Ive Botunac
Marijan Gržan

http://dx.doi.org/10.21278/brod68106

ISSN 0007-215X
eISSN 1845-5859

ANALYSIS OF SOFTWARE THREATS TO THE AUTOMATIC IDENTIFICATION SYSTEM

UDC 629.5.051-054
Professional paper

Summary

Automatic Identification System (AIS) represents an important improvement in the fields of maritime security and vessel tracking. It is used by the signatory countries to the SOLAS Convention and by private and public providers. Its main advantage is that it can be used as an additional navigation aids, especially in avoiding collision at sea and in search and rescue operations. The present work analyses the functioning of the AIS System and the ways of exchanging data among the users. We also study one of the vulnerabilities of the System that can be abused by malicious users. The threat itself is analysed in detail in order to provide insight into the very process from the creation of a program to its implementation.

Key words: *AIS; automatic identification system; cyber threat; vulnerability*

1. Introduction

As a part of the process of increasing maritime security by improving vessel tracking, the Automatic Identification System (AIS) was introduced. After the implementation of the IMO Resolution A.917(22) [3] and according to the regulation of the international SOLAS Convention, an obligation to implant an AIS device was imposed on July 1 2002, for all international navigation ships over 300 gross tons as well as for all passenger ships.

The implementation of the AIS System itself has brought many advantages in vessel tracking, search and rescue actions and maritime collision analyses. The device works in interaction with other navigation units on the ship that track the coordinates, speed and course, as well as other information used by the system.

Every day we are witnesses to the automatization in maritime affairs and we rely on an ever increasing number of electronic navigation devices. Despite the fact that the system enables greater security and functions as a supporting device, we should not ignore its disadvantages. Due to the maritime infrastructure development, merchant marine is becoming one of the most important profit sources, both for the government and for the private sector. That attractive data becomes of interest to many criminal groups engaged in maritime industry. On the basis of our study [1] of the AIS System security evaluation, we are able to

see the weak points that could be used by the attackers in order to compromise the system. With further investigation we want to draw attention to the possible abuses of the system's software.

Furthermore, in Section 2 we explain the functioning of the system in order to delve into the methods of exchanging data between the ship and the coast station in the next section. In the main part of the study we focus on the threats that can be carried out by specialized software solutions and we show how one of the models can be created. The results of the study are presented in Section 5, together with the conclusions of the analysis.

2. AIS System overview

AIS standard can be found in two forms. One of them, Class A, is used on the SOLAS Convention vessels, while Class B is a more affordable choice destined for non-SOLAS vessels. The transponder of a Class A unit has one VHF transceiver, two VHF TDMA receivers, one VHF DSC receiver and connections with the vessel devices that use standard vessel communication IEC 61162/NMEA 0183 [5]. In order to synchronize time and obtain information on the location, the device uses accurate GPS time data. Other navigation parameters are obtained from the sensors aboard the vessel.

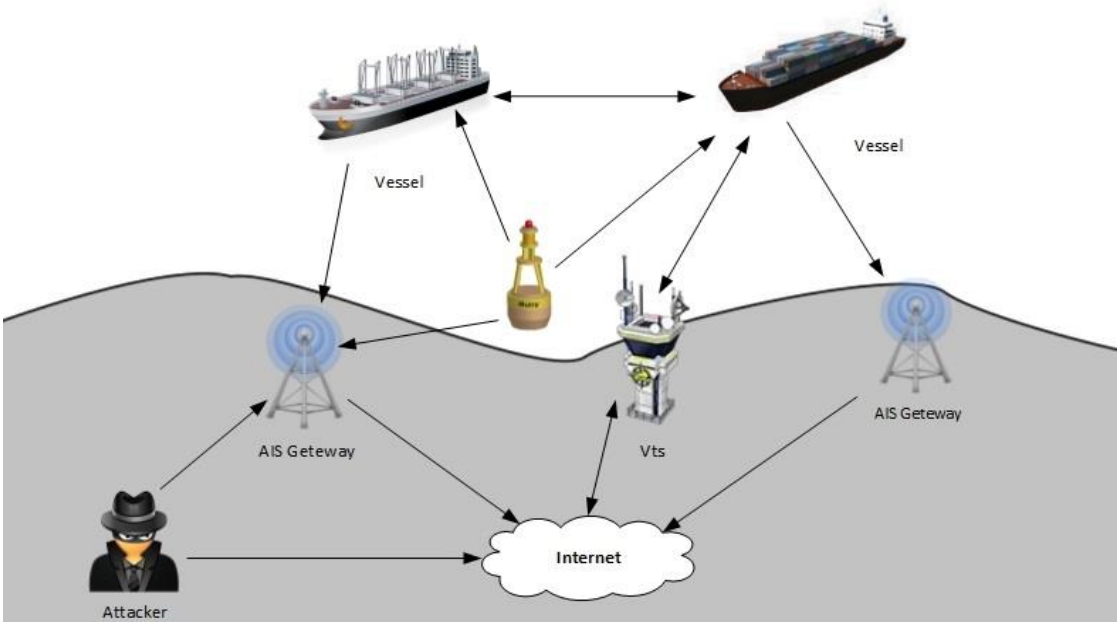

Fig 1. System overview

The emission from an AIS unit is autonomous and constant, and it uses two VHF frequencies: 161.975 MHz and 162.025 MHz Self-Organized Time Division Multiple Access (SOTDMA) is used for data exchange. It enables data emissions among multiple users via only one VHF channel. The location report emitted by one AIS station is integrated into one of the 2250 cells every 60 seconds. AIS stations are constantly synchronized in order to avoid information overlap in one cell. If the messages start to overload the network, the system automatically eliminates the more distanced stations in favor of those in closer proximity.

The data exchange itself is based on the modulation defined by ITU Recommendations [2]. In Figure 1 we lay out a simple example of the process of exchanging data between vessels, coast stations and a control center, as well as their transfer to the network.

The data exchanged between AIS stations can be static, dynamic, security or navigation related. During the installation of the system on a vessel, the static data that contain the MMSI (Maritime Mobile Service Identity) are manually set. MMSI is a nine-digit number that represents an identification mark of a vessel whose first three digits refer to its country of origin. Static data also include some basic information, like the IMO number, vessel type, length and width. The applicable dynamic data, updated automatically, provide information on the location, time, course and speed over ground, navigation status and other important information relevant for the maritime security.

3. Data exchange method

Regarding the structure of the AIS System, we notice that the standardized model is used. These models function on the basis of the data exchanged between coast AIS stations and control centers via the Internet. We see the same structure both in the public providers, like MarineTraffic.com, and the state ones, like Vessel Traffic Management and Information System (VTMIS).

In the case of the Republic of Croatia there are 17 coast AIS stations connected to the main control center in Rijeka via 128Mbit/s permanent connection provided by the state communications provider [6]. The national control center in Rijeka gathers all the data from the coast stations, presents it, stores it and forwards it to the users. European Union member states are obligated to exchange data with the European exchange platform of maritime states called SafeSeaNet. The network enhances communication between the local and regional state units on one hand, and the center, on the other, gathering information that prevents maritime accidents, contamination of the sea and other factors important for the maritime safety. Figure 2 shows the components of the system in the Republic of Croatia. We can see how the data gathered on the coast station are interchanged via the network with the other components of the system.

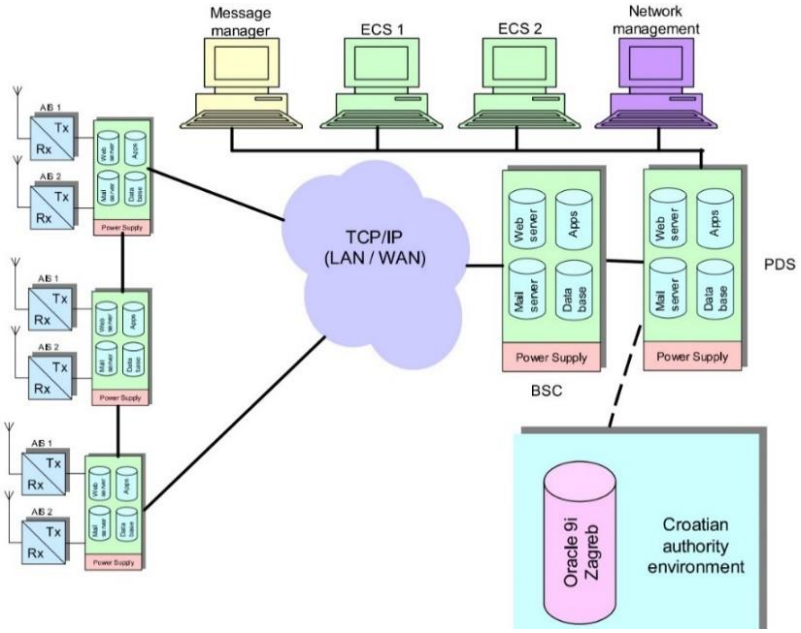

Fig 2. AIS system components in National Control Centre [6]

3.1 AIS data format

For the exchange of data sentences between vessels and VTS a two-layer AIVDM protocol is used. AIVDM protocol defines 27 types of messages that can be exchanged and each of them has one specific purpose [7]. The outer layer of AIVDM protocol is a variation of the NMEA 0183 protocol that is used in standardized data exchange in the maritime navigation system [9].

From the above mentioned messages that can be exchanged, the important ones for our study are the first three which define the vessel location report. Among the others we can emphasize the message 24, which informs about the static data, and the message 21, that provides a report from the navigation instruments.

Let us examine an example of an AIVDM sentence, coded according to the NMEA standard, that provides information about the location of a ship.

Example: *!AIVDM,1,1,,A,11mg=5@OD>17JD0I?f@72?wp0000,0*04*

In the body of the sentence the coded AIS data is the following part: *11mg=5@OD>17JD0I?f@72?wp0000*. In the NMEA coding for AIS every ASCII sign matches its special six-bit binary version [2]. After the decoding, we get a binary translation of the sentence, as shown in Table 1.

Table 1. Presentation of the content of an AIVDM sentence

Bits	Bits value	Parameter	Value
6	000001	Message ID	1
2	00	Repeat indicator	0
30	000111010110111100110100010101	MMSI number	123456789
4	0000	Navigational status	0
8	011111 01	Rate of turn	+697.5
10	0100 001110	Speed over ground	27.0
1	0	Position accuracy	0
28	00001000111011010010100000000	Longitude	15°36.0000'E
27	001100100111110111001000000	Latitude	44°7.2000'N
12	011100001000	Course over ground	180.0
9	11111111	True heading	511
6	111100	Time stamp	60
2	00	Maneuver indicator	0
3	000	Spare	0
1	0	RAIM-flag	0
19	0000000000000000000	Communication state	0

3.2 Broadcast information

Depending on its speed, an AIS unit on a vessel emits messages. This means that, if the vessel is anchored, it will emit a message every three minutes; if it is sailing at the speed of 14 knots, every 12 seconds; and if the speed is over 23 knots, every 2 seconds [2]. The messages are received by the AIS stations on the coast and then forwarded to the providers via the Internet. During the transfer the TCP or UDP Internet protocol can be used, as well as the receiving IP address of the provider. Today, Marine Traffic and Vessel Finder are among the most popular public providers that have their own web sites with all the necessary information, but also enable the data to be interpreted by third-party programs or sites. A similar way of emitting data is used by the state providers, but the technical details regarding the receiving IP addresses are not publicly available.

In the following section we would like to draw attention to the lack of security controls by the providers that receive AIVDM sentences [1]. The providers are not able to check the source that emitted the message and to see whether it is legitimate. This weak point can be found on every public provider and can enable deceptions malicious users can take advantage of.

4. A software threat

We have previously explained which types of messages can be exchanged via the AIS unit and we showed how they were coded. The characteristic that we will focus on in the AIS reporting system is the transfer of the above mentioned data onto AIS providers via the Internet. Such an approach in data collecting offers an insight into the situation at sea that is of crucial importance to VTS, harbormaster's office and other participants relevant for the maritime traffic security.

An AIS data manipulation can have a breach of the law as a result. The law states that the AIS data can serve as proof material in the offence procedure, as can be seen in the article 158 subsection 5 of the Offence Law: "If, during their supervision, an authorized civil servant has noticed directly an action of committing an offence or has established it immediately using adequate technical devices and has made an official note or technical recording, the official note and the technical recording serve as proof material in the offence procedure" [18].

4.1 Threat review

By the term "threat" we imply any disturbances that disable the timely functioning of the system and the credibility of its data. One of the attacks can be the creation of a false vessel that appears with the same static and dynamic data as a real one. An attacker can use the MMSI number of a real vessel and alter its data, for example its speed, course and coordinates. In this way we get a false location of the vessel and its parameters, which can lead to the alarming of the authorities, if the vessel is shown to be in a prohibited area. Such a possibility provides a wide range of malicious actions that an attacker could undertake.

Using computer programmed algorithms, attackers can take control of the data of all the vessels in an area. The data regarding the transportation of dangerous cargo can also be falsified, which can directly violate the universally accepted regulations and standards, as well as the Croatian regulations on vessel-related contamination of the sea. Studying the bibliography available to the date, we can find out that one author has already brought up the question of the possibility of creating false data packages. These threats can be attributed to

the vulnerability of the AIS open communication system which does not use cryptographic methods to ensure communication security [19]. Using these kinds of deceptions, Somali pirates, for instance, can falsify data regarding a hijacked vessel so that it appears it is still on its planned course while it actually finds itself in a perilous situation.

As we can see, potential attackers have a wide range of possibilities that can be used for malicious purposes. Their motivation can vary, depending on whether the attack is carried out by an individual or an organization. One can imagine that criminal organizations have a wider range of possibilities at their disposal, both when finances and manpower are concerned, which is why these attacks can be deemed more dangerous. One of the reasons for carrying out this kind of attack can be an intention to cover up a more serious attack. The attackers can manipulate the data so as to create a false location of a ship, in order to perform a real physical attack upon it.

5. Programming software threats

In this section we would like to show how to create a tool that can be used to disturb the transmission of the information via the AIS System, using the programming language C++ with standard libraries and a QT program framework that contains many libraries which are widely used in the creation of applications with graphic interface.

5.1 Creation of the program

In Table 1 we showed the elements of which an AIVDM sentence is composed, as well as the length and the value of each element. Furthermore, we had to create a function that would transform the input parameters into outcome content in binary form. In order to do so, we used the C++ library *bitset* that enables the storage of binary values within the variable. In this way, by entering the value of the MMSI number, we get its binary value of 30 bits. If its real binary value is not of 30 bits, the function *bitset* fills in the rest of the space with zeros in order to meet the established requirements. This is how we created the binary value of all the elements that an AIVDM sentence has to contain in order to report on a location, which was afterwards stored as *string* type information. An illustration of the function can be seen in Figure 3 where the income parameters are shown, together with the outcome parameter that the function produces.

```
string encode(int mmsi, float speed, float longi, float lati, float course)
{
    bitset<6> type(1);
    string repeat = "00";
    bitset<30> mmsi_b(mmsi);
    bitset<4> status(0);
    bitset<8> rot(125);
    bitset<10> speed_b(round(speed * 10));
    string accurancy = "0";
    bitset<28> longit =longitude_(longi);
    bitset<27> latit = latitude_(lati);
    bitset<12> course_b(round(course * 10));
    bitset<9> true_heading(511);
    bitset<6> ts_b(60);
    string flags = "000000";
    string rstatus = "0000000000000000000";

    string final = type.to_string() + repeat + mmsi_b.to_string()
                 + status.to_string() + rot.to_string() + speed_b.to_string()
                 + accurancy + longit.to_string() + latit.to_string()
                 + course_b.to_string() + true_heading.to_string()
                 + ts_b.to_string() + flags + rstatus;
    return final;
}
```

Fig 3. Function for coding an AIVDM sentence

The next step is to create a NMEA sentence from the binary value, which was described in the former section. As we have explained, a special way of converting a binary number into an ASCII sign is used, where one sign does not contain the usual 8, but rather 6 bits. In order to get one ASCII sign, we take a six-bit message, which means that a generated message of 168 bits corresponds to 28 signs. For one six bit long binary message we search the ASCII table and, excluding the first two figures, we calculate its decimal number value. If that number is higher than 39, we add 8, and if it is not, we add 48.

Example: We enter the binary value 010100 into the table and calculate its decimal value 20. Since that decimal value is lower than 39, we add 8. Now using the number 28 we consult the table and take the sign with the corresponding decimal value "D".

The last thing we have to do is introduce the data into one of the providers using the UDP Internet protocol. This is performed by sending the created sentence to the receiving IP address and the provider's port. The data concerning the public providers can be found on their official web pages.

5.2 Performing an Experiment

In order to administer a test, we will use the program we created for sending an AIVDM sentence to the public provider. We will use a technique of false representation and generate a false location and false data for a selected ship. After starting the program, we set the parameters which include the MMSI of the ship. The false AIVDM sentence is forwarded by the program to the MarineTraffic provider via the IP address and a determined port. The sent information can be seen on the official, publicly available page, as the Figure 4 shows.

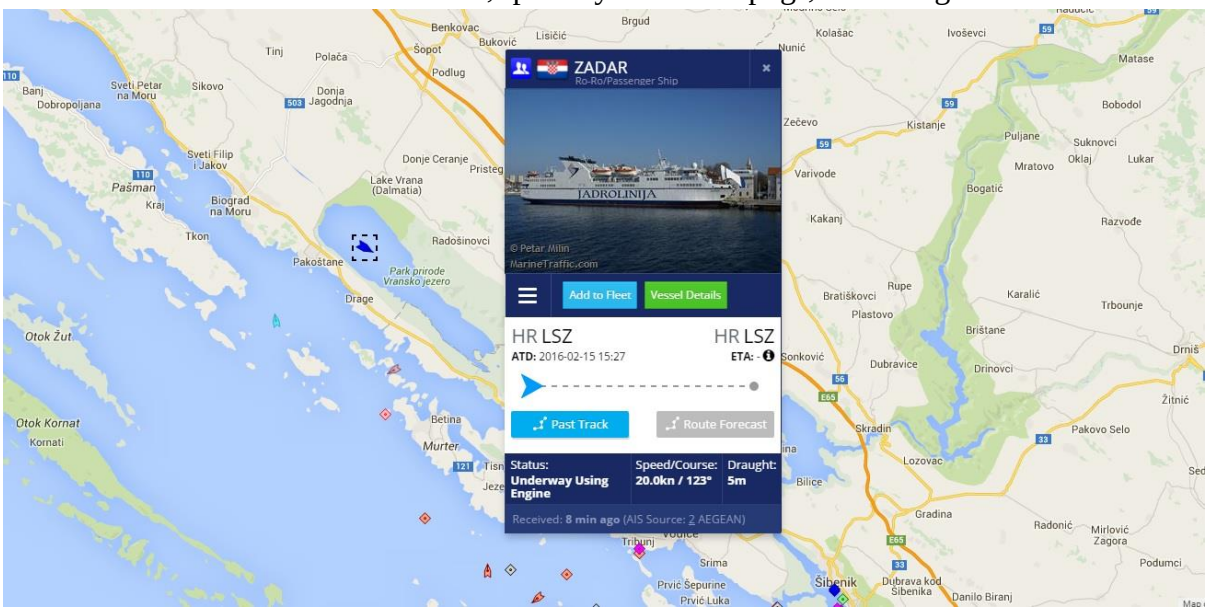

Fig 4. Results of the test

We would like to point out that the infrastructure of the public providers that offer AIS services is in no way related to the AIS system applied by the states. These false data appear only on the page of the chosen provider and cannot cause safety threats.

6. Conclusion

The abuse of the AIS System can result in serious problems in maintaining maritime security and the aim of this study was to draw attention to that. Nowadays the Internet offers easily reachable bibliography about the vulnerability of the system that can be used by potential attackers. We should be aware that, no matter the technological advancements used in everyday life, the importance of the human factor should not be ignored. The area of computer security in maritime affairs is a new discipline that is yet to find its place in the totality of the infrastructure.

In order to act preemptively, this area of expertise should be included in the future seamen education. Today we still lack official solutions to the abuses of the AIS System. One suggestion [1] was to introduce the public key infrastructure (PKI) that uses asymmetric cryptography in order to protect the integrity of the data. Another option is to introduce various types of machine learning techniques in order to recognize anomalies [15].

REFERENCES

[1] Balduzzi, M., Pasta, A. and Wilhoit, K., "A security evaluation of AIS Automated identification system", ACSAC '14 Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, 2014, pp. 436-445. https://doi.org/10.1145/2664243.2664257.

[2] International Telecommunications Union, "Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band", Recommendation ITU-R M.1371-5, 2014.

[3] International Maritime Organization, "Guidelines for the onboard operational use of shipborne automatic identification systems (AIS)", Resolution A.917(22), 2001.

[4] International Maritime Organization, "Automatic Identification Systems (AIS)", 2015, Available from: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx

[5] U.S. Coast Guard Navigation Center, "Automatic identification system overview", 2015, Available from: http://www.navcen.uscg.gov/?pageName=AISworks.

[6] Ministry of Maritime Affairs, Transport infrastructure, "CVTMIS data management system design", 2008.

[7] U.S. Coast Guard Navigation Center, "AIS Messages", 2015, Available from: http://www.navcen.uscg.gov/?pageName=AISMessages

[8] Raymond, E. S., "AIVDM/AIVDO Protocol Decoding", Available from: http://catb.org/gpsd/AIVDM.html.

[9] Raymond, E. S., "NMEA Revealed", Available from: http://www.catb.org/gpsd/NMEA.html#GIDS

[10] Gržan, M., "Procedures and Deck Officer Training in Cases of Intentional Radar System Jamming and Deception", Naše more, 61 (3-4), 2014, pp. 67-76.

[11] Matika, D. and Gržan, M., "Optimizing Marine Radar Performance in Enhancing the Safety of Navigation", Brodogradnja, 64 (3), 2013, pp. 305-322.

[12] Gržan, M. and Čovo, P., "Sequencing radar jamming – method and technical solution", Annals of DAAAM'2007 & Proceedings of the 18th International DAAAM Symposium "Intelligent Manufacturing & Automation: Focus on Creativity, Responsibility, and Ethics of Engineers", Wien, Austria, 2007.

[13] Katsilieris, F., Braca, P. and Coraluppi, S., "Detection of malicious AIS position spoofing by exploiting radar information", Information Fusion (FUSION), 2013 16th International Conference, 2013, pp. 1196-1203.

[14] Bošnjak, R., Šimunović, L. and Kavran, Z., "Automatic Identification System in Maritime Traffic and Error Analysis", Transactions on Maritime Science, 1(02), 2012, pp. 77-84. https://doi.org/10.7225/toms.v01.n02.002.

[15] Obradović, I., Miličević, M. and Žubrinić, K., "Machine Learning Approaches to Maritime Anomaly Detection", Naše more, 61(5-6), 2014, pp. 96-101.

[16] Komadina, P., Brčić, D. and Frančić, V., "VTMIS Service in the Improvement of the Adriatic Sea Maritime Transport Safety and Environmental Protection", Pomorski zbornik, 47(1.), 2014, pp. 27-40.

[17] Solo, D., Housley, R. and Ford, W., "Internet X. 509 Public Key Infrastructure Certificate and CRL profile", 2008. Available from: http://www.ietf.org/rfc/rfc245.

[18] „Prekršajni zakon", Narodne novine, 107/07, 39/13, 157/13, 110/15, 2015.

[19] Kezić, V., „'Meki' napadi na AIS mogući i na Jadranu", 2014. Available from: http://obris.org/hrvatska/meki-napadi-na-ais-moguci-i-na-jadranu/.

Submitted: 17.04.2016.
Accepted: 08.05.2016.

Ive Botunac, ive.botunac@gmail.com
Marijan Gržan, magrzan@unizd.hr
University of Zadar, Maritime Department, Mihovila Pavlinovića bb, 23000, Zadar