was the sender since only she possess her private key. It is the ability to authenticate the sender of AIS messages that makes PKC applicable to pAIS.

5 PROTECTED AIS OPERATIONAL OVERVIEW

A number of solutions to the security weaknesses of AIS have been proposed. Encrypted AIS [19] and other cryptography-based variants have seen use for special-purpose or limited fleets. Even when using a shared key, EAIS solves the problems described above by carefully introducing vessels into the "trusted" group. It has limited utility, however, for other vessels and the situational awareness of "public" maritime traffic.

Goudossis and Katsikas [5] provide an overview and critique of several other solutions to AIS security, including those proposed by Goudossis, Kostis, and Nikitakos [6], Hall, Lee, Benin, Armstrong, and Owen [7], and Oh, Seo, and Lee [17]. These solutions are encryption-based and address the issues mentioned above but require significant changes to the AIS protocol and/or add several layers of complexity to the communication network.

The pAIS project is a proof-of-concept effort to address security issues of AIS with a solution that is computationally simple, does not add a noticeable delay time in transmission, is backward compatible with existing protocols, could be implemented by a simple software upgrade, and would be able to communicate with the embedded base of equipment. While created independently, pAIS is essentially a realization of Mode 2 (authentication and integrity) security described by Goudossis and Katsikas [5] in their proposal for a Secure AIS protocol. Protected AIS is a mode of operation designed to address three specific security vulnerabilities:

- Lack of message integrity
- Lack of timing integrity
- Lack of sender authentication

These vulnerabilities are addressed as follows:

1. To provide message integrity, pAIS calculates an 8-bit checksum over the entire AIS message rather than merely the individual sentence fragments[2]. The message is a binary string composed of 6-bit bytes; the pAIS checksum is computed as a byte-by-byte exclusive OR (XOR) of the entire binary string (e.g., 7C).
2. To provide timing integrity, a timestamp string is prepared when the message is generated. The timestamp is a 14-character string composed of the year, month, day, hour, minute, and second of transmission (e.g., 20191014103714).
3. To provide sender authentication, the checksum and timestamp are combined to create a 16-character string, which is encrypted with the private key associated with the sending AIS device's MMSI. This creates the so-called protect string.

[2] An individual AIS transmission is called a *sentence*. Sentences are limited in size to approximately 360 bits. If a message is larger than 360 bits, it is split across multiple sentences. The NMEA AIS checksum provides bit error detection for each individual sentence but not the entire message.

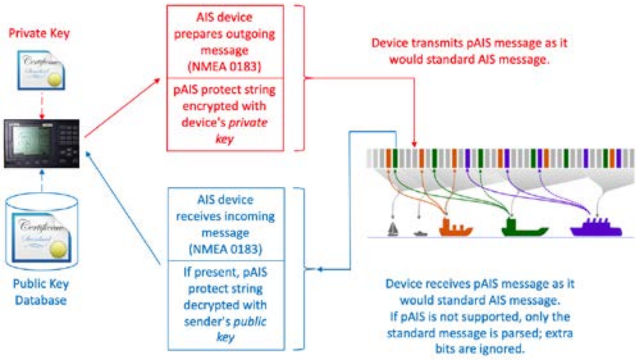


Figure 7. An AIS device in protect mode appends the pAIS protect string -- encrypted with its private key -- to its standard outgoing AIS transmission. A device receiving a pAIS message can ignore the protect string or decrypt it using the sender's public key.

Figure 7 shows the basic pAIS operation. An AIS transmitter operating in protect mode will generate a protect string, encrypted with its private key, for all outgoing transmissions. This string is appended to the standard AIS message to be transmitted. On the incoming side, AIS receivers "know" the standard length of AIS messages. If the incoming message exceeds the expected length and the receiver is not operating in protect mode, it merely ignores the extra bits; if the receiving station can operate in protect mode, it will decrypt the protect string using the private key associated with the sending station's MMSI.

Backward-compatibility is realized in this scheme because standard NMEA checksum and message processing procedures remain intact. The only difference with pAIS is that the binary string representing protected messages is longer than a standard message's binary string.

6 PROTECTED AIS SOFTWARE OVERVIEW

The prototype pAIS software is written in Perl and focuses on NMEA 0183 formatted messages. The software comprises a suite of programs that can be used to generate standard and protected AIS messages, as well as decode them.

Perl's Crypt::OpenSSL::RSA module is employed for generation of PKC public-private key pairs (Figure 8), encryption, and decryption. The pAIS software employs 256-bit RSA keys, generating a 258-bit protect string (which adds 25-350% overhead to standard AIS messages). This particular encryption module was selected because it offers the options of encrypting or decrypting with either the public or private key. While encrypting a message with the private key is logically similar to the message signature function in most encryption libraries, experiments with message signatures found that the shortest usable RSA key was 512 bits in length. This large key and the signature function produced a 540-bit protect string which was deemed too much overhead even for the prototype system.


```
-----BEGIN RSA PUBLIC KEY-----
MCgCIQDKTGvfR48HgnUqjZ+tGdi0jhtIt3mprfFkB4uWhmradQIDAQAB
-----END RSA PUBLIC KEY-----

-----BEGIN RSA PRIVATE KEY-----
MIGqAgEAAiEAykxr30ePB4J1Ko2frRnYtl4bSLd5qa3xZAeLloZq2nUCAwEAAQIh
AI6M/XKP9TzAdBmxRHRxAx8t/ENuiN7Gpjn2kz42C+M9AhEA+TRSsa0pwj2YLZ7W
L1Rz8wIRAM/QpuzHnqlb3QgloVtC2fcCEEKzG3MM2wFvRPzo54DxhLsCEFDlwJVb
//+dqyV9dpK4K3ECEGRqy+GxBwK1ndLz5Yr8HKw=
-----END RSA PRIVATE KEY-----
```


Figure 8. Sample RSA public/private key-pair that can be associated with a device's MMSI.

The following example shows how standard and protected AIS messages compare. This example uses a Type 1 (Position Report Class A) message with the following parameters:

- MMSI = 369121053
- Navigation status = Underway using engine
- Rate of turn = ~5° per minute to the port
- Latitude = 29.06°
- Longitude = -080.92°
- Speed = 17.2 knots
- Course over ground = 260°
- Heading = 272°
- UTC timestamp = 28 seconds

A standard NMEA 0183 message with this information would be transmitted over the air as:

```
!AIVDM,1,1,,A,15P1G7@uBdJ=Tv0@`=H::8Pp0000,0*08
```

Figure 9 shows the AIS sentence, the binary string representing the message payload, and the decoded message.

```
***** AIS Parser (Version: 3.2.8p, Build date: 10/13/2019) *****

AIS sentence(s) input from file type1_example.txt.

AIS sentence: !AIVDM,1,1,,A,15P1G7@uBdJ=Tv0@`=H::8Pp0000,0*08
 Talker ID: !AI - Mobile AIS station
 AIS Encapsulation Formatter: VDM - AIS VHF Data-Link Message
 Checksum verified
1 sentence(s) processed

Binary string: 0000010001011000000000001010111000111010000111101010010101100011010001101100100
1111100000000100001010000011010110000010100010100010001000001110000000000000000000000000000

--- Start of Transmission 1 ---

Message Type = 1 (Position Report Class A)
Repeat indicator = 0
Maritime Mobile Service Identity (MMSI) = 369121053
  ** This MMSI represents a ship.
  ** The Maritime Identification Digits (MID) are 369 -- United States of America
Navigation Status = 0 (Under way using engine)
Rate of Turn (ROTAIS) = -11 (-5.4°/min)
Speed over ground (SOG) = 17.2 kn
Position accuracy = 0 (Low, >10 m [default])
Longitude = 080.920000°W (080°55.20'W)
Latitude = 29.060000°N (29°03.60'N)
  ** Use this URL for a Google map of this position:
  ** http://www.google.com/maps/place/29.060000,-80.920000
Course over ground (COG) = 260.0°
True heading = 272°
Timestamp = 28 seconds
Maneuver indicator = 0 (Not available [default])
Spare = 0 (Unused; should be 0)
Receiver Autonomous Integrity Monitoring flag = 0 (RAIM not in use [default])
--- SOTDMA Communication State ---
Synchronization state = 0 (UTC direct)
Slot timeout = 0 slots remaining until slot change
Slot offset = 0

--- End of Transmission ---
```

Figure 9. Decoding a standard AIS Type 1 message.

In pAIS protected mode, the 258-bit protect string is appended to the standard data, generating the following two-sentence AIS message (the **bolded bits** represent the protect string):

!AIVDM,2,1,6,A,15P1G7@uBdJ=Tv0@`=H::8Pp0000**fk<m2;w3Dk4UmU4LV1m4Qr?s5=OS3vW3**,0*46

!AIVDM,2,2,6,A,**gwQ<d@MEKa**`,0*0B

When the message is read by a pAIS device using protect mode, the information is interpreted as shown in Figure 10:

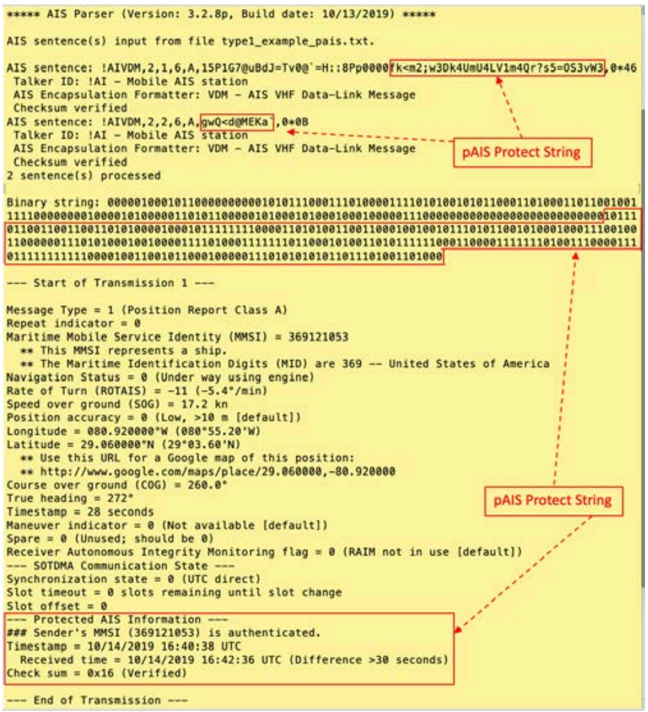
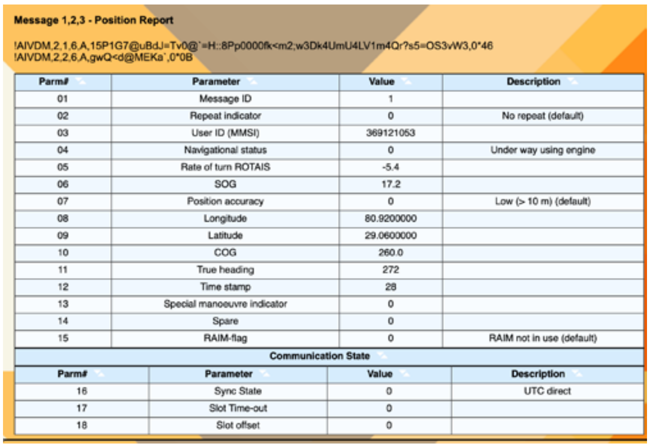


Figure 10. Parsing a Type 1 message with a pAIS protect string.

The pAIS message will also be decoded properly by well-behaving AIS devices and software unable to operate in protect mode because standard devices should ignore the unexpected data at the end of the transmission, as shown in Figure 11.


Message 1,2,3 - Position Report

!AIVDM,2,1,6,A,15P1G7@uBdJ=Tv0@`=H::8Pp0000fk<m2;w3Dk4UmU4LV1m4Qr?s5=OS3vW3,0*46
!AIVDM,2,2,6,A,gwQ<d@MEKa`,0*0B

Parm#	Parameter	Value	Description
01	Message ID	1	
02	Repeat indicator	0	No repeat (default)
03	User ID (MMSI)	369121053	
04	Navigational status	0	Under way using engine
05	Rate of turn ROTAIS	-5.4	
06	SOG	17.2	
07	Position accuracy	0	Low (> 10 m) (default)
08	Longitude	80.9200000	
09	Latitude	29.0600000	
10	COG	260.0	
11	True heading	272	
12	Time stamp	28	
13	Special manoeuvre indicator	0	
14	Spare	0	
15	RAIM-flag	0	RAIM not in use (default)
Communication State			
Parm#	Parameter	Value	Description
16	Sync State	0	UTC direct
17	Slot Time-out	0	
18	Slot offset	0	

Figure 11.Type 1 message with a pAIS protect string as interpreted by a non-pAIS decoder. (Site:https://www.maritec.co.za/aisvdmvdodecoding1.php)

7 LIMITATIONS AND AREAS FOR FURTHER DEVELOPMENT

The pAIS project was intended only as a demonstration of capability and, as such, is a prototype with operational limitations. The method described here does not use the strongest possible algorithms for some simple reasons; the intent of the prototype was to demonstrate simplicity, backward-compatibility, and ease of integration into existing software. Some of pAIS' limitations include:

- The use of byte-wise XOR is not the strongest checksum available, but it adds simplicity to the system by re-using code; the NMEA checksum algorithm is already part of AIS software. In addition, this checksum is sufficient for our needs; while an attacker might be able to brute-force a bogus message with the same checksum as a valid message, this is unlikely to be used in a real-time attack. In any case, a number of strong eight-bit cyclic redundancy check (CRC-8) algorithms could be employed without adding additional size to the protect string.
- The current timestamp uses a 14-character, human-readable string containing month, day, year, hour, minute, and second. This same information could be obtained using 10-byte Unix epoch time, which would shorten the amount of data to encrypt by four bytes. Upon testing, however, the length of the protect string remained at 258 bytes.
- A given timestamp might be duplicated if an AIS device transmits more than one message within a second or if two different AIS devices transmit a message within the same second. This timestamp duplication is not a problem because the timestamp is only intended to provide timing integrity on a per-message basis. Timestamp uniqueness is not a requirement since it is not tied to message identification.
- The RSA public/private key pair used in pAIS is 256 bits in length, significantly shorter than the best-practice key size of 2,048-4,096 bits. Upon experimentation, 256 was found to be the shortest key that could safely protect the 16-byte protection string. Choosing the shortest key length was a balance between security and overhead; this key size adds 43 six-bit characters to the length of a message which, as mentioned above, amounts to between 25-350% overhead. (The next smallest RSA key is 128 bits and was found to only protect a string up to five characters in length).

Protected AIS does not solve all of AIS' security problems. In particular, it does not counter an insider threat, when an authorized device already in the system is used to send bogus messages. Indeed, little can be done to protect against a bad actor who manually enters or otherwise configures bogus or incorrect information into an authenticated AIS device.

The pAIS scheme also provides no geographic validity checking because there is no way to "prove" the latitude and longitude of the transmitting device. Geographic validity checking would require an independent means of verification.

Every AIS device and AIS message has an MMSI associated with it so that public and private keys could be tied to the MMSI. The method described here does not specify how the public keys are distributed; for the pAIS prototype, the Pretty Good Privacy (PGP) model of shared keychains and a web of trust is used although that solution is not scalable to a world-wide network of tens of thousands of AIS devices. Goudossis and Katsikas [5] describe one mechanism based upon the creation of a global, X.509-like Maritime Public Key Infrastructure (PKI), where the registration and Certification Authorities would be managed and operated under the auspices of the

International Maritime Organization (IMO) and national maritime authorities.

Finally, pAIS was designed to work with NMEA 0183 formatted messages. Conceptually, there is no reason why it could not be extended to protect NMEA 2000 binary messages.

8 SUMMARY AND CONCLUSION

This paper has described pAIS, proof-of-concept software that adds bit integrity, timestamp integrity, and sender authentication to NMEA 0183 AIS messages. The scheme is designed to be simple, backward compatible, and able to co-exist with non-pAIS implementations.

This prototype software was developed for research applications to demonstrate that such a scheme was viable and feasible. AIS is increasing in importance as new applications get attached to the system; autonomous ocean-going and near-coastal vessels are merely the latest in a long line of mission-critical uses for AIS. Every new use of AIS adds to the reasons that the industry has to find ways to better secure the system.

Another lesson from this research had nothing to do with technology and everything to do with policy. Backward compatibility was an essential goal of the project so that introduction of protected AIS did not break a working network. But adding security as an additional layer to an existing system will ultimately do little good because bad actors will continue to operate in the non-secure mode and others will accept their messages. Without a strong policy that requires use of secure methods, add-on security will not achieve the goal of a secure AIS network.

REFERENCES

[1] Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A security evaluation of AIS automated identification system. In *Proceeding the 30th Annual Computer Security Applications Conference (ACSAC '14)*, pp. 436-445. New Orleans, Louisiana, December 8-12, 2014.

[2] Balduzzi, M., Wilhoit, K., & Pasta, A. (2014, December). A Security Evaluation of AIS. Trend Micro Research Paper. Retrieved from https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf

[3] Cutlip, K. (2017, March 31). AIS for Safety and Tracking: A Brief History. *Global Fishing Watch* Web site. Retrieved from https://globalfishingwatch.org/data/ais-for-safety-and-tracking-a-brief-history/

[4] Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. New York: John Wiley & Sons.

[5] Goudossis, A., & Katsikas, S.K. (2019, June). Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology*, *24*(2), 410-423. https://doi.org/10.1007/s00773-018-0561-3

[6] Goudossis, A., Kostis, T., & Nikitakos, N. (2012). Automatic identification system stated requirements for naval transponder security assurance. In A. Goudossis, T. Kostis, & N. Nikitakos (Eds.), Proceedings of the 2nd International Conference on Applications of Mathematics and Informatics in Military Sciences (AMIMS), Vari, Greece.

[7] Hall, J., Lee, J., Benin, J., Armstrong, C., & Owen, H. (2015). IEEE 1609 Influenced Automatic Identification System (AIS). In Proceedings of 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, May 11-14, 2015, pp. 1-5. https://doi.org/10.1109 /VTCSpring.2015.7145867

[8] International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA). (2016, June). An Overview of AIS (Edition 2). IALA Guideline 1082. Retrieved from https://www.navcen.uscg.gov/pdf/IALA_Guideline_1082_An_Overview_of_AIS.pdf

[9] International Maritime Organization (IMO). (2002, July 1). International Convention for the Safety of Life at Sea (SOLAS), Chapter V (Safety of Navigation), Regulation 19 (Carriage requirements for shipborne navigational systems and equipment). Retrieved from https://mcanet.mcga.gov.uk /public/c4/solas/index.html

[10] International Telecommunication Union (ITU). (2014, February). *Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band*. ITU-R Recommendation M.1371-5. M Series: Mobile, radiodetermination, amateur and related satellite services. Retrieved from https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1371-5-201402-I!!PDF-E.pdf

[11] International Telecommunication Union (ITU). (2015, March). *Assignment and use of identities in the maritime mobile service.* ITU-R Recommendation M.585-7. M Series: Mobile, radiodetermination, amateur and related satellite services. Retrieved from https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.585-7-201503-I!!PDF-E.pdf

[12] Kessler, G.C. (2019, October 14). AIS Research Using a Raspberry Pi. Retrieved from https://www.garykessler.net/library/ais_pi.html

[13] Kessler, G.C., Craiger, J.P., & Haass, J. (2018, September). A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation, 12(3), 429-437. https://doi.org/10.12716/1001.12.03.01

[14] National Marine Electronics Association (NMEA). (2019). NMEA 0183 Interface Standard. Retrieved from https://www.nmea.org/content/STANDARDS/NMEA_0183_Standard

[15] National Marine Electronics Association (NMEA). (2019). NMEA 2000® Interface Standard. Retrieved from https://www.nmea.org/content/STANDARDS/NMEA_2000

[16] National Marine Electronics Association (NMEA). (2019). OneNet Standard for IP Networking of Marine Electronic Devices. Retrieved from https://www.nmea.org/content/STANDARDS/OneNet

[17] Oh, S.H., Seo, D., & Lee, B. (2015). S3 (secure ship-to-ship) information sharing scheme using ship authentication in the e-navigation. International Journal of Security and its Applications, 9(2),97–110.

[18] Trend Micro Warns Of Vulnerabilities In Global Vessel Tracking Systems. (2017, February 3). *Firstpost* Web site. Retrieved from https://www.firstpost.com/business/biztech/business-tech/security/trend-micro-warns-of-vulnerabilities-in-global-vessel-tracking-systems-1895547.html

[19] U.S. Coast Guard (USCG). (2014, June 4). Encrypted Automatic Identification System (EAIS) Interface Design Description (IDD). Command, Control, and Communications Engineering Center (C3Cen).Retrieved from https://epic.org/foia/dhs/uscg/nais/EPIC-15-05-29-USCG-FOIA-20151030-Production-2.pdf

[20] U.S. Coast Guard (USCG). (2019, August 14). AIS Requirements. USCG Navigation Center Web site.

Retrieved from https://www.navcen.uscg.gov/?pageName= AISRequirementsRev