Digital Authentication Strategies for the Automated Identification System

Alexander Stewart, Erich Rice, and Paul Safonov
Masters Program in Information Assurance
Information Systems Department
St Cloud State University
St Cloud, MN 56303
apstewart@stcloudstate.edu

Abstract

The Automated Identification System (AIS) is an identity broadcasting system used worldwide on freshwater and saltwater ships of all sizes. It operates over Very High Frequency (VHF) radio channels and transmits a variety of information about the vessel and its activities such as position, speed and destination. The system has no built in security measures, which renders it open to a variety of attacks including spoofing, hijacking, and denial of service. Exploitation of these vulnerabilities can have significant consequences on the safety of ship operations. The majority of research on this topic has focused on using anomaly detection as a method to enhance the security of AIS. This paper investigates the threat posed by the vulnerabilities, and the possibility of using Public Key Infrastructure (PKI) as a method of authenticating messages to prevent spoofing, and it covers the challenges such an implementation would face.

1 Introduction

AIS is a widely used maritime communication technology that is little known outside the maritime community. Despite being used on ships of all sizes, and in many cases mandatory, it is vulnerable to a variety of attacks which could lead to an exploit of the system. The possible consequences for these exploits range from very minor to severe. This paper investigates options to provide digital authentication to reduce the possibility and effectiveness of spoofing messages. Options are considered with minimal modifications to the current system in mind; as the existing technology is so widespread, radical changes would greatly lower the chances of adoption.

2 Background

This section gives a brief introduction to the purpose and technical intricacies of AIS, as well as the vulnerabilities of the system and possible consequences of exploitation.

2.1 What is AIS

AIS is a maritime information broadcast system that is used for a variety of purposes. It was initially developed at the behest of the International Maritime Organization and mandated on "all ships of 300 gross tonnage and upwards engaged on international voyages and cargo ships of 500 gross tonnage and upwards not engaged on international voyages and passenger ships irrespective of size" in 2002 [1].

AIS broadcasts a variety of information over VHF channels to any transceiver in range. Primarily used for identifying geographical position (latitude and longitude), course, and speed, it can send any of 27 established messages which can contain other, more specific information. It is broadcast, and has no connection or receipt acknowledgement. There are several different types of entities using AIS including ships, shore stations, and both physical and virtual aids to navigation. Two VHF radio channels are reserved for AIS worldwide.

AIS uses several variants of Time Division Multiple Access (TDMA) to allow the broadcasting units to avoid interference. Given that a large number of AIS units move around, a rigidly organized broadcast scheme would not work. The primary scheme used for mobile units is Self-Organized (SOTDMA), which allows AIS transceivers to automatically adjust their transmission schedule around other units in the area [2]. Messages contain a data field to assist in organizing, and transceivers work based on the shared GPS time unit to avoid slots in use.

Figure 1 illustrates the uses of TDMA by different types of devices.

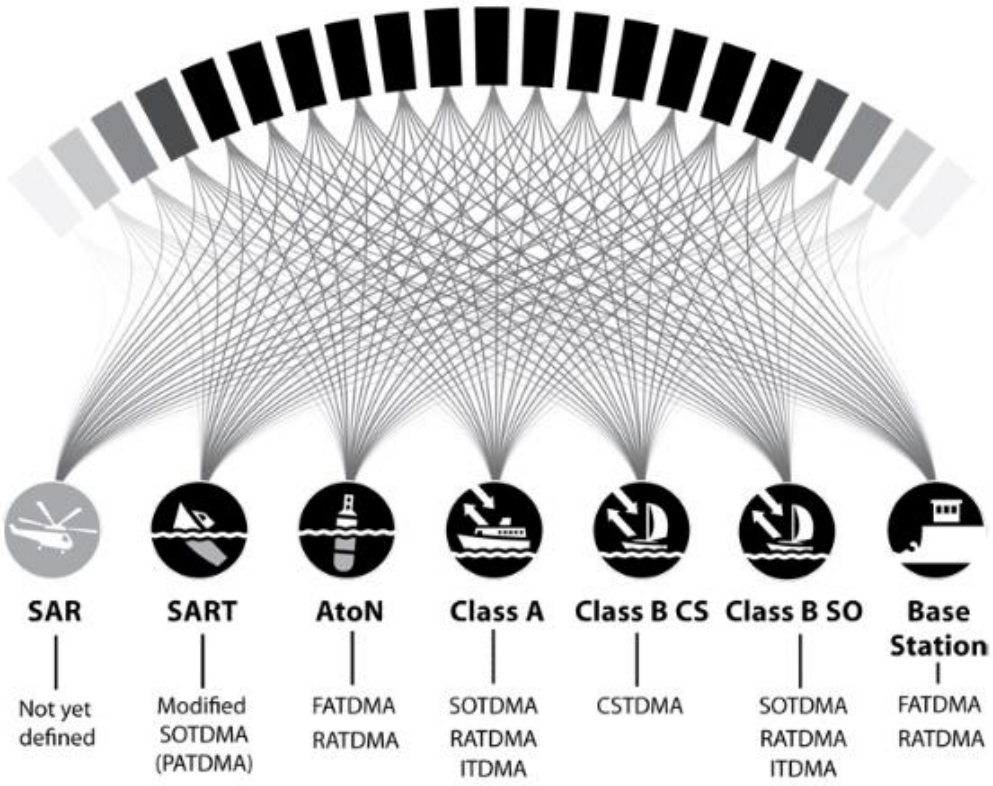

Fig. 1 TDMA Usage by Device Type [2]

ITU M.1371-5 [3] contains the detailed technical characteristics of AIS. Particularly relevant information includes the maximum duration and slot size, 26.667 ms and 256 bits respectively [3]. This translates into 2250 slots per minute for each channel. Despite the available space, messages contain a payload of less than 256 bits due to the necessary overhead involved in transmission.

Vessels are uniquely identified by a Maritime Mobile Service Identity, also known as an MMSI. The International Telecommunication Union created an identifier format in ITU-R M.585-7, as well as guidelines for its use and distribution. Each country has their own registry and method of generating and assigning new IDs, following the guidelines to ensure uniqueness.

2.2 AIS Vulnerabilities

The default AIS protocol is vulnerable to several exploitation techniques that can be split into three categories as defined by [4]; spoofing, hijacking, and denial of service. Even though the technology has been widely implemented since the early 2000's, [4] suspect they are "the first to conduct a security evaluation of AIS" (p. 25). As possibly the first structured security analysis of AIS, the authors start by analyzing the AIS protocol and

progress all the way to crafting and sending malicious AIS signals in a testing environment. This paper should, and does for this experiment, form a seminal work for the investigation of AIS vulnerabilities.

The consequences of AIS exploitation have a wide range of severity based on the attack vector exploited. Denial of service is fairly self-explanatory, but can be highly detrimental in areas of high traffic. Hijacking in this context could also be described as a man in the middle attack, either intercepting and modifying the AIS signals in software, or overriding VHF signals using a higher-powered transmitter.

AIS spoofing refers to the broadcasting of fake information. This can be done primarily in two methods; either falsely broadcasting one's own information or masquerading as a separate MMSI and broadcasting false information. Self-spoofing can be done to skirt international regulations and laws, such as regulated fishing zones. A vessel could spoof their own position outside the restricted zone, enabling them to illegally harvest while avoiding detection via AIS and also providing an alibi. Spoofing of another vessel's information could be done in an effort to lure vessels into unsafe waters or attempt to cause collisions.

3 Proposed Message Types

Given the proliferation of existing AIS units, a minimally invasive solution has a greater chance of being adopted in worthwhile numbers. With this in mind, certain options are effectively prohibited. Message Authentication Codes would not work because it relies on a shared secret key. Either one shared key is used for all units, which could be discovered and exploited, or a shared key pair system exists. A shared key pair would effectively make AIS a connection based protocol, as a broadcast would be useless to the majority of users that do not share the same secret key. Even if that obstacle is solved, the equation $\frac{n(n-1)}{2}$ which governs the number of needed secret key pairs would quickly eclipse the available SOTDMA slots.

A consideration for future work, as mentioned in [4] is that the open source X.509 public key certificate infrastructure could be used to provide digital authentication. The certificates found in the X.509 standard contain quite a bit of explanatory data, and would not fit within the message size guidelines found in [3]. Rather than attempt to adjust the X.509 certificates to fit, digital signatures using asymmetric encryption and hashing was also considered.

The options for implementing digital authentication proposed here involve creating a new message type, using one of the unused messages available. The protocol uses six bits for message id, and there are only 27 established messages. The authentication is provided using the classic technique of encrypting a hash digest using a private key. Authenticity is guaranteed if the decrypted hash matches with the generated hash of the received message, as only one sender has access to the private key that would allow such encryption.

3.1 Single Slot Message

Two different digital signature messages are proposed, allowing for the use of different hashing algorithms. The first type involves an authentication message that is sent after a regular message is transmitted. The fields of the authentication message are detailed in Table 1.

Parameter	Bits	Description
Message ID	6	Identifies message type (in this case, 28)
User ID	30	MMSI number of transmitter
Authentication data	128	Encrypted hash digest of message to be authenticated
Time Stamp	6	UTC second of transmission time
Communication State	19	Allows self-organizing of the TDMA system

Table 1: Proposed AIS Message Type 28

Upon receipt of the authentication message, the receiver would extract the encrypted hash digest, decrypt it using the public key corresponding to the sender's MMSI, and compare that value to a newly generated hash of the original message. Vessels MMSIs are unique, so each would only have one corresponding public key.

3.2 Multi-Slot Message

The limited size of a single slot AIS message greatly restricts the algorithms that can be used to generate the hash digest. Expanding to a multi-slot message allows for algorithms of greater size, as seen in the message fields in Table 2.

Parameter	Bits	Description
Message ID	6	Identifies message type (in this case, 29)
User ID	30	MMSI number of transmitter
Primary Message	Variable	Complete data from regular AIS message 1-27
Authentication data	Variable	Encrypted hash digest of Primary Message field
Time Stamp	6	UTC second of transmission time
Communication State	19	Allows self-organizing of the TDMA system

Table 2: Proposed AIS Message Type 29

To fit within existing ITU transmission guidelines, the Primary Message and Authentication Data field combined should not exceed 1003 bits. For spoofing prevention, the intended messages to authenticate include 1-4 and 21 which are the most common positioning messages. The maximum payload for message type 21, the largest, is 360 bits.

4 Challenges and Weaknesses

4.1 Single Slot Message

The single slot authentication message is the simplest, but also cryptographically the weakest.

The limited message size restricts the available hashing algorithms to sizes of around 128 bits. The MD5 algorithm is conveniently 128 bits, but has been proven insecure in a variety of ways [5]. Some of the characteristics of AIS may help to overcome those weaknesses. Even if an adversary can reliably generate a message that corresponds to a previously sent encrypted hash, the constant transmission means that an adversary would need to be able to create a very large number of exploits to effectively deceive someone. Table 3 contains the transmission schedule.

Ship's dynamic conditions	Nominal reporting interval
Ship at anchor or moored and not moving faster than 3 knots	3 min
Ship at anchor or moored and moving faster than 3 knots	10 s
Ship 0-14 knots	10 s
Ship 0-14 knots and changing course	3 1/3 s
Ship 14-23 knots	6 s
Ship 14-23 knots and changing course	2 s
Ship >23 knots	2 s
Ship >23 knots and changing course	2 s

Table 3: Class A shipborne mobile equipment reporting intervals [3]

This method also does not allow for an effective algorithm of matching the original message with the subsequently sent authentication data. A single slot does not allow enough space for message identifiers, and the included time field only contains the Coordinated Universal Time (UTC) second. One solution could be using a rotating buffer that keeps the most recently received message from a particular MMSI, and then applies the next authentication message from that MMSI to that saved message. If another non-authentication message is received, it replaces the one saved in the buffer. This would require extended memory allocation and management, which increases the complexity of the solution.

The simplicity of the single slot authentication message allows for transceivers without the authentication implemented to still function as normal. Any transceiver that is not coded to recognize message type 28 would simply disregard them, and continue to function as normal with the original, unauthenticated message. There would be no enhanced security, but also no loss of functionality.

4.2 Multi-Slot Message

The multi-slot message solves several of the concerns present for the single-slot message. With extra space comes the opportunity to accommodate a hashing algorithm of increased complexity and security, even up to SHA-512 with a message payload of appropriate size.

Where the multi-slot message proposed in Table 2 fails is simplicity. Any transceiver unable to process authentication messages would be unable to receive basic AIS data sent in this format.

Additionally, the extra total size provides much more specificity in matching messages. The format detailed in Table 2 includes the entire contents of the message, effectively creating one message with positioning and authentication data, but that field can be reduced to a style more like the single slot message and maintain separate positioning and authentication messages with a stronger identifying link between them.

4.3 Feasibility Challenges

Challenges faced by both single and multi-slot authentication messages are key management, distribution, and adoption. Each country already has an organization that handles the allocation of MMSIs, which could take on the task of key management.

Public key distribution could be handled by existing infrastructure with some modifications. There already exist methods of distributing important navigational information to concerned mariners that could be adapted to include public key information. Each country would be responsible for their own system, however, and not all may have the requisite infrastructure. An upside to this method is that for countries with a large number of ships, using existing regional distribution allows vessels to select relevant public key information. The chances of, for example, a harbor tug in the Great Lakes encountering a harbor tug from the Gulf of Mexico are almost nonexistent.

Private key distribution is a more difficult issue. The same distribution channels that exist do not have the security necessary to securely pass private keys. Likely, an entirely new distribution system would have to be implemented. Commercial AIS providers may be able to adjust their existing system for updates to accommodate private keys. Additionally, military and in some cases police and law enforcement may have existing secure channels that can accommodate private keys.

An altogether different challenge would be getting the public interested in adopting such a technology. AIS is widely distributed throughout the world, with hundreds of thousands of existing users. Transceivers can cost thousands of dollars, and are often integrated with other equipment such as charting displays. Cost would be a significant impeding factor in attempting to get any authentication technology accepted by the maritime community.

5 Conclusions

AIS is vulnerable to several types different attacks, and does have a very large user base. Despite this, there have been no known significant attacks on the system. While it is technically possible to implement some form of digital authentication to help combat the vulnerabilities, we think that the obstacles presented in this research are likely to prevent large scale support of the idea in the near future among the maritime community.

Further research working to identify possible security solutions for AIS could consider anomaly detection as an option, as is done in [6] and other papers, or the possibility of integrating digital signature authentication into an IMO sponsored update of AIS or a new generation of communication technology.

References

[1] International Maritime Organization, *International Convention for the Safety of Life At Sea, amended, Regulation 19.2.4*, Nov 1, 1974. [Online]. Available: http://solasv.mcga.gov.uk/Regulations/regulation19.htm#24. [Accessed: Mar. 14, 2018]

[2]All About AIS. *AIS TDMA Access schemes.* 2012 Available: http://www.allaboutais.com/jdownloads/Access%20schemes%20technical%20downloads/ais_tdma_access_schemes.pdf. [Accessed: Mar. 14, 2018]

[3] International Telecommunications Union, *Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band M.1371-5*. Feb 2014. Available: https://www.itu.int/rec/R-REC-M.1371-5-201402-I/en. [Accessed: Mar. 14, 2018]

[4] M. Balduzzi, K. Wilhoit, and A. Pasta. *A Security Evaluation of AIS*. ACSAC 30th Annual Computer Security Applications Conference Pages 436-445. doi 10.1145/2664243.2664257. Dec 2014.

[5] M. Stevens, *On Collisions for MD5*, Eindhoven University of Technology, 2007.

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