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

DOI: 10.12716/1001.14.02.03

Secure AIS with Identity-Based Authentication and Encryption

A. Goudosis
University of Piraeus, Athens, Greece
The Hellenic Quality Assurance and Accreditation Agency (HQA), Greece
Mediterranean College, Athens, Greece

S.K. Katsikas
Norwegian University of Science and Technology, Gjøvik, Norway
Open University of Cyprus, Nicosia, Cyprus

ABSTRACT: The Automatic Identification System (AIS) offers automatic traffic control and collision avoidance services to the maritime transportation sector worldwide. Because AIS lacks security mechanisms, it is vulnerable to misuse and exploitation by unlawful adversaries (e.g. sea-pirates, terrorists, smugglers). To address the security issues of the AIS, in an earlier paper [1], we proposed the deployment of a Maritime Certificate-less Identity-Based (mIBC) public-key cryptography infrastructure that enhances AIS with on-demand anonymity, authentication, and encryption capabilities. In this paper we address implementation aspects of that infrastructure. In particular, we propose to use the Sakai-Kasahara Identity-Based Encryption (IBE) approach to implement the mIBC infrastructure, following the IEEE 1363.3-2013 standard for Identity-Based Cryptography.

1 INTRODUCTION

The Automatic Identification System (AIS) is a maritime navigation safety communications system [2]; its main aim is to improve the maritime domain awareness beyond the limitations of the radars. Radars give a good perspective of the shoreline and of moving targets but their accuracy is limited by the presence of obstacles (e.g., small islands), the Radar-Cross Section (RCS) value of the targets and the weather conditions. In contrast, AIS transmissions remain accurate, with good or adverse weather conditions, in areas with many physical obstacles or heavy marine traffic (e.g., Malacca Straits). Shipborne AIS devices periodically transmit static data (i.e. vessel's name, MMSI [3], IMO-number, type, dimensions, departure port, arrival port, cargo, etc.) and dynamic real-time navigation data (i.e., Global Navigation Satellite System (GNSS), steering, speedometer, etc.) [3]. When this information, as received from all nearby AIS devices, is aggregated and overlaid on a vessel's electronic navigation chart, the officer-on-watch obtains a good overview of the nearby marine traffic. The use of the AIS is regulated by "Regulation 19" of SOLAS Chapter V, under the supervision of the International Maritime Organization (IMO) and the International Telecommunications Union (ITU).

[3] The MMSI (9-digits) is a number that distinctively identifies a vessel. The MMSI is assigned to all the radio communications of that vessel. The International Maritime Organization number (IMO-number) is also a distinctive identifier for a vessel and is formed by the prefix "IMO" followed by 7 digits. The main difference with the MMSI is that the IMO-number is the only persistent identifier for a vessel, from the start of its life to the end of it. On the contrary, the MMSI changes when a vessel changes flag and registration authority.

Many shore stations equipped with AIS receivers forward received AIS data to various publicly available internet sites[4]. Undoubtedly, this practice offers a valuable tool for the international maritime community but may also become a convenient tool for unlawful adversaries. Unrestrained disclosure of the AIS broadcasted data via the internet can be an aid to sea-pirates and may violate the privacy of passengers [4], [5]. Additionally, the AIS lacks source authentication of the transmitted data, as source authenticity of AIS data relies on the transmitted MMSI number of the ship and its name. However, none of these is officially hardcoded on the AIS devices, nor are the relevant messages signed and certified. Thus, anyone with little knowledge of AIS workings can use an AIS transmitter to create fake AIS data that impersonate non-existing ships, AtoN (Aid to Navigation) or SAR (Search And Rescue Operations) [6], [7]. Without AIS authentication, the maritime domain may be the true one or a fake representation of the marine traffic in the area. A possibly fake representation of the marine traffic in an area poses a very severe threat to the international maritime community. The threat landscape of the AIS ecosystem has been examined in [8]. Accordingly, enhancing the security of AIS becomes an issue of importance to the maritime community. The VHF Data Exchange System (VDES) is seen as an effective and efficient use of radio spectrum, building on the capabilities of AIS and addressing the increasing requirements for data through the system, including some security aspects. VDES is also secure by design. However, full take up of VDES is not expected to happen soon [9].

In [1] we introduced the concept of the Maritime Certificate-less Identity-Based Public Key Cryptography infrastructure (annotated for simplicity "maritime IBC" or "mIBC"), and proposed a solution to enhance the security of the AIS. In this paper, we refine and build upon that work and discuss implementation issues. Specifically, we discuss the implementation of the additional AIS modes of operation proposed in [1] using the AIS protocol and message structure specifications, the IEEE 1363.3-2013 standard, and the Sakai-Kasahara IBE scheme.

The remaining of this paper is organized as follows: In section two we discuss related work. Section 3 briefly reviews the AIS security proposal in our earlier work [1], so as to make the present paper self-sustained. In the third section we discuss the seamless implementation of AIS usage modes over the conventional AIS transport protocol. The initial setup and the operation of the three mIBC-AIS usage modes (3, 4, 5) that use cryptography and divert from the standard ones are discussed in section 4. Section 5 presents the structure of the AIS messages in the mIBC-AIS and describes the operation of the mIBC-App, an application designed to ensure transparent transmission/reception of the mIBC-AIS messages over the conventional AIS protocol. In Section 6 we discuss the operational overhead imposed by the proposed mIBC. Finally, section 7 summarizes our conclusions.

[4] e.g. www.marinetraffic.com

2 RELATED WORK

In [10] a new protocol for AIS that relies on a three-tiered approach to security with vessel identity verified by certificates assigned by an approving authority was proposed. This solution assumes the existence of a cryptographic infrastructure that provides the maritime community with some cryptographic capabilities. The authors in [11] use AIS, the Maritime Mobile Service Identities (MMSIs) of the vessels and Trusted Third Parties to propose a three-step mutual authentication scheme that uses AIS as the communication means to provide authentication capabilities to the ships rather than endowing the AIS itself with additional security capabilities.

The authors in [12] proposed a solution based on the creation of a global, x.509-like Maritime PKI, where the registration and Certification Authorities would be the IMO and the National Maritime Authorities. This proposal suffers from implementation difficulties, because implementing a PKI infrastructure in a global maritime environment may prove to be quite a demanding and complicated task, and because certificates are very resource demanding in the challenging and costly maritime wireless communication environment. For these same reasons, works that aim at improving the security of similar systems, such as the Automatic Dependent Surveillance-Broadcast (ADS-B) in aviation, and propose the use of identity-based cryptography and symmetric cryptography [13], [14] are inapplicable in the maritime environment. Work that is not yet clear whether or how it may affect the future of AIS security is also underway [15].

Commercial AIS products that use symmetric cryptography exist (e.g. [16]). Nevertheless, they provide proprietary encrypted AIS only in vessels equipped with the same AIS product. Additionally, a worldwide adoption of a symmetric cryptography system that would need to manage symmetric keys on a vast number of vessels worldwide is a very complex if at all possible task. Therefore, such a solution is insecure for systems with characteristics similar to those of AIS [17].

The cryptographic schemes that we use to implement mIBC are identity-based cryptographic schemes founded on the q-Bilinear Diffie-Hellman Inversion problem (q-BDHIP), based on the Sakai-Kasahara Identity-Based Encryption scheme [18], whose security was proved in [19]. The IEEE 1363.3-2013 "Standard for Identity-Based Cryptographic Techniques using Pairings" [20] specifies identity-based cryptographic schemes based on the bilinear mappings over elliptic curves known as pairings. This standard describes eight identity-based cryptographic schemes that use pairings in their implementation. The schemes include approaches to encryption, digital signatures, signcryption, and key exchanges. These schemes may be used to encrypt both stored data as well as data in transit. The standard describes algorithms for calculating pairings and gives parameters suitable for implementing the specified schemes at industry-standard security levels [21]. Applications of certificate-less Identity-Based Cryptography (IBC) to navigation are described in

[17], [22]. The use of pseudonyms in transportation applications is discussed in [23], [24].

3 SECURE AIS THROUGH THE MARITIME IBC (MIBC)

In [1], we proposed the security enhancement of AIS with the use of Identity-Based Public Key Cryptography (IBC) [25], [20] as the foundation of an International Maritime Identity-Based Cryptographic infrastructure (mIBC), under the supervision of the IMO.

IBC is a variation of public key cryptography proposed by Shamir in 1985 [25]. On public-key cryptography infrastructures (PKIs), each entity has a pair of mathematically connected keys, a Private (Secret) key and a Public Key. Data that are encrypted with the Private (Secret) key are decrypted with the corresponding Public Key and vice versa. A disadvantage of the PKIs [26] is that the participating entities have to somehow obtain the public keys of the other participating entities. The solution is the use of special certificates that bind the name of the entity with its public key. However, this poses a new problem; the participating entities in the PKI should have the ability to obtain securely the certificates of the other participants. Instead of certificates, the IBC variations use a publicly known unique identification of an entity as its Public key (e.g., entity's name, e-mail address, MMSI or pseudo-MMSI number in [1]).

Unfortunately, that convenience comes with a cost; IBC infrastructures need the existence of a trustworthy central coordinator. The trusted central coordinator [5] sets up the IBC infrastructure, and generates all the Private (Secret) keys of the IBC participated entities. Then, the participating entities obtain, by means of a secure channel, their Private (Secret) keys from the trusted central coordinator. The main disadvantage of the IBC is that, beyond the owner of the key, the Trusted Central Coordinator knows the Private (Secret) keys. On the other hand, the main advantages of IBC over traditional PKI are the simplicity of the infrastructure, resources savings, and self-proved information on the public key [22], [27], [28], [29].

The mIBC-PKG functionality can either be implemented by a single authority (e.g. IMO) or by a number of multiple inter-trusted mIBCs operating in parallel. For simplicity, in the sequel we assume the existence of only one International Maritime mIBC Private key generator (IMO-mIBC-PKG) as an IMO agency. However, the implementation of the other option is straightforward.

The approach involves defining five distinct AIS *usage modes* with various security features to choose from, according to the needs of the vessel during the trip, as follows:

1 The **mIBC-Typical-AIS (mode 1):** The AIS as is today, for routine use.

2 The **mIBC-Authenticated-AIS (mode 2):** Offers source authentication via cryptographically-signed AIS transmitted messages. Under mIBC, an AIS device signs the transmitted AIS data with its mIBC Private (Secret) key, and the receivers authenticate the signed AIS data by using only the MMSI of the transmitter.

3 The **mIBC-Anonymous-AIS (mode 3):** Offers legitimate anonymous AIS transmitted messages via cryptographically-signed "Pseudo-MMSIs." An AIS device transmits, instead of the real MMSI of the vessel, a pseudo-MMSI generated and cryptographically signed by the IMO-mIBC-PKG. From a cryptographic point of view the mIBC-Anonymous-AIS (mode 3) is identical with the mIBC-Authenticated-AIS (mode 2) but uses pseudo-MMSI instead of the real MMSI of the vessels [1].

4 The **mIBC-SK-IBE-AIS (mode 4):** Allows the transmission of encrypted AIS messages to a specific entity via an appropriate encryption scheme, such as the Sakai-Kasahara Identity Based Encryption scheme.

5 The **mIBC-AES-AIS (mode 5):** Allows the transmission of encrypted AIS messages to a group of participants (i.e. trustworthy vessels in an insecure area) via symmetric cryptography (e.g., AES [30]).

Their interrelationships are depicted in Figure 1. Details on the structure of the messages are given in Section 5.

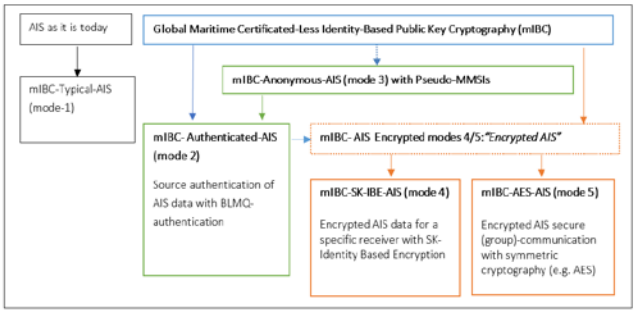

Figure 1. Usage modes of the secure mIBC-based AIS

4 IMPLEMENTING THE MARITIME IBC (MIBC)

The *entities* involved with the implementation of the mIBC are *a trusted coordinator* (also referred to as *Key Server* [20] or *Private Key Generator - PKG* [1]) and *the mIBC participants*. The trusted coordinator is an entity trusted by all the participants of the scheme. In this work, for efficiency and simplicity, we assign this role to a part of the IMO that we call *International Maritime Organization mIBC Private Key Generator (IMO-mIBC-PKG)*. mIC participants can be AIS devices, coast guards, patrol vessels, shipping companies, vessels, etc. mIBC participants may assume the role of *sender* or *receiver* of AIS messages, or both.

The IMO-mIBC-PKG is responsible for two initial operations of the mIBC, namely the *initial setup* of the scheme and the *extraction* (creation) of the Private (secret) keys of each participating entity. These are described in the sequel.

[5] Referred also as "Private Key Generator (PKG)" and "Key Server" (IEEE 1363.3-2013). We will use the term mIBC-PKG hitherto.

4.1 *Setting up the Maritime IBC (mIBC)*

In practice, the first operation of the IMO-mIBC-PKG is to define a number of cryptographic parameters, as specified in [20] and [31], that lead to the generation of the Master Secret Key and of the corresponding Naster Public Key. Specifically,

1 Establish a random number Generator ($R_{generator}$) by e.g. following the RFC5091, FIPS186-2 or X9.62 standards.
2 Choose the security parameter *t*, which is the size (in bits) of a prime number p that will be the order of the generated bilinear map cyclic groups G_1, G_2, $G_{T(arget)}$ (see below). Note that the larger the value of *t*, the more secure the scheme is.
3 Find a prime number p where $p > 2^t$ [31].
4 Generate three bilinear map cyclic groups G_1, G_2, $G_{T(arget)}$ of prime order p, by following [19], [32], [31].
5 Choose P_{G2}, a random generator of G_2
6 Find $P_{G1} \in G_1$ as a random generator of G_1, so that an efficient isomorphism φ: $G_2 \rightarrow G_1$ such that $\varphi(P_{G2})=P_{G1}$ exists.
7 e: $G_1 \times G_2 \rightarrow G_T$ is the bilinear pairing mapping.
8 Pick a random Master (Server) Secret key (Ms_{key}) $\in Z_p$.
9 Pre-calculate the pairing value $e(P_{G1}, P_{G2}) \in G_T$
10 Compute the corresponding Master (Server) Public key (M_{PUB}).

The second operation of the IMO-mIBC-PKG is to define the Cryptographic Hash functions to be used by all the participated entities.

1 (Sign 1/Enc1) H_1: $\{0,1\}^* \rightarrow Zp$, where p = "prime order" of G_1, G_2, G_T, is a cryptographic hash function viewed as a random oracle for hashing the $MMSI_{RECEIVER}$ of the receiver of the encrypted data [32]; it uses one of the SHA algorithms. Note that before using the MMSI in this algorithm, we must first convert it from bit-string to an octet string.
2 (Sign 2, h0) $H_2 : G_T \times \{0,1\}^* \rightarrow Z^*_p$ is a cryptographic hash function viewed as random oracle.
3 (Enc 2) $H_3 : G_T \rightarrow \{0,1\}^{length}$ is a cryptographic hash function viewed as a random oracle for XOR-ing with the AIS_{data} or AES_{Key}.; it uses one of the SHA algorithms. Note that because the input is a Finite Field element in G_3, it must be converted to an octet string before using the function.
4 (Enc 3) $H_4:\{0,1\}^{length} \times \{0,1\}^{length} \rightarrow Z_p$ for deriving a blinding coefficient
5 (Enc 4) $H_5 :\{0,1\}^{length} \rightarrow \{0,1\}^{length}$ for XoR-ing with plaintext

Finally, the IMO-mIBC-PKG publishes/disseminates the mIBC Public Parameters (mIBC-PP) = (G_1, G_2, G_T, e, P_{G1}, P_{G2}, M_{PUB}, $e(P_{G1}, P_{G2})$, φ, H_1, H_2, H_3, H_4, H_5) to all mIBC-enabled AIS equipment, using a secure channel (e.g., smart cards, smart tokens, etc.).

The IMO-mIBC-PKG is also responsible for safekeeping the secrecy of the Master (Server) Secret key (Ms_{key}). Because the Master (Server) Secret key (Mskey) plays the role of the Private Key of a Certification Authority in an X.509 Public Key Infrastructure, it requires the same level of advanced protection and disaster recovery plans must exist in case of compromise.

4.2 *Extracting the private keys of the participating entities*

The IMO-mIBC-PKG uses the MMSI (or the pseudo-MMSIs) as the publicly known ID of a vessel and combines it with the Public Parameters (PP) and the Master (Server) Secret key (Ms_{key}) of the mIBC to extract the corresponding Private (Secret) Key (SK_{MMSI}), of the vessel. The mandatory use of the Master (Server) Secret key (Ms_{key}) on the extraction operation prohibits an adversary to create fake Private (Secret) Keys even when they know the (publicly available) MMSI of the entity and the (publicly available) Public Parameters of the mIBC. The steps are as follows:

1 Represent the MMSI or the pseudo-MMSI as a string of bits on {0,1}
2 Compute the cryptographic hash H_1(MMSI)) or H_1(pseudo-MMSI)) respectively.
3 Compute the Private (Secret) Key_{MMSI} (SK_{MMSI}) = $(H_1(MMSI)) + Ms_{key})^{-1} Q_2 \in G_2$, where Ms_{key} is the Server (Master) Secret

Note that the main disadvantage of the Identity Based Cryptography scheme lies in this operation. Because, in contrast to the PKI, the Private (Secret) Key_{MMSI} (SK_{MMSI}) is generated centrally by the IMO-mIBC-PKG, two problems arise. First, the IMO-mIBC-PKG knows the Private (Secret) Key of the entity. Thus the security and especially the non-repudiation of the infrastructure relies heavily on the trustworthiness of the IMO-mIBC-PKG. Second, the Private (Secret) Key should be transferred from the IMO-mIBC-PKG to the AIS-device of the entity on a secure channel (e.g., smart cards, smart tokens, etc.). In [1] we proposed the manual transfer on tamper-proof devices by authorized personnel, but more convenient solutions can be found (e.g., secure internet connections).

4.3 *Operating the m-IBC*

4.3.1 *mIBC-Authenticated-AIS (mode 2) and mIBC-Anonymous-AIS (mode 3)*

The AIS device of the sending entity (the *sender*) signs the AIS data to be transmitted with its private key (SK_{MMSI}). The sender uses the Public Parameters of the mIBC, its $MMSI_{SIGNER}$, its Private (Secret) Key_{SIGNER} (SK_{signer}), a random number and the AIS_{data} to be signed. Then, the sender transmits the signed AIS data. The operation is as follows:

Input:

1 The message to be signed, $AIS_{data} \in \{0,1\}^{length}$, (length = length of the data in bits),
2 The Public Parameters, mIBC-PP = (G_1, G_2, G_T, e, P_{G1}, P_{G2}, M_{PUB}, $e(P_{G1}, P_{G2})$, φ, H_2,)
3 a random integer r, (0 < r < p-1), generated with the R_1 Generator of random numbers
4 the Private (Secret) Key_{SIGNER} (SK_{SIGNER}) $\in G_2$

Compute:

1 $u = e(P_{G1}, P_{G2})^r$
2 $h = H_2(AIS_{data}, u)$
3 $S = (r - h)\, SK_{SIGNER}$

Output:

1 The signed message is the triplet (AIS_{data}, h, S) $\in \{0,1\}^{length} \times Z_q \times G_1$

Any receiving entity can verify the authenticity of the received AIS data by using the (publicly available) $MMSI_{SIGNER}$ (or the pseudo- $MMSI_{SIGNER}$) of the sender and the mIBC Public Parameters (mIBC-PP). The *verifier* may be any equipment (hardware/software) that can receive AIS data directly (e.g. an AIS device) or forwarded AIS data via satellites or the internet (e.g., special software on law enforcement units, port-authorities, shipping companies, etc.). The operation is as follows:

Input:
1 The signed message triplet $(AIS_{data}, h, S) \in \{0,1\}^{length} \times Z_q \times G_1$
2 The official Public Parameters, mIBC-PP = (G_1, G_2, G_T, e, P_{G1}, P_{G2}, M_{PUB}, e (P_{G1}, P_{G2}), φ, H_1, H_2), *Note: H_3, H_4, H_5 are not used in this operation.*
3 the $MMSI_{SIGNER}$

Compute:
1 $u = e(S, H_1(MMSI_{SIGNER}) P_{G1} + M_{PUB}) e(P_{G1}, P_{G2})^{h}$
2 Verification: Signature is *Valid* if $h = H_2(AIS_{data}, u)$ and *Invalid* otherwise.

Output:
1 Valid or Invalid signature, and accordingly valid or invalid AIS-data.

4.3.2 *mIBC-SK-IBE-AIS (mode 4)*

The sender/transmitter uses the Public Parameters of the mIBC and the $MMSI_{RECEIVER}$ to encrypt the AIS_{data} (that can be an AES_{Key}), and transmits the ciphertext via a typical AIS device. The encryption operation steps are as follows:

Input:
1 The clear text $AIS_{data} \in \{0,1\}^{length}$,(length = length of the cleartext in bits
2 The official Public Parameters, mIBC-PP = (G_1, G_2, G_T, e, P_{G1}, P_{G2} M_{PUB}, e(P_{G1}, P_{G2}), φ, H_1, H_3, H_4, H_5)
3 A random integer $\sigma \in \{0,1\}^{length}$, generated with the R_1 Generator of random numbers.
4 the $MMSI_{RECEIVER}$ of the receiver in $\{0,1\}^*$

Compute:
1 Compute $r = H_4(\sigma, AIS_{data})$
2 Compute $g^r = e(P_{G1}, P_{G2})^r$
3 Compute $U = r(H_1(MMSI_{RECEIVER}) P_{G1} + M_{PUB})$
4 Compute $V = \sigma \circledcirc H_3(g^r)$
5 Compute $W = AIS_{data} \circledcirc H_5(\sigma)$
6 Ciphertext $c = (r Q_A, \sigma \circledcirc H_3(g^r), AIS_{data} \circledcirc H_5(\sigma)) \in G_1 \times \{0,1\}^{length} \times \{0,1\}^{length}$

Output:
1 The Ciphertext is the triplet $c = (U, V, W) \in G_1 \times \{0,1\}^{length} \times \{0,1\}^{length}$

All the AIS-enabled devices in range can receive the encrypted data, but only the receiver who knows the mIBC Private (Secret) key corresponding to the $MMSI_{RECEIVER}$ can decrypt the data. The steps are as follows:

Input:
1 The official Public Parameters, mIBC-PP = (G_1, G_2, G_T, e, P_{G1}, P_{G2} M_{PUB}, e(P_{G1}, P_{G2}), φ, H_1, H_3, H_4, H_5)
2 The Private (Secret) $Key_{RECEIVER}$ ($SK_{RECEIVER} \in G_2$)
3 The ciphertext c = (U, V, W)

Compute:
1 Compute $g = e(U, SK_{RECEIVER})$
2 Compute $\sigma = V \circledcirc H_3(g)$
3 Compute clear text $AIS_{data} = W \circledcirc H_5(\sigma)$
4 Compute $r = H_4(\sigma, AIS_{data})$

Output:
1 Valid if $U = r(H_1(MMSI_{RECEIVER}) P_{G1} + M_{PUB})$ else received data is not valid

4.3.3 *mIBC-AES-AIS (mode 5) with symmetric cryptography*

The use of encrypted AIS between the vessels of a so-called "blue-force" is not new and commercial products that implement it using symmetric cryptography exist. Nevertheless, they provide proprietary encrypted AIS only in vessels equipped with the same AIS product. For example, the SAAB R5 Supreme W-AIS System supports the DES, AIS, and Blowfish symmetric ciphers. Another example of an approach that is compatible with our work is the Encrypted Automatic Identification System (EAIS) proposed by the United States Coast Guard in [33]. Our innovation is the use of the mIBC-SK-IBE-AIS (mode 4) for disseminating the symmetric key to allow the maritime community and law enforcement units to create ad-hoc "blue forces," or *AIS Ad-hoc NETworks* (AISANETs) [1]. Following the analysis in [33], the 128-bit AES key is sufficient for Encrypted-AIS data between the members of a law-enforcement "blue-force". However, "blue-forces" tend to use strong combinations of ciphers and key sizes, because the symmetric key in the current approach is generated once, it is pre-loaded on the AIS devices, and it is expected to be secure for a time-period far longer than a day or two. On the other hand, our approach for the AIS Ad-hoc NETworks (AISANETs) uses a symmetric key only for a period of some hours, and then a new key will be generated and disseminated to the participating vessels.

5 MIBC-AIS MESSAGES

mIBC needs to be as transparent as possible to current AIS implementations. Therefore, new mIBC-AIS modes should not alter the currently used AIS protocol. To achieve this goal we introduce a new application, named "mIBC-AIS-App", described in section 5.3, to be used as an interface to implement the mIBC-AIS scheme over the currently available AIS infrastructure. It is important to note that we use the AIS protocol only as the underlying transportation carrier protocol to transmit the signed/encrypted mIBC-AIS Data of mIBC. In particular, mIBC-AIS data are encapsulated by the mIBC-AIS-App in the data payload subsection of existing AIS messages with ID 6 and ID 8. As we shall see, the latter are special AIS messages that permit the encapsulation of data of non-AIS dependent, arbitrary applications. The sender mIBC-AIS-App creates the appropriate mIBC-Data and then encapsulates it into the special AIS messages (ID 6, 8) that are transmitted via the standard AIS infrastructure. On the other end, the receiver mIBC-AIS-App decapsulates and processes the received mIBC-Data. This is analogous to the encapsulation of the Transmission Control Protocol (TCP) data inside the Internet Protocol (IP) packets.

5.1 *AIS message structure*

AIS defines 27 different types of AIS messages that are identified by their *Message-ID* [2]. Messages with Message-ID 1, 2, and 3 are Position Reports, Messages with Message-ID 4 are Base Station Reports, Messages with Message-ID 21 are Aid-to-Navigation (AtoN) AIS station Reports etc. Each AIS message may use one to five timeslots. The available payload data in each timeslot is 168 bits, and there exist AIS message types (e.g. "AIS ADDRESSED BINARY MESSAGE" (MESSAGE ID: 6) and "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID: 8)) that may use the maximum of the 5 timeslots i.e. just over 900 bits of payload data. AIS messages are also classified according to their priority (1 to 5) in the timeslot sequence. The majority of the AIS messages with priority one, occupy only one timeslot i.e. 168 bits of payload data. A notable exception is the AIS AIDS TO NAVIGATION (ATON) REPORT (MESSAGE ID21) that needs 272-360 bits.

Table 1. Example of a typical CLASS A AIS POSITION REPORT (MESSAGE ID: 1) Structure. Adapted from [2]

Parameter	Bits	Description
Message ID	6	Identifier for this message 1 3
User ID	30	MMSI number
Navigational status	4	0 = under way using engine, 1 = at anchor, 2 = not under command, 3 = restricted maneuverability, etc.
The rate of turn ROT_{AIS}	8	0 to +126 = turning right at up to 708 deg per min or higher, etc.
SOG	10	Speed over ground in 1/10 knot steps (0-102.2 knots)
Position accuracy	1	The position accuracy (PA) flag 1 = high (<= 10 m), 0 = low (> 10 m), 0 = default
Longitude	28	Longitude in 1/10 000 min …
Latitude	27	Latitude in 1/10 000 min …
COG	12	Course over ground in 1/10 = (0-3599). 3600 (E10h) = not available = default. 3 601-4 095 should not be used
True heading	9	Degrees (0-359) (511 indicates not available = default)
Timestamp	6	UTC second when the report was generated by the electronic position system (EPFS)
Special maneuver indicator	2	0 = not available = default, 1 = not engaged in special maneuver,2 = engaged in special maneuver
Spare	3	Not used. Should be set to zero. Reserved for future use.
RAIM-flag	1	Receiver autonomous integrity monitoring (RAIM) flag of the electronic position fixing device;
Communica-tion state	19	See Rec. ITU-R M.1371-5 Table 49
Total number of bits		168

The AIS standard dictates the exact structure of each message. The structure includes generic parameters (fields) found in all AIS messages (e.g. Message ID (max 6 bits), MMSI number (max 30 bits), etc.) and message-specific parameters (e.g. Timestamp (max 6 bits), Navigational status (max 5 its), Rate of turn (max 8 bits), etc.). Note that each parameter has a defined maximum size. AIS messages include a Timestamp (6 bits long) that is the Coordinated Universal Time (UTC) second when the report was generated by the electronic position fixing system (EPFS). An example of the structure of a typical Class A AIS position report message (MESSAGE ID21) is shown in Table 1.

5.2 *mIBC-AIS Messages*

Two AIS messages, namely Message ID6 and Message ID8 are particularly interesting for the transmission of the signed/encrypted AIS data from/to the mIBC-AIS-App. Their useful characteristic is the existence of an isolated data payload subsection that registered applications, not related to AIS, may use to transport their data [2]. Specifically, Message ID6 and Message ID8 allocate their Binary Data parameter packet section as follows: a) 16 bits as Application Identifier and b) 920/952 bits for Arbitrary Application Data payload for registered applications. Thus, the mIBC-AIS-App can be registered as an add-on AIS application with a unique ID and the Application Data payload of Message ID6 and Message ID8 can be used for the transport of mIBC-AIS-App data.

The "AIS ADDRESSED BINARY MESSAGE" (MESSAGE ID6) offers a maximum of 920 bits space for arbitrary application data addressed to a specific receiver (i.e., all the AIS devices that will not have the specific addressed MMSI will discard the received message ID6). Table 2 depicts a typical AIS ADDRESSED BINARY MESSAGE (MESSAGE ID6) with mIBC-AIS-App data encapsulated in its "Binary Data" section. This section includes two subsections to be used for the transmission of the mIBC-AIS data necessary for the implementation of secure AIS mode 4. According to the AIS specifications for Message ID6, only the application denoted by its ID in the "Application identifier" subsection is responsible for the encapsulated data inside the "Application data" subsection. Therefore, we use the "Application identifier" to denote the mIBC-AIS-App as the responsible application for the mIBC-AIS-Data encapsulated inside the "Application data" subsection. Because the standard AIS infrastructure does not interact with the data payload stored inside the "Binary Data" section of the Message ID6, the encapsulated mIBC-AIS data are isolated.

An identical approach can be followed for the transparent transmission of the mIBC-AIS data with the "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID8). The "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID8) offers a maximum of 952 bits space to broadcast arbitrary application payload data. This type of AIS message is used to transfer data necessary for the implementation of Secure AIS modes 2, 3, and 5. The structure of the AIS BROADCAST BINARY MESSAGE (MESSAGE ID8), as shown in Table 3, is identical with that of Message ID6, with the notable exception that the "Destination ID" section is absent in the (broadcast) Message ID8, resulting in a savings of 30 bits. The isolation of the encapsulated mIBC-AIS data payloads makes the proposed mIBC-AIS implementation transparent to the current standard AIS infrastructure.

Table 2. The structure of the AIS ADDRESSED BINARY MESSAGE (MESSAGE ID: 6). Adapted from [2]

Parameter	Number of bits	Description		
Message ID	6	Identifier for Message 6		
Repeat indicator	2	Indicates how many times a message has been repeated, 0-3; default = 0; 3 = do not repeat any more		
Source ID	30	MMSI number of the source station		
Sequence number	2	0-3		
Destination ID	30	MMSI number of the destination station. Note: This section does not exist on "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID: 8))		
Retransmit flag	1	Retransmit flag should be set upon retransmission: 0 = no retransmission = default; 1 = retransmitted		
Spare	1	Not used. Should be zero. Reserved for future use		
Binary data	Maximum 936	Application identifier	16 bits	*mIBC-AIS-App ID*
		Application data	Maximum 920 bits	Application specific Encapsulated data : *SK-Identity Based Encryption, mIBC-SK-IBE-AIS (mode 4)*
Maximum number of bits	Maximum 1 008	Occupies up to 3 slots, or up to 5 slots when able to use FATDMA reservations.		

Table 3. The structure of the AIS ADDRESSED BINARY MESSAGE (MESSAGE ID: 8) structure. Adapted from [2]

Parameter	Number of bits	Description		
Message ID	8	Identifier for Message 8		
Repeat indicator	2	Indicates how many times a message has been repeated, 0-3; default = 0; 3 = do not repeat any more		
Source ID	30	MMSI number of the source station		
Sequence number	2	0-3		
Retransmit flag	1	Retransmit flag should be set upon retransmission: 0 = no retransmission = default; 1 = retransmitted		
Spare	1	Not used. Should be zero. Reserved for future use		
Binary data	Maximum 936	Application identifier	16 bits	*mIBC-AIS-App ID*
		Application data	Maximum 920 bits	Application specific Encapsulated data: *"mIBC-Authenticated-AIS" (mode 2)* *"Anonymous-AIS" (mode 3)* *mIBC-AES-AIS (mode 5)*
Maximum number of bits	Maximum 1 008	Occupies up to 3 slots, or up to 5 slots when able to use FATDMA reservations.		

Table 4. Structure of the 1st "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID 8) encapsulating a CLASS A AIS POSITION REPORT (MESSAGE 1) in mIBC-Authenticated-AIS (mode 2)

Parameter	Number of bits	Description		
Message ID	6	Identifier for Message 8; always 8		
Source ID	30	MMSI number of the source station		
Binary data	Maximum 960	Application ID	16 bits	mIBC-AIS-App registration ID
		Application data	Maximum 952 bits	mIBC-AIS-App in mIBC-Authenticated-AIS (mode 2) DATA - Part 1 / 2 a) Adds encoded in Spare parameter (3bits) of AIS_{data} the total expected parts (i.e., in this example the Spare parameter will be two (2) b) Authenticated AIS_{data} is the data in parameters of CLASS A AIS POSITION REPORT (MESSAGES 1)) (max 168 bits). For security reasons we include in the AIS_{data} the identification data (e.g., MMSI) of the vessel and the timestamp of the signed Message-ID:1 c) 1st part of the Signature (h, S) of the original AIS_{data} Note: mIBC-AIS-App computes the total size of the AISdata + Signature (h, S) and determines how many Messages ID: 8 (i.e., Parts) have to transmit. (For completeness in this example we assume that the overall size of AISdata + Signature (h, S) exceeds the maximum size of a MESSAGE-ID: 8 and two parts are needed)

Table 5 Structure of the 2nd "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID 8) encapsulating a CLASS A AIS POSITION REPORT (MESSAGE 1) in mIBC-Authenticated-AIS (mode 2).

Parameter	Number of bits	Description		
Message ID	6	Identifier for Message 8; always 8		
Source ID	30	MMSI number of the source station		
Binary data	Maximum 960	Application ID	16 bits	mIBC-AIS-App ID
		Application data	Maximum 952 bits	mIBC-AIS-App in Authentication (mode 2) DATA - Part 2 / 2 *(In the 2nd part the remaining bits of the Signature (h, S) are transmitted.)* 2nd part of the Signature (h, S) bits *(The size of the remaining bits may need less than 5 time-slots.*

Table 6. Structure of the 1st "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID 6) encapsulating a 128bit AES key in mIBC-SK-IBE-AIS (mode 4)

Parameter	Number of bits	Description		
Message ID	6	Identifier for Message 6; always 6		
Source ID	30	MMSI number of the source station		
Destination ID	30	MMSI number of the destination station		
Binary data	Maximum 936	Application ID	16 bits	mIBC-IBE-App registration ID
		Application data	Maximum 920 bits	mIBC-SK-IBE-AIS (mode 4) DATA payload: Ciphertext triplet (U, V, W) (1st part)

Table 7. Structure of a "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID 8) in mIBC-AES-AIS (mode 5)

Parameter	Number of bits	Description		
Message ID	6	Identifier for Message 8; always 8		Unencrypted
Source ID	30	MMSI number of the source station		Unencrypted
Spare	3	Information about the encryption parameters coded and added to the Spare parameter (3bits) of original AIS_{data}. (e.g. Spare value = 010 may imply AES-128 in CBC mode)		Unencrypted
Binary data	Maximum 960	Application ID	mIBC-AIS-App in Encryption (mode 5) registration ID	Unencrypted
		Application data	mIBC-AIS-App in Encryption (mode 5) DATA AIS_{data}	Unencrypted ENCRYPTED

A mIBC-Authenticated-AIS (mode 2) message is a broadcasting transmission that we encapsulate inside a typical "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID 8), which offers a maximum of 952 bits space for arbitrary application data. If we use MNT curves, with a 128 bit key, the signature alone is 768 bits long; this allows for a useful payload of 168 bits for the original AIS data. The majority of the typical "priority" AIS messages broadcasted by the AIS are shorter than 168 bits. Hence, it is feasible to encapsulate them, together with their mIBC-AIS Signature, inside a single "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID 8). Unfortunately, there are important AIS messages, such as the AIDS TO NAVIGATION (ATON) REPORT (MESSAGE 21), that need 272 – 360 bits of space; these cannot be encapsulated together with their signature inside one "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID 8). Besides, a higher mIBC security level may use cryptographic parameters that will yield longer signatures which would be impossible to encapsulate within only one MESSAGE ID 8. To resolve this, the proposed implementation provides for the partition of the signature and the original AIS data into multiple "AIS BINARY BROADCAST MESSAGE" (MESSAGE ID 8) messages, as in Figure 2. The mIBC-AIS-App at the two ends of the communication channel is responsible for the appropriate partition and reconstruction of the signature and of the original AIS data into the multiple ID8 messages.

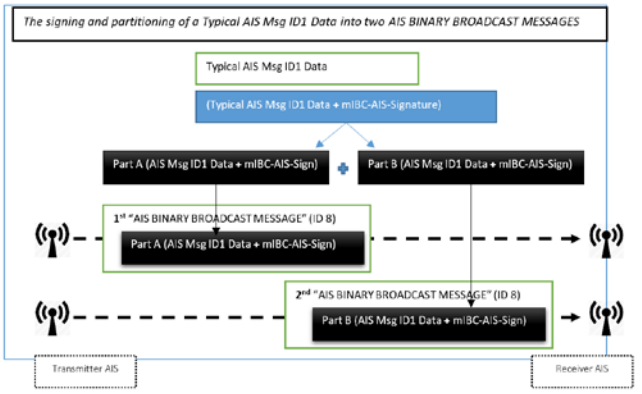

Figure 2. The signing and partitioning of a Typical AIS Msg ID1 Data into two AIS BINARY BROADCAST MESSAGES (ID 8) in mIBC-Authenticated-AIS (mode 2)

The first and second messages are structured as in Tables 4 and 5 respectively. In the interest of saving space, non mIBC-relevant parameters are omitted.

As will be seen in the next section, the overhead bandwidth for the mIBC-SK-IBE-AIS (mode 4) encryption is considerable. This is why we propose to use mIBC-SK-IBE-AIS (mode 4) mainly for the dissemination of the new AES symmetric keys of the mIBC-AES-AIS (mode 5). We believe that the 128-AES algorithm with a key length of 128 bits provides more than adequate security for the AIS in insecure areas. Bear in mind that in our case we do not need to store secret data for years but only to protect AIS transmitted data for hours or up to a few days. In this case, the ciphertext will be almost equal with the key,

i.e. 128bits long. The AIS ADDRESSED BINARY MESSAGE (MESSAGE ID: 6) has 920bits data payload; therefore, at most two AIS ADDRESSED BINARY MESSAGES (MESSAGE ID: 6) with over 1800 bits of combined payload packets will be enough to transfer the mIBC-SK-IBE-AIS (mode 4) data. The message partitioning details are identical to the Message(s) construction for the mIBC- Authenticated-AIS (mode 2), shown in Figure 1. The structure of the 1st "AIS ADDRESSED BROADCAST MESSAGE" (MESSAGE ID 6) encapsulating a 128bit AES key in mIBC-SK-IBE-AIS (mode 4), is shown in Table 6. Note that the mIBC-AIS-App computes the total size of the AESKey + encrypted Ciphertext triplet (U, V, W) and determines how many Messages ID:6 (i.e., Parts) have to be transmitted. The remaining parts of the signed and encrypted output triplet (c, S, T) will be transmitted with additional AIS ADDRESSED BINARY MESSAGE (MESSAGE ID: 6).

A possible encrypted AIS Message structure via the mIBC-AIS-App in Encryption (mode 5) is shown in Table 7. Non mIBC-relevant parameters are omitted. Note that the mIBC-AIS-App computes the total size of the Encrypted AISdata. Depending on the symmetric cipher (e.g., AES128) the mode (e.g., CBC, CTR) and other parameters, the overhead varies from 16 bytes (e.g. for the IV (Initial Value) plus the padding (e.g. 1 to 16 bytes for PKCS#5 padding) if we use the CBC mode. Therefore, for a standard AIS message, one AIS BROADCAST BINARY MESSAGE (MESSAGE ID: 8) (i.e., 1 to 5 slots) suffices.

5.3 *The mIBC-AIS-App*

The mIBC-AIS-App is a piece of code that may be implemented either as a firmware update on current AIS devices or on separate hardware to be connected between the AIS device and the AIS antenna. In either case, the mIBC- AIS-App will be an intermediate between the currently running AIS and the AIS antenna of the vessel. The mIBC-AIS-App assumes sole responsibility for the transmission of all mIBC enabled AIS messages. It intercepts the AIS messages, exports their data, cryptographically manipulates them, encapsulates them in AIS Messages ID6 and/or ID8 and forwards them to the AIS antenna.

In particular, the mIBC-AIS-App:

1 Forwards the typical AIS messages unaltered to the AIS antenna/AIS device, respectively, when in mIBC-Standard-AIS (mode-1) usage mode.
2 Implements the mIBC-AIS modes 2, 3, 4, 5 by:
3 Stores (or accesses) the cryptographic parameters (i.e., Public Parameters, MMSI or Pseudo-MMSI, mIBC key-pair of the vessel);
4 Carries out all the cryptographic operations, computations and procedures.
5 Forwards the outcome of the cryptographic operations/computations of the received signed/encrypted AIS data to the appropriate end devices, i.e. AIS or ECDS displays or any other compatible software/hardware of the vessel.
6 Encapsulates/Decapsulates the mIBC-AIS data to/from AIS Messages ID6 and ID8.

Figures 3 and 4 depict the use of the mIBC-AIS-App and its interaction with the AIS devices. In Figure 3 the mIBC-AIS-App is switched to mIBC-Standard-AIS (mode 1) and thus does not interfere with the AIS operation. The Transmitter-AIS device transmits -via a standard AIS Message ID1- the collected static, voyage, positional and navigational data of the vessel. The Receiver-AIS device receives the AIS data and displays them to the appropriate navigational equipment. In both cases, the mIBC-AIS-App forwards the Original Message ID1 without altering it. In mIBC-Standard-AIS (mode 1) all AIS messages are forwarded un-altered by the mIBC-AIS-App. In contrast, in Figure 4 the mIBC-AIS-App is switched to one of the AIS secure modes (i.e. modes 2-5). The Transmitter-AIS device collects static, voyage, positional and navigational data of the vessels and creates a standard AIS positional AIS Message ID1. The mIBC-AIS-App of the transmitter: a) Intercepts the AIS positional AIS Message ID1 before its transmission; b) Reads the data of the AIS Message ID1; c) Signs or Encrypts the appropriate data according to the mIBC-AIS usage mode; d) Encapsulates the Signed/Encrypted data inside the "Application data" section of the Messages ID6 and/or ID8; e) Transmits -via the AIS antenna- the newly created Messages ID6 and/or ID8. On the receiver side, the mIBC-AIS-App: a) Intercepts the Messages ID6 and/or ID8 received by the AIS antenna; b) Decapsulates and concatenates the mIBC data from each received Message ID6 and/or ID8; B) Verifies or Decrypts the received mIBC data according to the mIBC-AIS usage mode; c) Reconstructs and Forwards to the Receiver AIS device the original AIS Message ID1; d) The original AIS Message ID1 is displayed on the navigational equipment of the vessel.

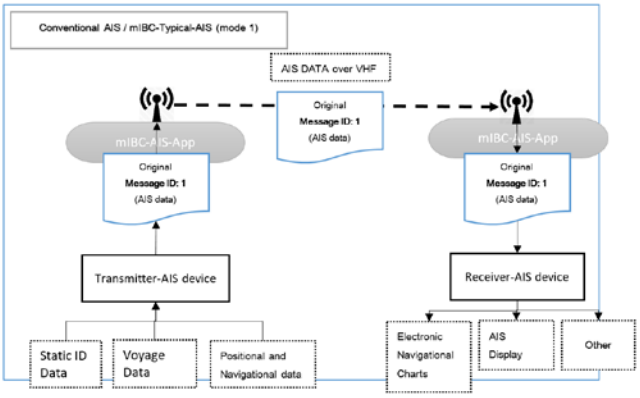

Figure 3. Conventional AIS and the mIBC-Typical-AIS (mode 1)

An attacker is unable to spoof or decrypt the transmitted Message ID6 and/or ID8 created by the mIBC-AIS-App. At the same time the mIBC-AIS-App operations remain transparent to the crew, and the navigational equipment of the ship. The result is that in the mIBC-Standard-AIS (mode 1), an interceptor of the AIS messages may see all kinds of the Message IDs as it can today. In the mIBC-AIS secure modes of operation, an interceptor may see only AIS Messages ID6 and/or ID8 that contain mIBC-AIS data payloads.

6 MIBC OPERATIONAL OVERHEAD

6.1 *mIBC-Authenticated-AIS (mode 2) overhead*

The operational overhead imposed by the mIBC is proportional to the chosen security level. Stronger security implies larger cryptographic parameters that in turn imply a more considerable computational and bandwidth overhead. Herein we present operational overhead estimates that are based mainly on the work in [32] and in [31].

6.1.1 *Bandwidth overhead estimates*

As mIBC-Authenticated-AIS (mode 2) bandwidth overhead we define the additional bits needed for signing the original AIS data. The signature is the cryptographic tuple (h, S) ϵ Z_q x G_1; therefore the additional bandwidth overhead is the sum of the length of h (in bits) plus the length of S (in bits). According to table 7 [32], we estimate the sizes of Z_q and G, with "point compression" on Super Singular (SS) curves at 80 bit security, MNT curves at 80 bit security and MNT curves at 128 bit security.

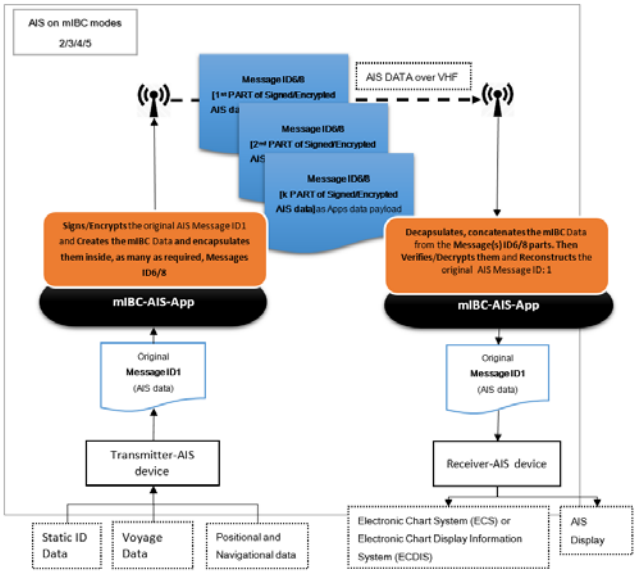

Figure 4. The mIBC-AIS in security modes 2/3/4/5.

Table 7. mIBC-Authenticated-AIS (mode 2) bandwidth overhead estimates

	Super Singular (SS) curves at 80 bit security	MNT at 80 bit security	MNT at 128 bit security
h ϵ Z_q	160 bits	160 bits	256 bits
S ϵ G_1	512 bits	171 bits	512
The estimated bandwidth overhead is the sum (h + S)			
	672 bits	**331 bits**	**768 bits**

6.1.2 *Computational overhead estimates*

All the participating entities in the mIBC infrastructure have plenty of computational power, and thus the computational overhead should not be a problem. However, as an example, we present the following computational overhead estimates. In general, the majority of the computational overhead comparison methodologies count the separate mathematical operations needed in each IBC proposed implementation. The mathematical operations are exponentiations, scalar point multiplications, and pairing evaluations. In the proposed IBC scheme the signing process uses two scalar point multiplications and the verification process one scalar point multiplication and one pairing evaluation. Thus according to [31], the above implementation needs 1.56 milliseconds to sign a message, and 3.60 milliseconds to verify a signature. However, we must take into account that [31] was published back in 2005 and used C++ based implementations on an Athlon XP at 2GHz to compute the authentication and signcryption schemes under a supersingular curve (SS) of embedding degree k=6 over $F_{3^{97}}$. It is expected that modern technology will achieve far better speeds.

6.2 *mIBC-SK-IBE-AIS (mode 4) overhead*

Our estimates are based on the work in [32] and in [31]. We highlight that in case where the confidential transmitted data is a symmetric key (i.e., AES_{Key}) the security level offered by mIBC-SK-IBE-AIS (mode 4) should be equal with the security level offered by the disseminated AES key. In general, the security level of a hybrid cryptographic scheme is the minimum between the level of the security offered by the cryptographic key and the security level of the mechanism that disseminates that cryptographic key.

6.2.1 *Bandwidth overhead estimates*

The bandwidth overhead is the bits additional to cleartext AIS data required to be transmitted for each mIBC-SK-IBE-AIS (mode 4) confidential data transmission. The transmitted encrypted data is the triplet ciphertext (c) = (U, V, W) ϵ G_1 x $\{0,1\}^{length}$x $\{0,1\}^{length}$. According to table 8 [32], we estimate the bandwidth overhead, with "point compression" on Super Singular (SS) curves at 80bit security, MNT at 80 bit security and MNT at 128 bit security.

Table 8. Estimated bandwidth overhead for the mIBC-SK-IBE-AIS (mode 4) messages

	Super Singular (SS) curves at 80bit security	MNT at 80bit security	MNT at 128bit security
Public Parameters (not transmitted via mIBC-AIS, thus do not add in mIBC-AIS bandwidth overhead)	2048 bits	1368 bits	4096 bits
Ciphertext (excluding msg.) mIBC-AIS overhead bandwidth	672 bits	331 bits	768 bits

The same conditions stand here as in the example for authentication in section 6.1.2. The general computational overhead estimates presented here are based on the work in [32]. In [32] the indicative sizes with "point compression" optimizations for G_1, G_2, G_T and Z_p groups for standard elliptic curves types are given. These values are for Super-Singular (SS) elliptic curve at 80-bit security: Z_p=160 bits, G_1=512 bits, G_2=512 bits, G_T=1024 bits. For MNT elliptic curve at

128-bit security: Z_p=256 bits, G_1=512 bits, G_2=3072 bits, G_T=3072 bits. Also [32] defines an "indicative" time-unit as the time needed for point multiplication on a random 171-bit elliptic curve for a random 160-bit exponent. Under the above settings, the following indicative results for SK-IBE are derived: For Super-Singular (SS) elliptic curve at 80-bit security: Secret (Private) key extraction costs 2-time units, encryption costs 6-time units and decryption costs 104-time units. For MNT elliptic curve at 128-bit security: Secret (Private) key extraction costs 100-time units, encryption costs 36-time units and decryption costs 1506 time units. Finally, the BLMQ Signcryption scheme that has similar characteristics needs 2.65 milliseconds to Sign and Encrypt for one group exponentiation and two scalar point multiplications [31]. The processing time for Decryption and Verification is 6.09 milliseconds for one group exponentiation and two pairing evaluations.

7 CONCLUSION

In our previous work [1] we introduced the concept of a secure AIS founded on Identity Based Cryptography. In this work, we focused on proving the feasibility of our idea by describing a working model based on specific AIS attributes and specific Identity Based Cryptographic schemes. We have proposed a Maritime Identity Based Cryptographic infrastructure (mIBC) under the IMO. We described five usage modes for the proposed secure mIBC-AIS. The mIBC-Typical-AIS (mode 1) works like the typical AIS; it is the default mIBC-AIS usage mode. The mIBC- Authenticated-AIS (mode 2) enhances AIS transmissions with source authentication capabilities; its implementation is based on the BLMQ identity-based signatures operations formalized in the IEEE 1363.3-2013 standard. The mIBC-Anonymous-AIS (mode 3) uses Pseudo-MMSIs to provide AIS with anonymity, as described in detail in [1]. When in mIBC-SK-IBE-AIS (mode 4) usage mode, the mIBC-AIS can send arbitrary encrypted data to any entity under mIBC without any previous contact or pre-configuration with the receiver entity. For the implementation of the mIBC-SK-IBE-AIS (mode 4), we used the security proof of Sakai-Kasahara's Identity-Based Encryption scheme in [19]. The last usage mode is the mIBC-AES-AIS (mode 5), which provides for Encrypted AIS secure (group)-communication with symmetric cryptography (e.g., AES). Today, encrypted AIS with symmetric ciphers (e.g., AES) is offered by various vendors of commercial AIS devices but always for pre-defined "blue-forces" that they use pre-installed symmetric AES keys. In contrast, we use the mIBC-SK-IBE-AIS (mode 4) to disseminate the symmetric AES keys of the mIBC-AES-AIS (mode 5), to any trustworthy entity, ad-hoc, without any pre-communication or symmetric-key pre-installation. Responsible for the proposed mIBC-AIS functionality is the mIBC-AIS-App intermediate application, that lies between the typical AIS devise and its AIS antenna. The mIBC-AIS-App is responsible for intercepting the original AIS data, to perform the cryptographic operations and to encapsulate/decapsulate the mIBC-AIS data into standard AIS Messages ID6/8 as arbitrary data payloads. In this way, the implementation of the mIBC-AIS uses the currently available AIS infrastructure but does not directly interact with it. This enables the mIBC-AIS to be a transparent add-on to the currently available AIS infrastructure. We conclude that a practical implementation of our approach is feasible. We intend to proceed with a prototype implementation of the proposed scheme, including the mIBC-App, and to experiment with it in order to assess its performance.

REFERENCES

[1] A. Goudossis and S. Katsikas, "Towards a secure automatic identification system (AIS)," *Journal of Marine Science and Technology,* vol. 24, no. 2, pp. 410-423, 2019.

[2] U. C. G. N. Center, "HOW AIS WORKS," U.S. Coast Guard Navigation Center , 09 08 2016. [Online]. Available: https://www.navcen.uscg.gov/?pageName=AISworks. [Accessed 02 08 2019].

[3] U. C. G. N. Center, "AIS CLASS A SHIP STATIC AND VOYAGE RELATED DATA (MESSAGE 5)," U.S. Coast Guard Navigation Center, 16 11 2017. [Online]. Available: https://www.navcen.uscg.gov/?pageName=AISMessagesAStatic. [Accessed 02 08 2019].

[4] B. Ellison, "Mandated AIS, an aid to pirates?," Panbo, 2019. [Online]. Available: https://www.panbo.com/mandated-ais-an-aid-to-pirates/. [Accessed 02 08 2019].

[5] C. Guarnieri, "Should ship data be open to the public?," Verdict Media Limited, 25 06 2013. [Online]. Available: https://www.ship-technology.com/features/featureship-data-be-open-public-security/. [Accessed 02 08 2019].

[6] M. Balduzzi, K. Wilhoit and A. Pasta, "A Security Evaluation of AIS," Trend Micro.

[7] I. M. O. (IMO), "Maritime Security and Piracy," International Maritime Organization (IMO), [Online]. Available: http://www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx. [Accessed 02 08 2019].

[8] G. Kessler, Craiger, J.P. and J. Haass, "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation,* vol. 12, no. 3, pp. 429-437, 2018.

[9] F. Lazaro, R. Raulefs, W. Wang, F. Clazzer and S. Plass, "VHF Data Exchange System (VDES): an enabling technology for maritime communications," *CEAS Space Journal,* vol. 11, no. 1, pp. 55-63, 2019.

[10] J. Hall, J. Lee, J. Benin, C. Armstrong and H. Owen, "IEEE 1609 influenced automatic identification system (AIS)," in *IEEE Vehicular Technology Conference*, Glasgow, UK, 2015.

[11] I. M. Organization, *Resolution A.1106(29), IMO REVISED GUIDELINES FOR THE ONBOARD OPERATIONAL USE OF SHIPBORNE AUTOMATIC IDENTIFICATION SYSTEMS (AIS),* International Maritime Organization, 2015.

[12] A. Goudosis, T. Kostis and N. Nikitakos, "Automatic Identification System Stated Requirements for Naval Transponder Security Assurance," in *N. Goudosis, A ; Kostis, T ; Nikitakos, "Automatic Identification System Stated Requirements for Naval Transponder 2nd International Conference on Applications of Mathematics & Informatics In Military Sciences (AMIMS)*, Vari, Greece, 2012.

[13] D. He, N. Kumar, K.-K. R. Choo and W. Wu, "Efficient Hierarchical Identity-Based Signature with Batch Verification for Automatic Dependent Surveillance-

Broadcast System," *IEEE Transactions on Information Forensics and Security,* vol. 12, no. 2, pp. 454 - 464, 2017.
[14] J. Baek, E. Hableel, Y.-J. Byon, D. Wong, K. Jang and H. Yeo, "How to Protect ADS-B : Confidentiality Framework and Efficient Realization Based on Staged Identity-Based Encryption," *IEEE Transactions on Intelligent Transportation Systems,* vol. 18, no. 3, pp. 690-700, 2017.
[15] IALA, "e-Navigation," IALA AISM, [Online]. Available: https://www.iala-aism.org/technical/e-navigation/. [Accessed 02 08 2019].
[16] SAAB, "NETWORKED SECURE W-AIS TRANSPONDER FOR OPERATIONAL SECURITY," [Online]. Available: http://saab.com/security/maritime-traffic-management/traffic-management/R5-Supreme-W-AIS/. [Accessed 5 November 2017].
[17] M. Strohmeier, V. Lenders and I. Martinovic, "On the security of the automatic dependent surveillance-broadcast protocol," *IEEE Communications Surveys and Tutorials,* vol. 17, no. 2, p. 1066–1087, 2015.
[18] R. Sakai and M. Kasahara, "ID based Cryptosystems with Pairing on Elliptic Curve," Cryptology ePrint Archive, 2003.
[19] L. Chen and Z. Cheng, "Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme," *Cryptography and Coding,* vol. vol. 3796, p. 442–459, 2005.
[20] IEEE, *IEEE 1363.3-2013 - IEEE Standard for Identity-Based Cryptographic Techniques using Pairings,* IEEE, 2013.
[21] E. Barker, "Recommendation for Key Management Part 1: General. NIST Spec. Publ. 800-57 Part 1 Revis. 4.," NIST, 2016.
[22] S. Zhao, A. Aggarwal, R. Frost and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Communications Surveys and Tutorials,* vol. 14, no. 2, p. 380–399, 2012.
[23] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei and P. Papadimitratos, "VeSPA," in *2nd ACM Workshop on Hot Topics of Wireless Networks Security and Privacy - HotWiSec '13*, Budapest, Hungary, 2013.
[24] IEEE, *1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages,* IEEE, 2016.
[25] A. Shamir, "Identity-Based Cryptosystems and signature schemes," in *CRYPT0 '84*, 1984.
[26] R. Perlman, "An overview of PKI trust models," *IEEE Networks,* vol. 13, no. 6, p. 38–43, 1999.
[27] Y. Fang, X. Zhu and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," *IEEE Wireless Communications,* vol. 16, no. 2, pp. 24-30, 2009.
[28] Y. Zhou, Y. Fang and Y. Zhang, "Securing wireless sensor networks: a survey," *IEEE Communications Surveys & Tutorials,* vol. 10, no. 3, pp. 6-28, 2008.
[29] M. Bohio and A. Miri, "Efficient identity-based security schemes for ad hoc network routing protocols," *Ad Hoc Networks,* vol. 2, no. 3, p. 309–317, 2004.
[30] Federal Information Processing Standards,, *ADVANCED ENCRYPTION STANDARD (AES),* Federal Information Processing Standards, 2001.
[31] P. S. L. M. Barreto, B. Libert, N. McCullagh and J. Quisquater, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps," in *International Conference on the Theory and Application of Cryptology and Information Security*, 2005.
[32] X. Boyen, "A tapestry of identity-based encryption: practical frameworks compared," *International Journal of Applied Cryptography,* vol. 1, no. 1, pp. 3-21, 2008.
[33] H. Castro, "Encrypted Automatic Identification System (EAIS) Interface Design Description (IDD)," U.S. Coast Guard (USCG), 2014.