5-2018

Analysis Of Possible Authentication Strategies For The Automated Identification System

Alexander Stewart
St. Cloud State University, apstewart@stcloudstate.edu

Analysis of Possible Authentication Strategies for the Automated Identification System

by

Alexander Stewart

A Thesis

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in Information Assurance

May, 2018

Thesis Committee:
Paul Safonov, Chairperson
Jie Meichsner
Erich Rice

Abstract

Automatic Identification System, commonly known as AIS, is a maritime communication system that is used to keep track of positions and activities of ships. It is widely implemented all around the world, and mandated on vessels over a certain size according to the International Maritime Organization. It is a signal broadcast over radio frequencies that contains ship characteristics, position, speed, and other information. AIS is also being implemented in aids to navigation, supplementing and in some cases replacing traditional aids such as lighthouses and buoys. The protocol standard contains no security, leaving AIS vulnerable to spoofing, hijacking, and denial of service attacks. This paper explores the possible consequences of AIS exploitation, as well as options to mitigate risk. Digital signature authentication of AIS signals is examined with particular attention paid to the feasibility and challenges of wide scale implementation. Ultimately the potential benefits of digital signature authentication are considered to be outweighed by the challenges of implementation.

Table of Contents

Chapter Page

List of Tables

List of Figures

Chapter I: Introduction

Introduction

Automatic Identification System, commonly known as AIS, is a maritime communication system that is used to keep track of positions and activities of ships. Worldwide adoption of the technology is increasing every year, and it is being used to supplement or replace aids to navigation to reduce costs and increase service availability. It is used to great effect to enhance situational awareness and safety in high traffic areas and large ports in areas such as Singapore, Hong Kong, Los Angeles, and many others. AIS allows for a notable decrease in bridge to bridge telecommunications, keeping radio frequencies open for emergency use.

Research has shown that there are several types of attacks that AIS is vulnerable to, and with no inherent security measures, the technology is very vulnerable to exploitation. Anomaly detection strategies are heavily proposed and studied, but may not be appropriate for all cases. This paper is primarily concerned with authentication strategies that may be applied to AIS as well as adopting them to existing AIS infrastructure.

Problem Statement

Across the world, AIS is used as a navigational aide by hundreds of thousands of ships and that number is only increasing. The possible consequences of maritime accidents combined with the general ignorance of security risks and possible threats make this an issue of global significance, that can only grow more important as adoption increases and knowledge of the vulnerabilities spreads.

Nature and Significance of the Problem

Starting in 2002, the International Maritime Organization mandated that "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 shall be fitted with an automatic identification system" (IMO Reg 19.2.4). Adoption is growing even when not required, and agencies responsible for aids to navigation (ATON), such as buoys and lighthouses, are beginning to create virtual replacements for physical ATON to save on costs and increase usability. This means that hundreds of thousands of vessels are using AIS, which provides a very large attack surface to any malicious actor.

Objective of the Study

The objective of this study is to determine if there is an authentication method that could be applied to AIS with minimal adjustments to the protocol so that it could be implemented on existing systems.

Study Questions

Is digital signature based authentication able to be successfully applied to AIS? What must be altered to allow function with existing technology, or conversely, what characteristics or functionality of existing technology must be altered to allow authentication methods? Is message authentication a viable solution to the problems faced by AIS?

Limitations of the Study

This study is restricted to considering the problem of spoofing AIS signals, and how digital signatures would help address that problem. There are other AIS vulnerabilities not

thoroughly investigated. Additionally, this research is focused on a qualitative analysis of the issues involved, and does not rigorously investigate the variety of AIS transceivers.

Definition of Terms

AIS – Automatic Identification System

ATON – Aids to Navigation

TDMA –Time Division Multiple Access

IMO – International Maritime Organization

MMSI – Maritime Mobile Service Identity

Summary

AIS is a powerful technology, that is used throughout the world. There are no built in methods of authenticating a signal, so a malicious actor is able to generate and broadcast a signal that is almost impossible to identify. With a thorough understanding of the risks and technologies involved, solutions might possible that can help mitigate the inherent risks of the system. Digital authentication is one such method that may be able to alleviate the threat posed by spoofing of AIS signals.

Chapter II: Background and Review of Literature

Introduction

AIS is very familiar to mariners but hardly anyone else, so some thorough background on the workings of AIS is provided, covering the general use and also some key technical details. The primary body of work covering AIS vulnerabilities is explored to establish the existing vulnerabilities and consequences of exploitation. An in depth scenario detailing a potential AIS spoofing attack is presented using a location in southern Green Bay, part of Lake Michigan in the United States to help elaborate exploitation possibilities. There are many academic studies and papers regarding the use of anomaly detection and analysis to enhance AIS security, and fewer studies contemplating alternative methods.

Background Related to the Problem

An AIS transceiver is specially constructed to use radio signals over Very High Frequency (VFH) wavelengths. This unit transmits and receives AIS data to and from other vessels, with 27 possible messages defined in ITU 1371-4 (ITU). Standard transmissions include Maritime Mobile Service Identity (MMSI), geographic position in the form of latitude and longitude, navigation status, among others. While containing a GPS unit for clock corrections, it is most common for an external GPS receiver to be connected to the AIS unit to provide positional information. AIS units are frequently connected to electronic charting displays, which affords the navigator the ability to view location data in real time.

To illuminate the problems potentially caused by the inability to authenticate AIS, a hypothetical scenario involving the port of Green Bay in Lake Michigan was devised. First, some background information on ATON in the Great Lakes region must be provided. Due to the

extreme winter temperatures and risk of ice formation, many buoys are removed during the months of October, November, and December and returned to the water once the ice has receded, usually in April or May. The exact dates are published by the United States Coast Guard, in a publication called the Light List which provides the characteristics of aids to. Depending on the position of the buoy, some may be replaced with a less visible, more streamlined version which is better designed to function in the ice. If the regular buoys were to be left in the water during the winter, there is a high risk of damage and potential loss which would be very costly to replace.

Recently, AIS beacons have been created for some of the buoys present in the Great Lakes to enhance their usefulness during the winter months. The Green Bay Harbor Entrance Channel, a waterway quite familiar to the author, undergoes a significant change during the winter. There are 24 buoys in the waterway; prior to the winter 13 are replaced with ice capable buoys, 10 are removed completely, and one buoy is maintained year round as ice capable, neither removed nor replaced navigation (USCG Light List 2017). Three of the buoys that are removed, and two that are replaced also have an AIS beacon. Figure 2.1 shows the channel with all buoys in place, highlighted with circles.

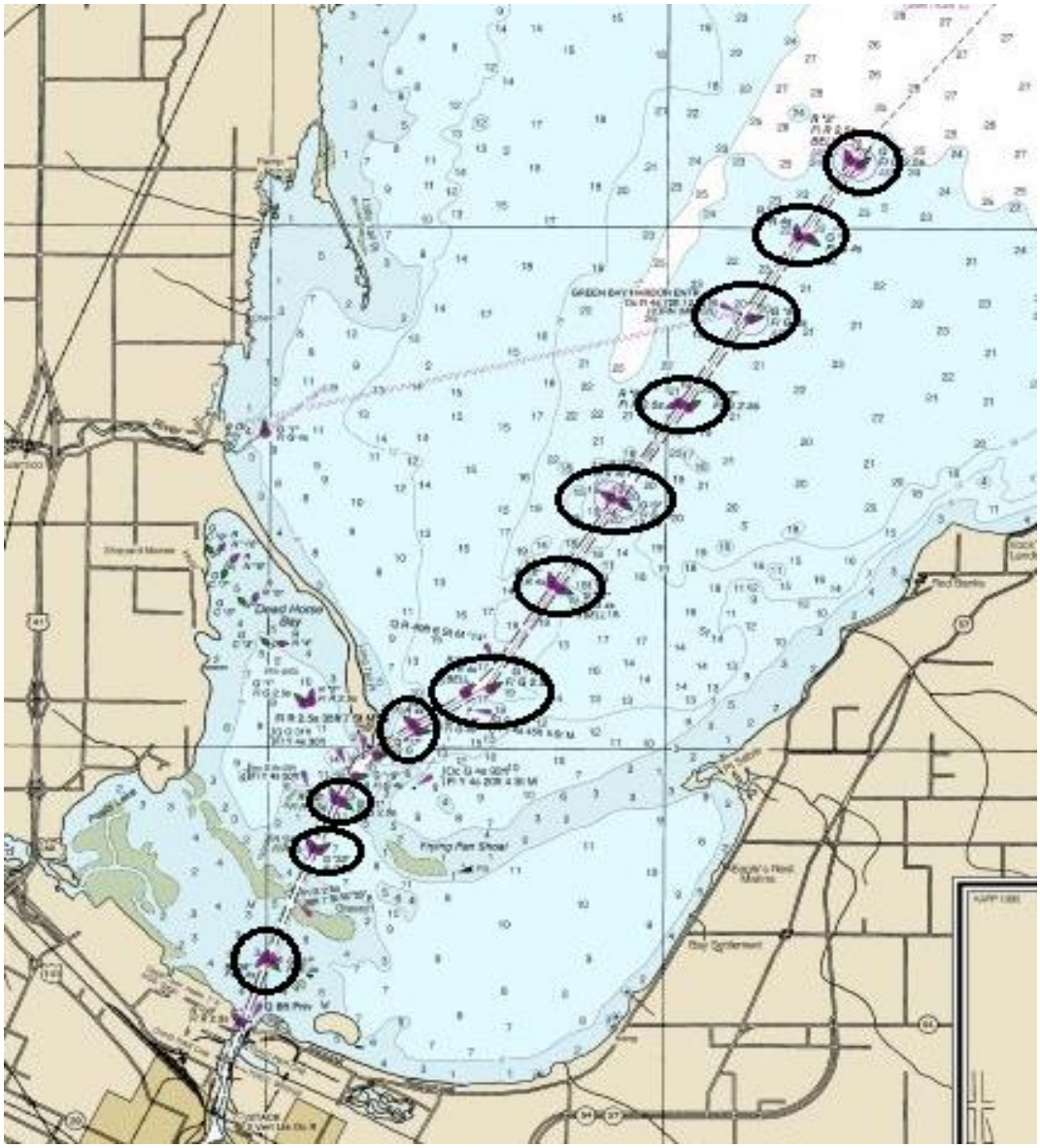

Figure 2.1: Green Bay Harbor Entrance Channel Summer Buoys (NOAA 2017)

Figure 2.2 shows the remaining physical buoys, after the winter replacements are made. The arrow denotes an area of particular significance, elaborated below. The outer approach to the harbor experiences a drastic reduction in available buoys, and the buoys that are present are significantly less visible.

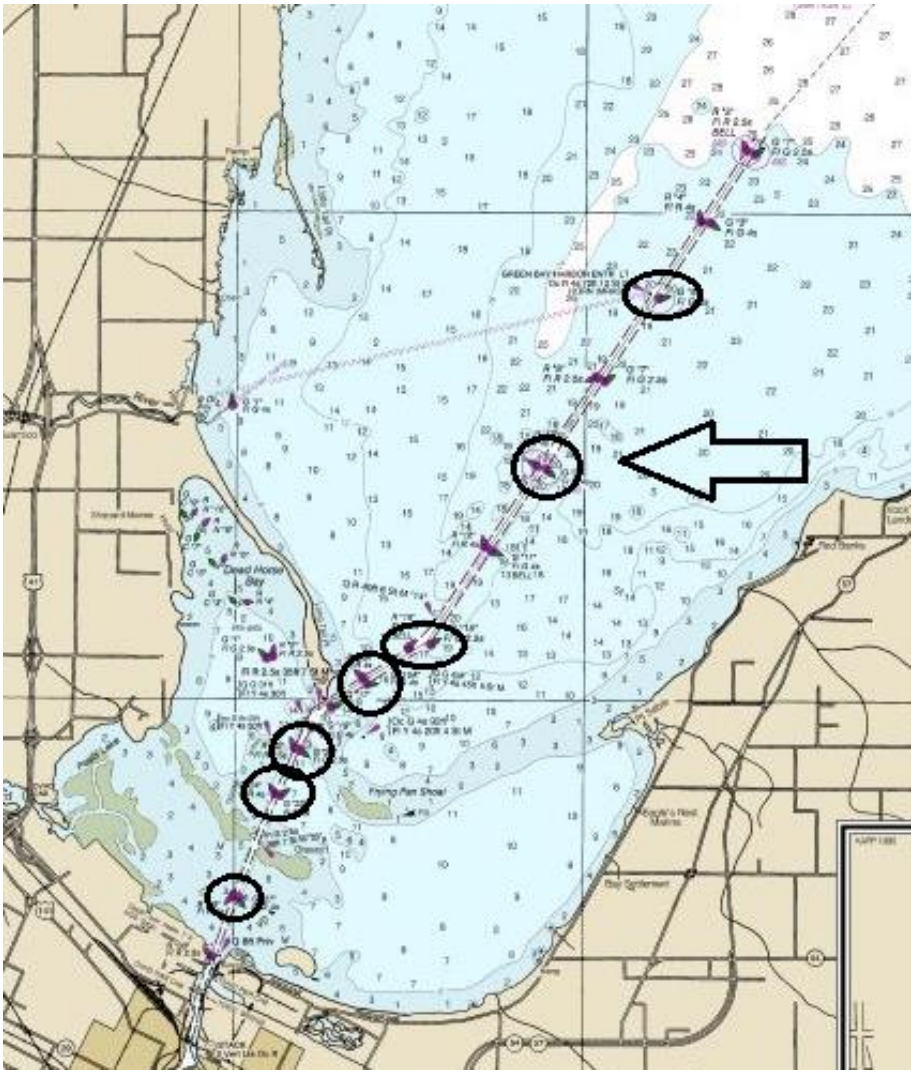

Figure 2.2: Green Bay Harbor Entrance Channel Winter Buoys (NOAA 2017)

The lay of the channel and the placement of the AIS beacons could potentially be exploited by a malicious actor. The depth of the channel that cargo ships follow into the port of Green Bay is at least 25 feet (NOAA 2017). Cargo ships on the Great Lakes have a tendency to fill to maximum capacity, so a ship planning to enter Green Bay will take on enough cargo that they require such a depth. Figure # 2.3 highlights the position of two buoys that are removed, replaced with less visible ice buoys, and have an accompanying AIS beacon.

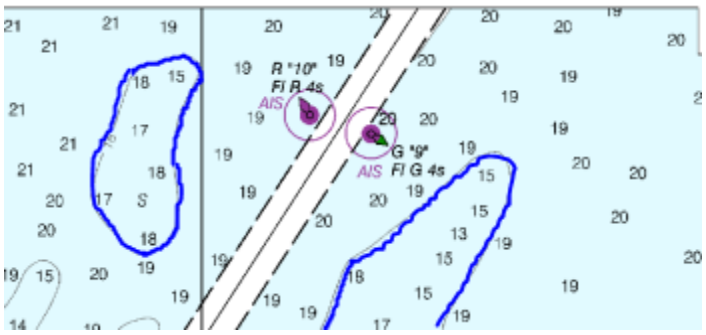

Figure 2.3: Green Bay Harbor Entrance Channel Buoys 9 + 10 Shoals (NOAA 2017)

Also noted in Figure 2.3 are two areas directly outside the channel where the water depth drops significantly. The highlighted area to the right side of the channel ranges in depth from 13 to 18 feet. If a malicious actor was to spoof the location of the two AIS beacons corresponding to the buoys in that location, it is possible that he could show their positions several hundred feet to either side of the channel. This would potentially lead a ship to the shallow water area, and cause them to run aground.

An experienced mariner would accurately judge this to be a highly unlikely scenario. Any cargo ship captain on the Great Lakes has years of training and experience, and there are many different aids to navigation not specifically mentioned designed to ease the transit of the Green Bay Harbor Entrance Channel. Furthermore, the nature of the lake bottom in that area is primarily mud and sand; even if a vessel were to strike bottom there, it is unlikely to cause serious harm.

The intention of this example is to show that, by spoofing only a few AIS signals, damage could be caused and traffic could be severely obstructed. The port of Green Bay does not experience high volumes of vessel traffic; the higher the traffic, the more likely the chance that a vessel ends up falling prey to AIS spoofing. An increase in traffic causes more distractions, and makes it more likely that an AIS signal will be trusted without verifying with

additional tools. In high traffic ports, it is much more likely to encounter vessels that do not frequently travel the area, and are thus unaccustomed to where AIS signals should be.

It is valuable to briefly cover two common attack scenarios that are relevant to digital authentication: replay attacks and collision resistant attacks. Collision resistant attacks involve a certificate authority, or some trusted third party that verifies the authenticity of a document or message. Used extensively in website certificates, it allows a consumer to verify that the website is trusted by a legitimate authority, and thus safe to use. When an attacker is involved in this scenario, the attacker can exploit the properties of hashing functions to pass off malicious information as legitimate. Any hash function vulnerable to a collision attack can be exploited in this manner. The attacker sends one innocuous message to the certificate authority, which reviews it and appends an authentication certificate. The value of the certificate is copied onto a second, malicious message which generates the same hash value as the first message. When the consumer checks the hash contained in the certificate against the message the values match, and the consumer is led to believe that the certificate authority authenticated the second, malicious message. For greater detail on the steps involved, consider Stallings or Gebhardt *et al.*

A replay attack is also well defined in Stallings. In brief, it involves a malicious actor recording a message from a legitimate source in full. At some later time, the malicious actor retransmits the message. The message may be accepted as legitimate by the receiver, depending on the security controls present. The easiest way to thwart replay attacks is to have strict time limits on messages; either a message is only valid for a defined period of time, or the message contains enough unalterable identifying information that a replay would be easily detectable.

Contained within ITU M.1371-5 are the technical characteristics of AIS. Particularly relevant information includes the maximum duration and slot size, 26.667 ms and 256 bits respectively (p. 16, ITU M.1371-5). 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.

AIS uses several variants of Time Division Multiple Access (TDMA) to allow the broadcasting units to avoid interference. Given that a large amount 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 as shown in Figure 2.4. Messages contain a data field to assist in organizing, and transceivers work based on the shared GPS time unit to avoid slots in use (All About AIS, 2012).

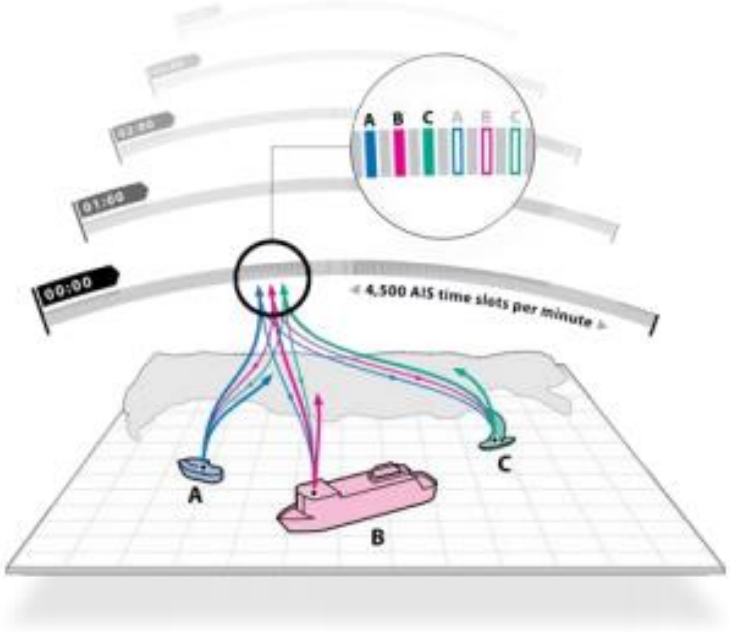

Figure 2.4: TDMA Slot Allocation (All About AIS, 2012)

Other TDMA variants are defined in Appendix A, as well as the message types that use those allocations. Stationary units do not need to organize around other transceivers, so are able to use set broadcast slots. The ability to autonomously dynamically organize multiple broadcasting units is key to the success of AIS. It keeps the transmissions relatively lightweight and successfully accommodates the mobile nature of ships.

Literature Related to the Problem

The default AIS protocol is vulnerable to several exploitation techniques that can be split into three categories defined by Balduzzi et al (2014); spoofing, hijacking, and denial of service. Even though the technology has been widely implemented since the early 2000's, Balduzzi et al (2014) suspect they are "the first to conduct a security evaluation of AIS" (p. 10). As possibly the first structured security analysis of AIS, they start from 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.

There is a body of work investigating AIS security issues, prompted in part by a recommendation from Balduzzi et al. that focuses on using anomaly detection techniques. The basic principle is to establish a baseline of normal behavior that new data can be compared against, which any malicious data being flagged as anomalous and can then be treated differently. Anomaly detection is a popular research area, and certainly has applications towards AIS security, but I argue it may not be the most appropriate solution for AIS spoofing.

The criteria necessary for determining anomaly may not be present, or present to the same degree, when considering ATON. One integrity assessment method proposed by Iphar et

al (2016) uses questions such as "'Is the speed consistent with the type of vessel' or 'Are the declared GNSS coordinates compatible with the existence of a navigable area'" (p. 3). The first question is useful for vessel traffic; it would easily detect the anomaly of a tugboat or barge travelling at 35 knots, but less useful for buoys. A buoy is chained to a sinker which is anchored in a specific geographic location. The amount of chain attached to the buoy has to accommodate for tides, winds, and other weather conditions, so there is some amount of slack for a buoy to move around the central point. Despite only moving within a certain area, it is possible for a buoy to have some speed, and also rapidly and unpredictably shift direction. There is certainly a limit to what speeds a buoy can expect to achieve, and Iphar et al's method would force a malicious actor to be very careful about spoofing a message, but not eliminate the possibility altogether.

Another method of anomaly detection proposed by Mazzarella et al (2017) focuses on vessels turning off AIS broadcasts when they engage in illegal activity. There is a large amount of activity that varies in legality based on position, such as fishing, dumping, transferring persons, or simply transiting. This method, while effective, only applies to vessels, and relies on a break in established AIS patterns.

There are several papers investigating the use of AIS in maritime domain awareness, such as those by Iphar et al (2015) and Wreski and Lavoie (2017). While not directly related to the topic of AIS security, these papers nonetheless enhance the importance of AIS security due to how integral AIS is to situational awareness of the maritime domain. Without trust in AIS, a large portion of the available information is no longer reliable and drastically impacts the ability of a nation or organization to grasp the operational picture of their waters.

AIS encryption exists in commercial forms today, provided by companies that manufacture maritime equipment such as Kongsberg and Saab (SAAB AB 2017). This symmetric encryption is intended for use by Navy, Coast Guard, or police forces; it allows a group of vessels, all with the same type of AIS transponder, to send AIS messages that can only be decrypted by other members of the group in possession of the encryption key. Depending on the transponder configuration, it is possible for the equipped vessel to send and receive unencrypted AIS messages as well, sometimes simultaneously.

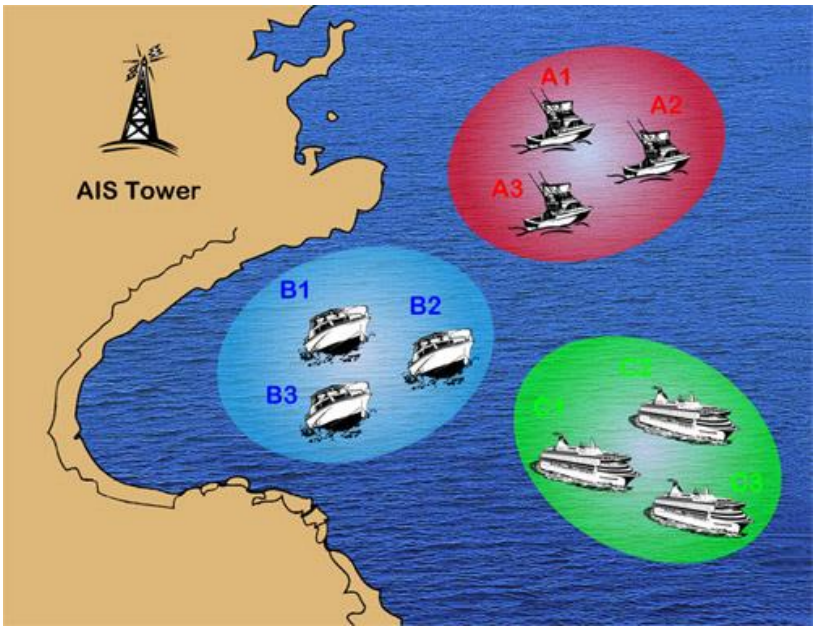

Figure 2.5: Alltek Marine Electronics Corp. AIS_Encryption (Alltek)

An example of where this type of encryption could be used is during police drug stakeouts; each vessel in the police fleet would want to be aware of each other's position for safety, but would not want the information to be public where it might be used by an adversary to avoid the stakeout. In Figure 2.5, this would be represented by group B having encrypted AIS units. When operating in encrypted mode, vessels in group A and C would not be able to see vessels in group B, but the vessels in group B can see each other and the other two groups.

These types of encryption, commonly known as blue force AIS or blue force tracking, have little value for authentication of AIS signals. It is limited to a select group of vessels, and relies on a specific configuration of equipment so it is not widely adaptable. Fundamentally, it focuses on confidentiality of the signal, not authentication.

Summary

The scientific and maritime communities are well aware of the problems facing AIS. Efforts have been made to analyze, define, and tackle the vulnerabilities, but given the immense scope of AIS implementation there are areas yet uncovered by significant research. Anomaly detection grabs the lion's share of the time, and certain commercial solutions do exist to enhance the security of AIS, but none directly address the issue of spoofing and the need for signal authentication.

Chapter III: Methodology

Introduction

This chapter contains an outline of what information is going to be investigated and how it will be integrated into the study, as well as an outline of what the software development hopes to achieve.

Design of the Study

This research is intended to evaluate the feasibility and demonstrate a proof of concept example of implementing digital authentication to enhance the security of AIS signals. It is primarily qualitative in nature; live signals were not studied. Given the nature of the research questions at play, it is more reasonable to determine the feasibility prior to extensive work on developing a technical solution.

First, research was done into the technical foundations of AIS and the varying methods of digital authentication to examine the possibility of combining the two. Once a thorough understanding of the technical challenges was achieved, several authentication methods were conceived of. The feasibility and advantages of each method were analyzed.

Data Collection

Real time data was not collected for this project, as it is focused on proof of concept evaluation and execution of digital authentication. Research information was collected from a variety of sources, primarily government and technical standards.

Tools and Techniques

Essentially, the envisioned system is an additional software layer that would process authentication messages in line between the radio receiver and the AIS processing. If an AIS

message is authenticated, then the software layer returns a verified signal. If the message is not authenticated, the software layer returns an unverified signal. Future settings could be customized regarding what the display software does with verified and unverified signals. If someone without this software layer encounters an AIS authentication message, it is dropped and ignored. Python was used to develop this proof of concept software application. Python was chosen primarily due to the robust supported libraries and ease of syntax. Existing Python libraries related to cryptography such as *pycrpto* were used.

Due to its nature as an interpreted language instead of compiled, the performance specifications of the program were not thoroughly evaluated. More importance is placed on the demonstration of proof of workability; given that the results may not be feasible to apply in a large scale implementation, it is premature to be concerned with program optimization.

Summary

The research and work conducted in this study focused on acquiring the requisite knowledge about AIS and authentication to propose possible solutions. Each solution was evaluated for technical, as well as practical, feasibility.

Chapter IV: Data Presentation and Analysis

Introduction

In this chapter, all the gathered information covering the technical framework of AIS signals and how digital authentication might interact with it is presented. New AIS message formats for authentication are proposed, and evaluated for security and feasibility. The problem of key distribution is addressed.

Data Presentation

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 use and distribution. Each country is to follow the guidelines to establish their own registry of vessels so as to avoid duplication. The nine digit MMSI should not be used in the generation of key pairs, as they are publicly known, but could prove useful in administering and listing public keys. In the United States, there are two organizations that allocate MMSI numbers. The Federal Communication Commission allocates MMSIs for private and commercial use, while the National Telecommunications Administration handles federal use.

A message authentication code (MAC) is a method of authentication between two parties that share a secret key. While MACs are an efficient method of authentication for end to end communications in some circumstances, there are several reasons that they are not appropriate for the problem of securing AIS communications.

It would be impossible to rely on unique secret key pairs for each possible combination of AIS units. Given the hundreds of thousands of vessels equipped with AIS, the number of possible key pairs would be astronomical. Even if they were limited to common operating areas,

some ships would still have an immense amount of possible pairs. Furthermore, AIS is broadcast, not connection-based. The added complexity and time needed to detect other ships, identify them, exchange keys and then initiate a communication based on the secret key would remove the benefit of AIS. The SOTDMA transmission method is not equipped to handle large amounts of traffic in that manner; instead of five ships broadcasting in turn, taking up five message slots, each ship would send to each other ship and take up 10 message slots. This would expand following the equation $\frac{n(n-1)}{2}$ where *n* is equal to the total number of AIS entities within communication distance. Any more than 68 AIS entities would overload the available channels. Considering the crowded nature of busy ports and the range at which some shore based installations can broadcast, this would be easily achievable.

Just as multiple shared secret keys causes a problem, so too would the reuse of a secret key. It would have to be included in some manner on the transceiver, as the operational environments of AIS preclude constant access to the internet. In the event that a MAC is used, the secret key for a particular AIS capable ship or beacon would be available to anyone with a transceiver as they need the information to decode and authenticate the message. With this knowledge, which is necessary for successfully authenticating received messages, a malicious actor could forge messages using the key which would appear genuine. The secret key could be concealed in a variety of ways to make it difficult to access, but ultimately, unlimited physical access to the device and its contents will eventually reveal the secret key, at which point the authentication system is compromised.

MD5 was chosen as the proof of concept hashing algorithm due to several considerations. The size of the hash created (128 bits) is able to fit within a single message of the SOTDMA

transmission scheme, which helps reduce the possibility of dropped packets. This also eliminates the need for receipt acknowledgement, which would be very challenging to implement given the broadcast connectionless nature of AIS. It would certainly be possible to create a system that reconstructs an authentication message sent over several packets, but there would be no way to request retransmission of corrupted or missing packets.

Prior to choosing MD5 for the single slot hash, a time trial was run in Python on the various hashing algorithms found in the pycrypto library. Given the AIS slot duration of 26.667 ms, an algorithm that takes significant time to execute would possibly interfere with the SOTDMA schedule. MD5 and the SHA family were selected, and tested by executing the function on a single slot AIS message. 10,000 trials were conducted using the script in Appendix B on Ubuntu 16.04, and the minimum time for each algorithm contained in Table 4.1.

Table 4.1: Hash Algorithm Time Data

Algorithm	Minimum time interval to hash one AIS sentence over 10,000 trials
MD5	9.53674316406e-7
SHA1	9.53674316406e-7
SHA224	9.53674316406e-7
SHA256	9.53674316406e-7
SHA384	9.53674316406e-7
SHA512	9.53674316406e-7

As is evident from the table, all the values are the same. What this shows is that there is no significant difference in the performance of the algorithms, and all of them are short enough to pose no problem to the regular AIS slot size. The reason the minimum value is chosen is due to the particularities of the Python *timeit* library used. Taking the arithmetic mean of the trials

would include interference from other CPU processes, and not accurately represent the execution time of the function itself.

Also contained in Appendix B is a basic format guide for how an authenticated AIS message could be generated.

Despite being suggested by Balduzzi *et al*, the X.509 open source standard is not considered in this study as a means of digital authentication. This is primarily due to the size of certificates created following that standard. With the goal in mind of minimal adjustments to the existing process of AIS, the X.509 certificates would exceed the guidelines published by the ITU which state that "if the length of the data requires a transmission using FATDMA reserved slots exceeding five (5) slots [...] or, for a mobile AIS station, if the total number of RATDMA transmissions of Messages 6, 8, 12, 14 and 25 in this frame exceeds 20 slots the AIS should not transmit the data" (p 60, ITU M.1371-5). There may certainly be validity in using the X.509 PKI standard, but it does not fit the minimally invasive focus of this research.

Data Analysis

The vulnerability of MD5 as compared to the SHA family or other hashing algorithms may in part be mitigated by the structure of the messages sent for AIS. Any attacker attempting to exploit hash collision or preimage attacks would run in to two major problems. As a result of AIS functioning as a continuous broadcast of information with constant, minor changes, a large number of exploits would need to be gathered, to consistently deceive a user for long enough to achieve some malicious purpose. One flawless hash collision would only deceive a user for as long as it takes for the next AIS message to be received. Transmission rates vary based on the message type, but are typically 10 seconds or less for most operating conditions (see Appendix

C). Additionally, those exploits would have to be realistic enough to deceive a user, which requires specific values that an attacker cannot control. To deceive a user operating in a channel or harbor, the geographic positions have to be consistent and possible, which covers a very small subset of the possible values for the latitude and longitude fields.

AIS is particularly vulnerable to replay attacks, but not all that susceptible to collision resistant attacks focused on the birthday paradox. There is no three-party transaction that an attacker could exploit, as the authenticator is also the creator of one of the messages. While an attacker could find two AIS messages that produce the same hash value, they would not have access to the generating station's private key to encrypt them.

Replay attacks take advantage of the absence of precise time indicators found within default AIS messages. With only six bits devoted to sending the UTC second of transmission, messages are not limited and could hypothetically be sent whenever the UTC second matches.

An attacker could generate a message with a hash value that matches a previously sent legitimate message (known as a pre-image attack), and then append the previously sent encrypted hash value to the new message. The decrypted hash matches the generated hash of the message, so the transmission appears legitimate. Several issues exist that would prevent or inhibit an attacker from exploiting this, however. If the legitimate broadcaster is continuing to send messages, then the SOTDMA controls would place time constraints on the attacker to protect the malicious messages from interference on the radio channels. When combined with the speed at which messages are broadcast, this means the attacker would need a ludicrous number of messages to effectively deceive anyone. While this is likely possible, given enough time and expertise, the barrier will prevent most from even making the attempt.

If an attacker is able to exploit cryptographic hashes by creating a message that matches a previously sent hash value in an attempt to deceive a legitimate user, the content of the information can easily be identified as anomalous, if not fraudulent. Fields such as Course, Heading, Longitude, and Latitude may be radically different if bits are altered from the true nature of the contact. Even if the encrypted hash value matches the message, the message itself will be nonsensical. Despite the cryptographic assurances that the message is legitimate, it will be noticed as anomalous by any competent mariner, who will reject it for inaccuracy even without knowing that the security has been compromised.

To demonstrate the potential effects changing one bit has on position, consider an arbitrary point in Lake Superior, Latitude 46.765106 and Longitude -92.026352, shown below in Figure 4.6. This point is roughly 3.25 miles (5.2 kilometers) from the harbor entrance, and approximately 2.25 miles (3.6 km) from the closest point of land. Converted to their binary equivalents, those coordinates are 110101100001001011011000 and 110100101010000110110000011.

Figure 4.6: Position outside Duluth Harbor

Obviously a change of a single bit has varying effects, based on how significant the bit is. Changing the least significant bit (LSB) would be very difficult to detect, while changing the most significant bit (MSB) would be immediately and glaringly obvious. For instance, a change of the 9th LSB only results in a difference of approximately 100 feet. While not a huge value, consider the close quarters in which some malicious spoofing might take place; 100 feet could still be detected. As more significant bits change, the difference grows significantly more pronounced. Changing only the 10th LSB shows a difference of approximately 210 feet, while the 11th will provide a difference of 425 feet. Shown in Figure 4.7 below, changing the 16th LSB provides a distance difference of almost 2.6 miles (4.2 km). The original position is highlighted with the red marker, and the new position is to the right.

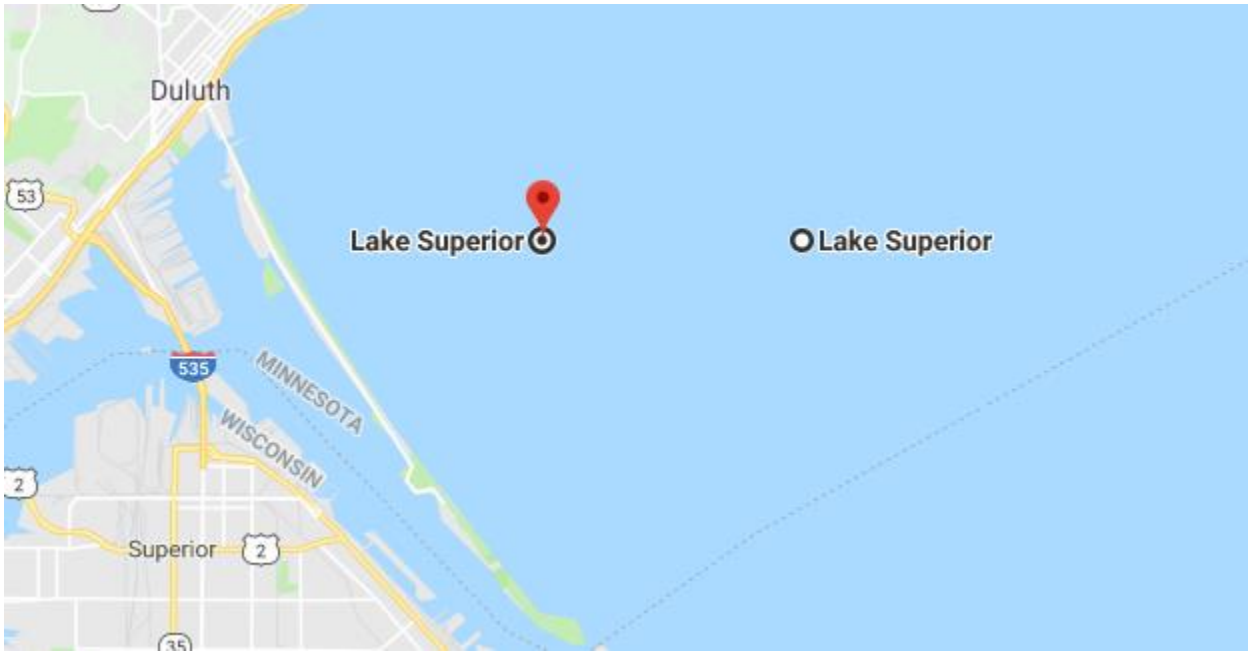

Figure 4.7: Change of 16th LSB

As such, any change to more than 50% of the bits of the 30 bit longitude field results in a significant difference of several hundred feet or more. Latitude values would be affected in a similar manner. This greatly restricts the ability of an attacker to generate an arbitrary message that matches a hash.

There are two possible formats for AIS authentication messages considered here, with some variations. The first is an independent authentication message, which creates a new standard in an unused message id. There are several variations within this idea. Both would require a new message type be created using one of the unused message ids, and both would require some method of storing an AIS message temporarily while waiting for the authentication message to arrive.

Option one would be to occupy only a single slot, shown in Table 4.2, which would limit the size of the hashing algorithm due to the maximum slot size of 256 bits. A distinct problem

caused by this approach is that there is limited space to include a message reference to ensure that the authentication is compared to the correct original message. The Time Stamp and Communication state field are used for error detection and correction, as well as coordinating slot allocation so that message are not simultaneously broadcast.

Table 4.2: Proposed AIS Message Type 28

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

This does not leave much space for any kind of identifier. One solution might be to implement a message buffer in the software layer on the receiving end. A received message from a particular MMSI would be stored, and the next authentication message from that MMSI be compared against the stored regular message. Receiving a new regular message replaces the buffered message. Overall, this method would allow for the use of single message slots, but be prone to inaccuracy by being unable to accurately match up authentication messages with the messages to be authenticated. The security concerns posed by shorter hashing algorithms also reduce the attractiveness of this solution. This is the method most susceptible to replay attacks, due to the limited space available.

Another option for creating a new independent authentication message would be to use multiple slots. This delays the authentication process compared to a single slot message, as the message must be received in full and reconstructed. On the positive side, this allows for a much longer, more secure hashing algorithm to be used. The standard message size for a five slot

message such as message types 12-14 is 1008 bits, which could easily accommodate hash functions with outputs of 512 bits or more such as SHA3-512 or WHIRLPOOL. This greatly increases security over the proven vulnerabilities found in shorter length hash functions. Additionally, the extended payload size allows for highly accurate message correlation. A three slot message, with a maximum size of 768 bits, could fit a 512 bit hash, 30 bit MMSI, 6 bit message ID, and still have 220 bits to accommodate time, positon, or other specific data that would identify the message to be authenticated. Depending on the size of the message to be authenticated, it would be possible to repeat the message in its entirety, in addition to including an encrypted hash value, which leads to the second type of authentication message.

Table 4.3: Proposed AIS Message Type 29

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

The second type of considered authentication message would be a multi-slot message consisting of the original message as well as the authentication content, shown in Table 4.3. Reconstructed into a single NMEA sentence, this would eliminate several problems. There would be no receipt delay between receiving a standard message and the authentication message. There would be a small verification delay, but that would also be present for standalone authentication messages. There would be no need to store standard messages while waiting for authentication messages. Using multiple slots allows for larger hash algorithms as well, though

possibly limited by the combination with an existing message. Adding a 512 bit hash would require at least two slots added to any current message length.

Option two is the clear winner as far as cryptographic strength is concerned. Unfortunately, that is not all that must be considered. Option two also requires the most alteration of existing systems to function. A system not set up to recognize authentication would have the following problems. If existing message types are used, the system would not be able to handle the abnormal sizes. If new message types are created, such as using message type 28 (currently unused) to represent an authenticated message of type 1, the non-authenticating system would not be able to interpret the undefined message. Considering both possibilities of option one, any non-authenticating system would be able to discard what appear to the system to be anomalous messages and process the regular AIS traffic. There is no enhanced security, but also no loss of existing functionality.

There are many intricacies to be considered when addressing the problem of key distribution for any asymmetric authentication method in AIS. The specific areas include initial private and public key distribution for existing units, new generation of private/public key pairs for future units, and updating known public keys and compromised private keys post initial distribution. This paper is concerned primarily with the administrative environment of the United States, with which the author is most familiar. General concepts should translate to most other countries, while the names of organizations and specific details will not.

Initial distribution of public keys is, for the most part, an already solved problem. Some AIS units are able to connect to a web interface for software and firmware updates (Kongsberg 2015) from which it would be trivial to also update a list of public keys when one is changed or

added. This would require that commercial companies invest the time and server resources to distribute public keys; if there is little to no interest from civilian companies, and it is deemed important enough, the US Coast Guard could create a public key server and administer it in addition to their regular maritime management duties. As the Coast Guard is responsible for domestic maritime security in the United States, this is a natural extension of their function.

For AIS units without the ability to directly access an update server, the existing framework of Notice to Mariners (NTM) can be used to distribute public key information. NTMs are publicly distributed updates which contain important maritime navigational information. In addition to containing a link to an online repository of public keys, the NTMs could also list which keys have been updated for which regions. From this resource, a consumer could copy the updated list of public keys to external storage and transfer to the AIS device.

The Coast Guard has an existing distribution system for NTMs, so this would require little change to include distribution of public keys. NTMs are further split into Local NTMs, distributed regionally according to the Coast Guard Districts shown in Figure 4.8. This has the added advantage of allowing a vessel to select those updates that are most relevant to them: a vessel operating solely in the Great Lakes does not need public key information from Hawaii.

Figure 4.8: Coast Guard Districts (USCG NAVCEN, 2018)

Obviously with public keys being public information, there is no concern about encrypting their distribution. Normal care must be taken to ensure that they are not altered or otherwise interfered with, but they are intended to be publicly available. Not so with private keys, which pose a far more challenging problem for AIS.

One portion of the private key distribution is also easily solved. Coast Guard, Navy, and other government vessels already possess secure communications channels for the distribution of classified information. Given that the keys will be distributed to private, commercial entities, they do not fall under the stricter requirements of securing classified information. Therefore, the existing government and military channels will more than satisfactorily protect the distribution.

However, this only works to distribute private keys to government vessels and federal ATON. There is no similar existing distribution network that can be directly adapted for commercial and private vessels. Each manufacturer of AIS devices has their own way to publish

updates, which may possibly be used in the distribution of private keys. That would likely require heavy adaptation of the existing methods. The requirement to keep private keys individually secure necessitates different methods than what is essentially a broadcast of universal software updates. In addition, it would require that the manufacturers devote resources to the upkeep and distribution, as well as require a second communication channel from the generator of private keys to the manufacturer for distribution.

With this in mind, an alternate system presents itself. Given that the government possesses secure channels that can be used for key distribution, an initial trial could be made using only federally maintained MMSIs. A standard could be created such that federal MMSIs broadcast some form of authenticated message. An optional upgrade for commercial systems would allow the deciphering of the authenticated message. The private key management is done by the government, and existing systems can be used for the distribution of public keys. The benefit to the typical consumer would be seen primarily from the authentication of AIS ATON, which is more frequently encountered in high traffic waterways.

Summary

Digital authentication using the signature method of asymmetrically encrypting a hash digest can be technically applied to the existing format of AIS in several ways. There are some problems that it does solve, but it fails in other regards. Key distribution to support digital signatures is more challenging. Some existing infrastructure could be used, but much would have to be replaced or upgraded to successfully transmit private keys confidentially.

Chapter V: Results, Conclusions, and Recommendations

Introduction

In this chapter, the study questions posed in Chapter One are answered. Additionally, the conducted research is summarized and final thoughts presented along with possibilities for future research on this subject matter.

Results

1. Is digital signature based authentication able to be successfully applied to AIS?

It is absolutely possible to implement authentication using existing hashing algorithms and asymmetric encryption to create digital signatures. Depending on the method desired, most established hashing algorithms can be used.

2. What must be altered to allow them to function with existing technology, or conversely, what characteristics or functionality of existing technology must be altered to allow authentication methods?

To implement digital signature authentication, there would need to be nontrivial adjustments made to existing systems. It is possible to use the existing radio channels and organization schemes to distribute authenticated messages without change, but the generation and receipt of the signals would require new equipment.

3. Is message authentication a viable solution to the problems faced by AIS?

Digital message authentication is a technically possible but realistically unfeasible solution to the issues found in AIS. There would need to be agreement on a key distribution system, as well as a time frame for implementation. Given the quantity of active AIS devices, it would be a tremendous undertaking.

Conclusion

There is not currently enough of a threat to AIS to make the expenditure of resources worth it. Additionally, there are problems with AIS that message authentication would not solve. It primarily addresses spoofing but would not cover self-spoofing, as in broadcasting one's own position falsely for purposes such as evading customs or international borders. Anomaly detection is a more realistic and flexible approach to detecting such incidents.

Absent a large scale exploitation of AIS, it would be a more effective use of resources to increase training and professionalism of mariners. Reducing overreliance on AIS, and encouraging active correlation with alternate sources, eliminates most of the issues that digital authentication would solve. Digital authentication should be considered for any new system designed to replace or supplement AIS.

Future Work

There are distinct avenues of exploration if one wanted to delve further into the topic. A practical experiment using an AIS receiver can easily be imagined. Using the characteristics of the receiver, a dedicated software layer can be designed to directly interface and manage authentication of signals. Control over both the transmitter and receiver is necessary, which unfortunately limits the use of existing signal dumps as none would have any authenticated data.

Another possible area would be a limited distribution scheme focusing on federal entities. With the existing distribution methods more ably supporting secure private key distribution, one of the major security concerns would be removed.

References

All About AIS. 2012 *AIS TDMA Access schemes*. Retrieved from http://www.allaboutais.com/jdownloads/Access%20schemes%20technical%20downloads/ais_tdma_access_schemes.pdf

Alltek Marine Electronics Corp. (n.d). *AIS_Encryption* [Infographic]. Retrieved from http://www.alltekmarine.com/images/AIS_Encryption.jpg.

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

Gebhardt, M., Illies, G., Schindler, W. (2006) *A Note of the Practical Value of Single Hash Collisions for Special File Formats*. Bundesamt für Sicherheit in der Informationstechnik (BSI) Godesberger Allee 185–189 53175 Bonn, Germany. Retrieved from https://pdfs.semanticscholar.org/f124/959267e1bc7b5b568de244a5a4f1276dd74a.pdf

International Maritime Organization (IMO). *International Convention for the Safety of Life At Sea, amended, Regulation 19.2.4*, 1 November 1974, available at: http://solasv.mcga.gov.uk/Regulations/regulation19.htm#24

International Telecommunications Union (ITU). *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 at https://www.itu.int/rec/R-REC-M.1371-5-201402-I/en

International Telecommunication Union. *Recommendation ITU-R M.585-7 Assignment and use of identities in the maritime mobile service*. March 2015. Retrieved from http://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.585-7-201503-I!!PDF-E.pdf

Iphar, C. Napoli, A. Ray, C. *A method for integrity assessment of information in a worldwide maritime localization system.* June 2016. AGILE 2016 Helsinki. **hal-01421920, version 1.** Retrieved from http://www.hal.inserm.fr/ENSMP_CRC/hal-01421920v1.

Iphar, C. Napoli, A. Ray, C. *Detection of false AIS messages for the improvement of maritime situational awareness*. Oct 2015. OCEANS'15 MTS/IEEE Washington. DOI: 10.23919/OCEANS.2015.7401841. Retrieved from http://ieeexplore.ieee.org/document/7401841/

KONGSBERG SEATEX AS. *AIS 300 Data Sheet.* June 2015. Kongsberg, Norway. Retrieved from https://www.km.kongsberg.com/ks/web/nokbg0397.nsf/AllWeb/BEA28E28C4D3E5EFC1256F9700348931/$file/Datasheet_AIS300_june2015.pdf?OpenElement

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

National Oceanic and Atmospheric Administration (NOAA). *Head of Green Bay, including Fox River below De Pere;Green Bay, Chart No. 14918*. 28th Ed., Dec 2015 corrected through 30 Sep 2017. Available at http://www.charts.noaa.gov/OnLineViewer/14918.shtml

SAAB AB. *R5 SECURE W-AIS.* Copyright 2017. Linköping, Sweden. Retrieved from http://saab.com/security/maritime-traffic-management/traffic-management/R5-Supreme-W-AIS/

Stallings, W. (2017). Cryptography and network security: principles and practice (Vol. 7). Hoboken, NJ: Pearson Education Inc.

U. S. Coast Guard Navigation Center. *Local Notice to Mariners [digital image]*. Alexandria, VA. 10 Jan 2018. Retrieved from https://www.navcen.uscg.gov/?pageName=lnmMain

U. S. Coast Guard Navigation Center. 30 July 2014. *AUTOMATIC IDENTIFICATION SYSTEM OVERVIEW.* Alexandria, VA. Retrieved from https://www.navcen.uscg.gov/?pageName=AISmain

US Dept. of Homeland Security, US Coast Guard. *Light List Volume VII Great Lakes.* Pages 208-209. January 2017. Available at https://www.navcen.uscg.gov/?pageName=lightlists

Wreski, E., Lavoie, E. March 2017. *A Concept of Operations for an unclassified common operational picture in support of Maritime Domain Awareness.* Naval Postgraduate School. Retrieved from http://hdl.handle.net/10945/52954.

Appendix A. AIS Message Types

MSG ID	Name	Access Scheme	Comm. State	MSG Size (bits)
1	POSITION REPORT	S,R,A	SOTDMA	168
2	POSITION REPORT	S	SOTDMA	168
3	POSITION REPORT	R	ITDMA	168
4	BASE STATION REPORT	F,R	SOTDMA	168
5	STATIC AND VOYAGE RELATED DATA	R,I	N/A	424
6	BINARY ADDRESSED MESSAGE	R,F,I	N/A	1008
7	BINARY ACKNOWLEDGEMENT	R,F,I	N/A	1008
8	BINARY BROADCAST MESSAGE	R,F,I	N/A	1008
9	STANDARD SAR AIRCRAFT POSITON REPORT	S,R,I	SOTDMA, ITDMA	168
10	UTC/DATE INQUIRY	R,F,I	N/A	72
11	UTC/DATE RESPONSE	R,I	SOTDMA	168
12	ADDRESSED SAFETY RELATED MESSAGE	R,F,I	N/A	1008
13	SAFETY RELATED ACKNOWLEDGEMENT	R,F,I	N/A	1008
14	SAFETY RELATED BROADCAST MESSAGE	R,F,I	N/A	1008
15	INTERROGATION	R,F,I	N/A	88-160
16	ASSIGNMENT MODE COMMAND	R,F,I	N/A	96-144
17	DGNSS BROADCAST BINARY MESSAGE	R,F,I	N/A	80-816
18	STANDARD CLASS B EQUIPMENT POSITION REPORT	S,I,C	SOTDMA, ITDMA	168
19	EXTENDED CLASS B EQUIPMENT POSITION REPORT	I	N/A	312
20	DATA LINK MANAGEMENT MESSAGE	R,F,I	N/A	72-160
21	AIDS-TO-NAVIGATION REPORT	R,F,I	N/A	272-360
22	CHANNEL MANAGEMENT	R,F,I	N/A	168
23	GROUP ASSIGNMENT COMMAND	R,F,I	N/A	160
24	STATIC DATA REPORT	R,I,C,F	N/A	168
25	SINGLE SLOT BINARY MESSAGE	R,I,C,F	N/A	168
26	MULTIPLE SLOT BINARY MESSAGE	R,I,C,F	SOTDMA,	1064

	WITH COMMUNICATION STATE		ITDMA	
27	POSITION REPORT FOR LONG RANGE APPLICATIONS	M	N/A	96
28-63	RESERVED FOR FUTURE USE	N/A	N/A	N/A

Access Schemes

F - FATDMA Fixed Access Time Division Multiple Access
I - ITDMA Incremental Time Division Multiple Access
S - SOTDMA Self Organized Time Division Multiple Access
R - RATDMA Random Access Time Division Multiple Access
M - MSSA Multi-channel Slot Selection Access

Constructed from US Coast Guard Navigation Center *AUTOMATIC IDENTIFICATION SYSTEM OVERVIEW*

Appendix B. Hash and Encrypt Format Code, Key Generator, and Timing Test

```
# Authentication Function
# input an AIS message, output an authentication message
# The function receives the input str, generates an md5 hash, encrypts it with the private key, and creates a new message that contains the encrypted hash as a payload

import hashlib
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import datetime
import base64

# random AIS string taken from catb.org/gpsd/AIVDM.html, AIVDM/AIVDO protocol decoding

# for proof of concept purposes, consider the MMSI 367527820, of the Vista Star operating out of Duluth, MN
# encoded using AIVDM protocol, that MMSI is Er0<<
# to ensure proper decryption of the string, the encrypted and hashed value will be concatenated with the MMSI which will be used to select the proper public key

ais_str = '!AIVDM,1,1,,B,177KQJ5000G?tO`K>RA1wUbN0TKH,0*5C'
```

```
# splitting the string by commas
# this creates an array of each comma delimited section of the original msg

split_str = ais_str.split(",")

# split_str[1] and [2] contain the default sequencing
# [1] is the fragment count
# [2] is the current message count
# 3,2 would mean this is the second of three fragmented messages

# apply the md5 algorithm to the original message
hash_obj =  hashlib.md5(ais_str)

# encrypt the hash digest using the private key
# first need to import the stored private key
get_key = open("priv_key_store.txt", "r")
priv_key = RSA.importKey(get_key.read())

cipher = PKCS1_OAEP.new(priv_key)
ciphertext = cipher.encrypt(hash_obj.hexdigest())
```

```
# get the current second and convert to binary
now = datetime.datetime.now()
utc_sec = base64.b64encode(str(now.second))

# create a string containing the MMSI of the broadcasting vessel, and the encrypted hash digest,
and other data
# the message type for this one is 28, an as yet unused message type
# 28 -> 011100 -> L
# communication state is left null for this example
# the value should be determined by the parent AIS unit following standard protocols
hash_str = 'LEr0<<' + ciphertext + utc_sec
auth_str = split_str[0] + ',' + '1' + ',' + '1' + ',3,' + split_str[4] + ',' + hash_str + ','

# create checksum from string
# NMEA checksum is the sequential XOR of the string
i=1
checksum = 0
while i < len(auth_str):
    checksum = checksum ^ ord(auth_str[i])
    i+=1

final_str = auth_str + '*' + hex(checksum)
```

```
print(final_str)
```

```
from Crypto.PublicKey import RSA

from Crypto import Random


# create a random number generator object

random_generator = Random.new().read

# generate a key pair of 1024 random bits

key = RSA.generate(1024, random_generator)


# create two files, to store the public and private keys

priv_key = open("priv_key_store.txt", "w")

pub_key = open("pub_key_store.txt", "w")


#export the public and private keys to the respective files

priv_key.write(key.exportKey('PEM'))

pub_key.write(key.publickey().exportKey('PEM'))
```

```
# timeit is a library that contains useful time functions
import timeit

# create a timeit Timer object
# the first argument,
hashlib.md5('!AIVDM,1,1,,B,177KQJ5000G?tO`K>RA1wUbN0TKH,0*5C, is the code to be
timed
# the second argument, import hashlib, is setup code that is run once
md5_time =
timeit.Timer("hashlib.md5('!AIVDM,1,1,,B,177KQJ5000G?tO`K>RA1wUbN0TKH,0*5C')",
"import hashlib")

# call the function like so
# t.timeit(#) where # is the amount of times the code is executed
# it returns one number, the elapsed time
# so t.timeit(1000) runs the statement 1000 times and returns the total time it took to do so



# the repeat function allows for repeated trials of the code
# called like so t.repeat(#,##)
# the second argument is the rumber of times the code is run per cycle
```

```
# the first argument is the number of cycles
# it returns a number of values equal to the number of cycles
# so t.repeat(10,2) will run the code twice and return how long it took to do that, 10 times.  You will get 10 numbers
# t.repeat(10,1) will run the code once, 10 times.
# general advice is to look at the min() of the times instead of the average, as the average will be thrown off by other cpu calls that you don't have control over.


sha1_time =
timeit.Timer("hashlib.sha1('!AIVDM,1,1,,B,177KQJ5000G?tO`K>RA1wUbN0TKH,0*5C')",
"import hashlib")
sha224_time =
timeit.Timer("hashlib.sha224('!AIVDM,1,1,,B,177KQJ5000G?tO`K>RA1wUbN0TKH,0*5C')",
"import hashlib")
sha256_time =
timeit.Timer("hashlib.sha256('!AIVDM,1,1,,B,177KQJ5000G?tO`K>RA1wUbN0TKH,0*5C')",
"import hashlib")
sha384_time =
timeit.Timer("hashlib.sha384('!AIVDM,1,1,,B,177KQJ5000G?tO`K>RA1wUbN0TKH,0*5C')",
"import hashlib")
sha512_time =
timeit.Timer("hashlib.sha512('!AIVDM,1,1,,B,177KQJ5000G?tO`K>RA1wUbN0TKH,0*5C')",
```

```
"import hashlib")


print 'minimum value from 10,000 trials'
print 'md5'
print min(md5_time.repeat(10000,1))
print 'sha1'
print min(sha1_time.repeat(10000,1))
print 'sha224'
print min(sha224_time.repeat(10000,1))
print 'sha256'
print min(sha256_time.repeat(10000,1))
print 'sha384'
print min(sha384_time.repeat(10000,1))
print 'sha512'
print min(sha512_time.repeat(10000,1))
```

Appendix C. Class A Shipborne Mobile Equipment Reporting Intervals

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

Reconstructed from ITU M.1371-5