

---

# TOWARDS A SECURE AUTOMATIC IDENTIFICATION SYSTEM (AIS)

ATHANASSIOS GOUDOSSIS<sup>1</sup> AND SOKRATIS K. KATSIKAS<sup>1,2</sup>

[a.goudosis@gmail.com](mailto:a.goudosis@gmail.com), [sokratis.katsikas@ntnu.no](mailto:sokratis.katsikas@ntnu.no)

<sup>1</sup> Systems Security Laboratory, Dept. of Digital Systems, University of Piraeus, Greece.

<sup>2</sup> Center for Cyber and Information Security, Dept. of Information Security and Communications Technology, Norwegian University of Science and Technology, Gjøvik, Norway.

## KEYWORDS

Automatic Identification System (AIS), Identity Based Public Cryptography, Symmetric cryptography, Maritime security, e-Navigation.

## ABSTRACT

The Automatic Identification System (AIS) is the emerging system for automatic traffic control and collision avoidance services in the maritime transportation sector. It is one of the cornerstone systems for improved marine domain awareness and is embedded in e-navigation, e-bridging, and autonomous ships proposals. However, AIS has some security vulnerabilities, that can be exploited to invade privacy of passengers, to launch intentional collision attacks by pirates and terrorists, etc. In this work, we explore how Identity-Based Public Cryptography and Symmetric Cryptography may enhance the security properties of the AIS.

## 1. INTRODUCTION

The International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) describes AIS as “a communications system using four worldwide channels in the VHF maritime mobile band, for the exchange of navigation data. There are numerous AIS devices, known as stations, which are identified by a unique Maritime Mobile Service Identity (MMSI) and use an international open standard to communicate. AIS stations are designed to operate autonomously (without interaction by ship or shore personnel) and may also be instructed to transmit in a different manner – for example may be interrogated (polled) or be commanded to transmit more frequently, or on a different frequency (assignment)” [1]. AIS enables the automatic exchange of shipboard data between one vessel and another and between a vessel and a shore station.

All ships of 300 Gross Tonnage (GT) and upwards engaged on international voyages; cargo ships of 500 GT and upwards not engaged on international voyages; and all passenger ships, irrespective of size, engaged on international or domestic voyages are required to be fitted with AIS, by SOLAS regulation 19 Chapter V [2]. In addition, most commercial vessels operating on American waterways are required to have AIS [3] and all EU fishing vessels of overall length exceeding 15 meters are also required to be fitted with AIS as of May 2014 [4], [5], [6].

Initially developed as a collision avoidance aid, AIS is now used for a variety of purposes: AIS can be used for exchanging information, including safety related such, between vessels within VHF range of each other or between a vessel and a shore station. It can also be used for automatic reporting in areas of mandatory and voluntary reporting. Applications such as vessel tracking [7], [8], [9]; extraction of knowledge [10]; vessel behavior identification [11], [12], [13]; anomaly detection on vessel movements [14], [15], [16]; ship surveillance, tracking and security [17]; discovery of traffic patterns [18]; traffic simulation [19]; accident analysis [20]; ship routing development [21]; near miss detection [22]; collision risk

assessment [23]; exhaust emission estimation [24]; ecological impact analysis [25]; and maritime spatial planning [26] have also been proposed.

The range of AIS at sea without repeaters is typically 20 nautical miles. However, there are many stations equipped with AIS receivers that forward eavesdropped AIS data to specialized internet sites<sup>1</sup>. In fact, the ability to easily obtain all the information on a vessel's voyage, in real time, via commercially available equipment or even on the internet differentiates AIS from other maritime traffic control and collision avoidance shipborne systems. At the same time, it makes it vulnerable to malicious attacks.

The first concerns about security vulnerabilities of the AIS arose when many seamen stated that unrestrained disclosure of the AIS broadcasted data may be an aid to sea-pirates [27], [28] or that making AIS data freely available may violate the privacy of passengers [29]. Since then, a number of security vulnerabilities of the AIS have been revealed [30], [31]. An official guidance that leaves to the captains the decision to switch off their AIS equipment in pirate high risk areas [32], may be considered as a controversial solution.

In this paper we address the issue of the security of AIS seen as an information system and we propose a solution to improve it. The concept is founded on a Maritime Certificate-less Identity-Based Public Key Cryptography infrastructure (annotated for simplicity "maritime IBC" or "mIBC"). Assuming that such a maritime IBC exists, we research the critical properties of anonymizing a vessel's AIS data by using a pseudo-MMSIs implementation. Further, we propose the ad-hoc use of encrypted AIS messages in dangerous sea areas under a Trusted Third Party coordination (e.g. UN Patrol Ship). In particular, we propose the use of symmetric key cryptography, and we use the underline Global Maritime Certificate-less Identity-Based Public Key Cryptography for the symmetric key escrow.

The remaining of the paper is structured as follows: In section 2 we present the related work. In section 3 we then describe briefly the workings of AIS; its security vulnerabilities; attacks that may be launched against the ship by exploiting these; and the resulting requirements for the secure operation of AIS. In section 4 we describe our proposal for improving the security of AIS and we show how this proposal satisfies all requirements. In section 5 we discuss some implementation issues. Finally, in section 6 we summarize our conclusions.

## 2. RELATED WORK

There is surprisingly little published work on the security of the AIS. Some of its vulnerabilities were first reported in [30], where it was also shown that these "affect all transponders deployed globally on vessels and other maritime stations like lighthouses, buoys, AIS gateways, vessel traffic services and aircraft involved in SAR operations." The authors in [31] reproduced and verified some of the vulnerabilities reported in [30]. In order to alleviate some of these, they propose 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; the protocol uses pseudonyms based on the IEEE 1609 standard. Three tiers (usage modes) of AIS are proposed. When on the first (default), AIS broadcasts only navigational information under a pseudonym. The second tier allows the encrypted exchange of information between two vessels. Last, a third tier "Retrieval mode" allows authorized organizations to gather information on the vessel from the AIS.

The solution proposed in [31] assumes the existence of a cryptographic infrastructure that provides the maritime community with some cryptographic capabilities. The authors in [33] use AIS, the Maritime Mobile Service Identities (MMSIs)<sup>2</sup> of the vessels and Trusted Third Parties to propose a 3-step mutual authentication scheme to increase ship-to-

---

<sup>1</sup> e.g. [www.marinetraffic.com](http://www.marinetraffic.com)

<sup>2</sup> 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 the vessels and has the prefix "IMO" followed by 7-digits. The main difference 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, MMSI change when a vessel changes flag and registration authority.

ship communication security. The scheme works in 3-steps, namely Pre-authentication, Mutual-authentication, and Group authentication. However, the proposed scheme 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 [34] 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. In this approach, the National Maritime CAs would be cross-trusted or root-trusted via the IMO root certificate. Each vessel and each high-ranking marine officer would obtain a public key certificate from the competent maritime CA. The proposed Maritime PKI, inter alia, would assume responsibility for the secure distribution of the keys of symmetric algorithms when a need for encrypted data transactions between vessel-to-vessel or vessel-to-shore bases would arise. 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 communications 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 [35], [36] are inapplicable in the maritime environment. Work that is not yet clear whether or how may affect the future of AIS security is also underway<sup>3</sup>.

Commercial AIS products that use symmetric cryptography exist. Nevertheless, they provide proprietary encrypted AIS only in vessels equipped with the same AIS product (e.g. Coast Guard, Special Forces, etc.). Such a product is SAAB's R5 Supreme W-AIS System [37] that supports DES, AIS and Blowfish. However, a worldwide adoption of symmetric cryptography system that distributes the same symmetric keys on a vast number of vessels worldwide is a very complex task. Even more challenging is to keep the symmetric key secret after its distribution to a large number of vessels around the globe. Therefore, such a solution is insecure for systems with characteristics similar to those of AIS [38].

Our research uses concepts of and results in Certificate-less Identity-Based Cryptography (IBC) [39], [38]; pseudonyms [40], [31], [41]; ADS-B [38], [35], [36], [42]; VANETs [43], [44], [45]; and MANETs [39], [46], [47].

### 3. THE AIS AND ITS SECURITY

AIS was designed to enhance “safety of life at sea” and “the safety and efficiency of navigation” by providing cost-effective, real-time, traffic control and collision avoidance information. It allows the automatic and continuous exchange of data between vessels (V-to-V) and between vessels and coastal authorities (V-to-C) in range. A vessel's AIS broadcasts specific data in specific time intervals, and at the same time it receives the data broadcasted by the AIS of other vessels in range. The exchanged data are classified as static; dynamic; voyage-related; and safety-related. Static data include the International Maritime Organization Number; the length; beam; and the type of the vessel. Dynamic data are the position; the time stamp in UTC; the course; the speed over ground; the heading; the rate of turn; and the navigational status of the vessel. Voyage-related data are the draught; potentially hazardous cargo type; destination; estimated time of arrival; and route waypoints of the vessel.

Some AIS vulnerabilities have been documented in [30], [31]. In this section we discuss these in an information security context, i.e. with respect to the attributes of information security: confidentiality, integrity, availability; and those of secure communication: message source authentication, and non-repudiation. Threats that exploit software, physical, mechanical and electronic characteristics of the AIS device, of antennas, power supplies etc. are beyond the scope of this work. Similarly, we do not consider the security, integrity, availability and functioning of systems and devices with which AIS may collaborate, such as GPS.

AIS broadcasted messages are neither encrypted nor authenticated; therefore, any unauthorized AIS receiver within range can uncontrollably read and forward AIS transmitted data to internet sites. This gives rise to the following attack

---

<sup>3</sup> <http://www.iala-aism.org/products-projects/e-navigation/>

scenario as shown in Figure 1: in dangerous sea areas, where pirates or terrorists lurk, at time  $t_0$  the attacker uses AIS information from the internet to select, track, and follow its distant target ship (S2). At time  $t_0 + n$ , the attacker is within range of the AIS of the target, and uses their AIS receiver to distinguish the target among other radar signals, even in heavy traffic waters. In order to thwart this scenario, the master may switch off the AIS transmitter.

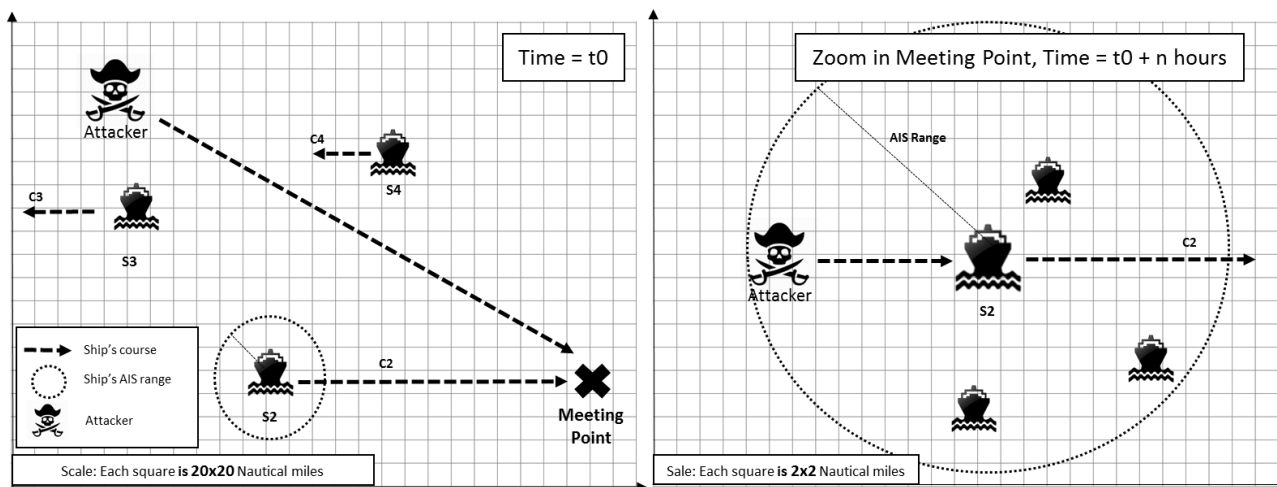


Figure 1: Attack scenario exploiting AIS lack of encryption

Additionally, the uncontrolled disclosure of information on the voyage of the vessel gives rise to threats against privacy, such as those depicted in Figure 2. These are threats that relate to VIP tracking, financial intelligence, sea-pirates and potential attacks by terrorists.

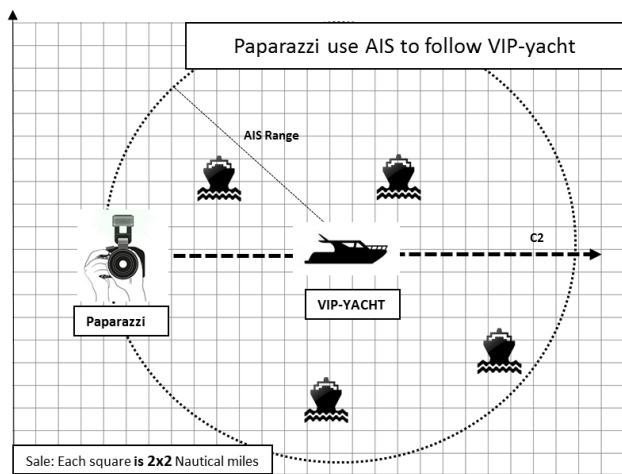


Figure 2: Attack against privacy scenario, exploiting AIS's lack of encryption

The absence of source authentication makes AIS vulnerable to vessel spoofing. A virtual ship may broadcast false data, e.g., false alarms, false traffic information, false maneuvering information. This gives rise to the following attack scenario as shown in Figure 3: in order to make the target to change course, an attacker sends false AIS messages to emulate a nonexistent boat on the course of the target.

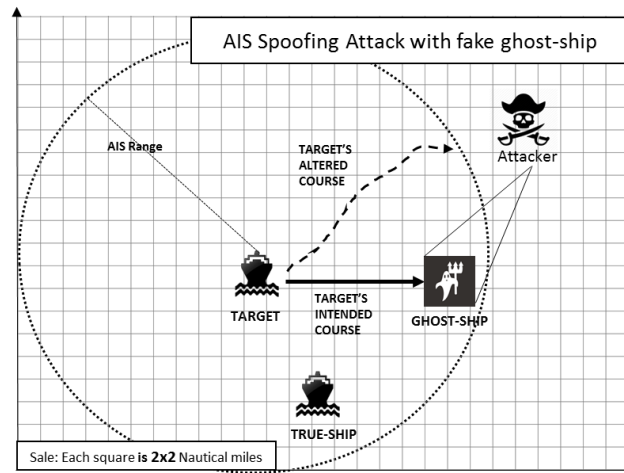


Figure 3: Spoofing attack scenario, exploiting AIS's lack of source authentication

Additionally, the absence of data integrity makes AIS messages vulnerable to unauthorized modifications. Surprisingly, non-repudiation of AIS messages has not yet attracted interest until now, despite its importance in investigating maritime accidents or violation of maritime laws.

Several attacks against the availability of AIS (e.g., slot starvation; frequency hopping; trimming attack) or of AIS misuse have been documented [48]. However, surprisingly, the worst threat to the availability of the AIS is the deliberate switching-off of the system by the crew, either in following official guidelines in dangerous areas or in violating the regulations to avoid the invasion of privacy of their passengers. This has as a side effect the deterioration of navigation safety.

Based on the discussion above, the requirements for a security enhanced AIS are as follows:

- 1) **Confidentiality:** AIS broadcasted messages should be encrypted.
- 2) **Privacy and Anonymity upon request:** Where confidentiality offers some protection from threats against privacy, full privacy and anonymity of a vessel upon request needs to be offered, to address authenticated adversaries. Thus, it must be possible to prove that even an anonymous vessel is an authorized and legitimate one; and that some non-repudiation capability must exist even for anonymous vessels.
- 3) **Message Source Authentication and Data Integrity:** AIS broadcasted messages must be authenticated.
- 4) **Non-repudiation of AIS messages:** AIS messages should enjoy the non-repudiation property.
- 5) **Completeness, Simplicity, and Feasibility.** Finally, yet importantly, the approach for a security enhanced AIS, must be complete and feasible in the complex maritime domain where AIS is a productive system, onboard the majority of vessels around the globe today. Thus, a proposed solution for AIS needs to be flexible to use by crews; simple; widely acceptable; easy to integrate; and financially affordable.

## 4. ARCHITECTURE OF A SECURE AIS

The global maritime environment is complex and interconnected [49]; it is governed by international and national regulations and maritime laws, and its stakeholders include international organizations (e.g. IMO), national authorities, agents, brokers, shipping companies, crewmembers. Communications are usually unreliable, with limited bandwidth and expensive. Especially on vast open sea areas, where the only reliable communication option between a vessel and shore base are the expensive satellites links. For our purposes a simplified tree hierarchical model of the maritime environment can be used. IMO is the root node; its children nodes are the national maritime authorities and their children nodes are the registered vessels flying the respective flag.

The vessels equipped with AIS create special AIS Ad-hoc NETWORKS (AISANETs), as depicted in Figure 4. The official AIS network model consists of single-hop unidirectional broadcast links. When at sea, each vessel broadcasts and receives the AIS data within a typical range of 20 nautical miles. Hence, vessels in range create around them random overlapping, ephemeral and dynamic ad-hoc networks that live for an arbitrary time, depending on the relative courses and speeds of the vessels in AIS range. These AIS ad-hoc networks can be considered as a special case of Mobile Ad-hoc NETWORKS (MANETs) [50], where the mobile entities are the vessels, the communication protocol is AIS and the underneath wireless network is the AIS broadcast frequency. Their lifetime and topology are dynamic because of the movement of the participating vessels. Furthermore, they are self-configured, as there is no previous knowledge or agreement about the number or the identity of the vessels participating in the ad-hoc AIS network. However, a very useful property of AISANETs is the existence of central authorities (IMO and the National Maritime Authorities) that allows pre-agreed administration tasks. Similarities of AISANETs with VANETs and with the Automatic Detection System-B (ADS-B) in aviation can also be identified.

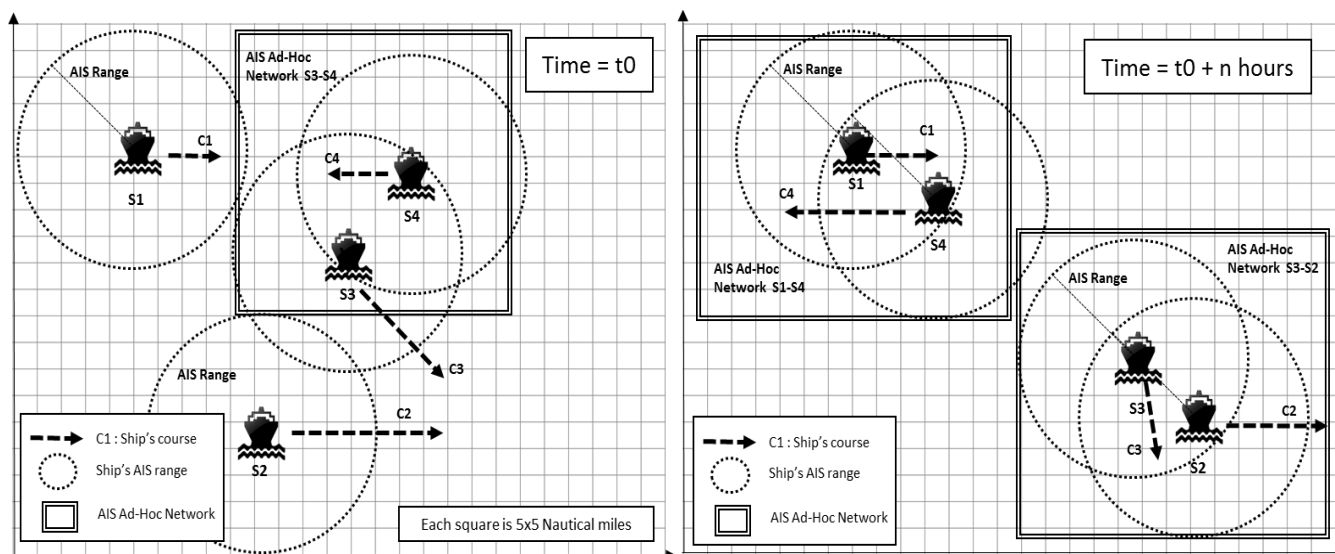


Figure 4: AIS Ad-hoc NETWORKS

Our concept for a secure AIS makes four main AIS Usage Modes available to the master:

1. "Simple AIS": AIS as it is today.
2. "Source authentication and data integrity AIS": The sender of AIS messages is authenticated and the integrity of the AIS messages is preserved.
3. "Privacy Preserving AIS": Anonymous but legitimate AIS broadcasting.
4. "Encrypted AIS": Flexibility with two plus two main variations, capable of operating both public key and symmetric key ciphers.
  - a. "Full encrypted AIS" or "Partially encrypted AIS": The captains may choose, at any time, to encrypt only those data considered to be sensitive (e.g. navigational data in clear-text, identity-data encrypted).
  - b. "1-1 Encrypted AIS with mIBC key-pair": For encrypted AIS transmissions to authorities or to the shipping company. Also, "Encrypted AIS with a symmetric algorithm", for broadcasting encrypted data to a group of chosen recipients.

Modes (2, 3, and 4) can be used simultaneously. An overview of the concept is shown in Figure 5.

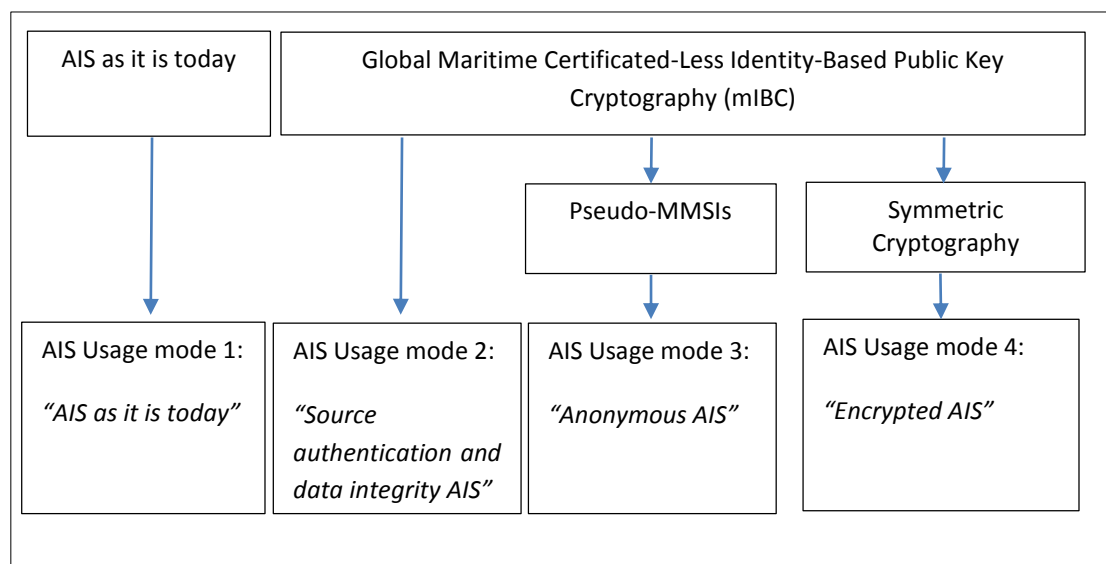


Figure 5: Overview of the concept

#### 4.1 THE CORNERSTONE: A MARITIME CERTIFICATE-LESS IDENTITY-BASED PUBLIC KEY CRYPTOGRAPHY (MIBC)

IBC was introduced by Shamir back in 1984 [51] to simplify the mainstream public key infrastructures of the time. IBC is a branch of Public Key Cryptography whose main characteristic is that the public key is a publicly known distinctive identity of each member (e.g. name, e-mail, etc.). Therefore, the implementation of IBC needs neither Certification Authorities nor certificates. In practice, this distinctive property gives us the opportunity to design considerably simpler and less resource-demanding public key implementations. This simplicity attracts MANET researchers since the appearance of the first working proposal back in 2001 [52]. As noted in [39], IBC is suitable especially when “efficient key management and moderated security is required”; this is perfectly aligned with the needs of a secure AIS. In brief, the main IBC advantages over traditional PKI, are the simplicity of the infrastructure, resources economy and self-proved information of the public key [39], [53], [54], [55] [40].

The advantages of IBC over PKI in the maritime context are

1. **The simplicity of the Infrastructure:** In the complex maritime environment, instead of creating CAs and sub-CAs or cross CAs that are required by the traditional PKI solutions, a maritime IBC requires only Private Key Generator Authorities; these in the maritime environment can be the National Maritime Registers/Authorities.
2. **Easiest worldwide adoption:** The absence of multiple CAs facilitates the adoption of the system by countries that do not have the resources, political, technical or financial, to support a national CA. The requirement for a private key generation authority is simpler than that for a fully functional CA.
3. **Scalability:** The IBC solution is as scalable as a public key infrastructure can be. As an example, note that National Private Keys Generators may co-exist with a root IMO-Private Keys Generator.
4. **Bandwidth economy:** With the use of certificateless IBC PKI we avoid consuming bandwidth for the transmission of the certificates that would be needed in a traditional PKI solution; this is crucial in heavy traffic waterways where the simultaneous AIS messages may be dozens or even hundreds. It should be noted that in general, IBC is more computationally demanding than a certificate-based solution. However, this is not a problem aboard ships, where adequate computational resources are available.
5. **Encrypted communication simplicity in open seas:** In a maritime IBC, the public key of a vessel is computed from the vessel’s publicly available MMSI number that is easily obtained via VHF, from on-line maritime vessel catalogs, from the authorities or from the shipping company.
6. **Identity-Based Cryptography is a foundation for hybrid cryptosystems:** The IBC infrastructure can be used for the distribution of symmetric keys, to create symmetric key encrypted AISANETs, as we shall later discuss.

We assume the following model of a maritime IBC that is based on the simplified maritime environment tree hierarchy. We need a maritime IBC implementation that equips with cryptographic key pairs the following participants: *International Maritime Organization (IMO)*, the *National Maritime Authorities*, the *vessels*, *beacons*, and *buoys*. To design an Identity-Based Cryptographic infrastructure, we need to specify the distinctive identifier of each entity, that would be its public key; the entity that will generate the corresponding private key; and how each entity will receive their private key.

The public keys of the vessels are derived by their distinctive MMSI numbers, the public key of IMO and each National and International Maritime Organization are derived by their distinguishing names, by using special, publicly known, mIBC- related, functions. Thus everyone automatically knows all public keys and no certificates are necessary. IMO is the Private Key Generator for the corresponding public keys of the National Maritime Authorities. The National Maritime Authorities (NMA-PKG) are the Private Key Generators for the corresponding keys of the vessels, buoys, beacons ...etc. The initial private key-escrow is manual via a smart token given to an authorized representative of each vessel by the key generator, i.e. the NMA-PKG.

In brief, according to this design, in the beginning IMO self-generates its private key. Then IMO generates the private keys for the registered National Maritime Authorities (NMA). The latter are responsible for generating the private keys of the registered vessels, buoys, and beacons under their flag, as in Figure 6. The private key of each vessel *is stored in a smart token* and transferred to the vessel by authorized personnel. On board the vessel, the smart token is plugged in a special mIBC-middleware device or directly in a mIBC-enabled AIS device. IMO has the additional roles of the key holder of the revocation list and of the disseminator; of the top Trusted Third Party for non-repudiation disputes; and of the top center for pre-agreed administration tasks. This scheme is easily expandable to cover the whole chain of maritime activities (e.g. shipping companies, shipping brokers).

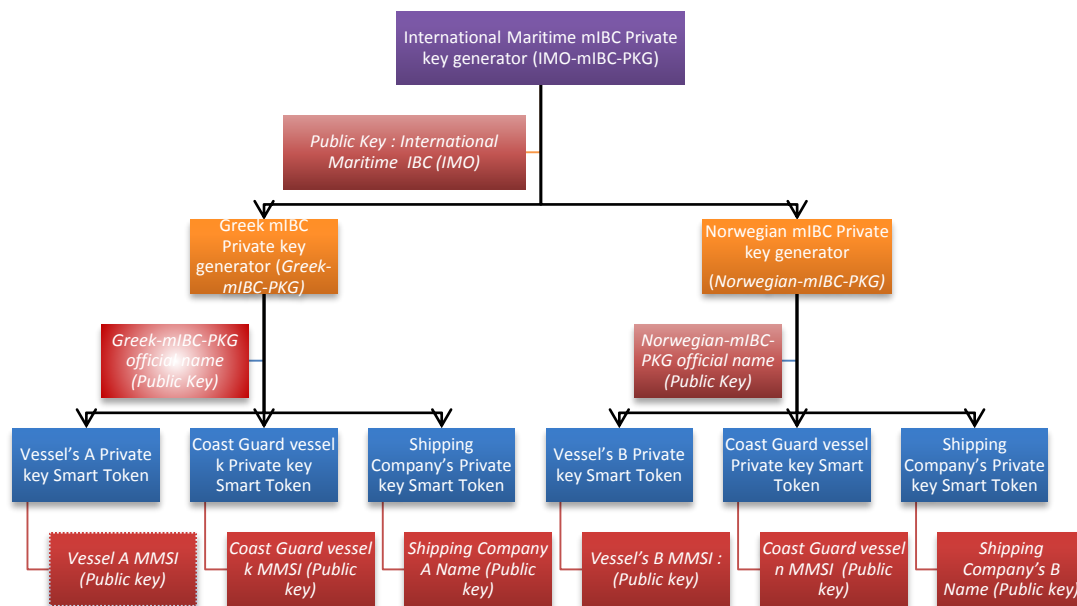


Figure 6: The proposed Maritime IBC

#### 4.2 PRESERVING PRIVACY: ANONYMOUS-AIS USAGE MODE USING PSEUDONYMOUS MMSIS

The term “digital pseudonym” or just “pseudonym” was introduced by D. Chaum back in 1985 [56] in an article that tried to introduce the notion of “security without identification.” However, pseudonyms became popular due to the work on anonymity for VANETs; this has led to the IEEE 1609 group of standards for Wireless Access in Vehicular Environment (WAVE) [41]. In the context of the mIBC, “pseudonyms” will give to a vessel the ability to preserve its anonymity when it uses AIS under certain circumstances. Based on the concept of a legitimate pseudo-id, we can offer anonymity of the vessel via pseudonymous MMSIs. In brief, the vessel sends a signed Request to its National mIBC Private Key Generator



(National-mIBC-PKG) authority indicating its desire to validate new pseudonymous MMSIs, hereafter called *pseudo-MMSIs*. The National-mIBC-PKG authority creates a pack of pseudo-MMSI numbers and sends them securely, i.e. by a message encrypted with the mIBC public key of the receiver to the vessel. Then, instead of its real MMSI, the AIS of the vessel broadcasts a pseudo-MMSI. We note that the National-mIBC-PKG authority keeps records that bind all the released pseudo-MMSIs with the true identity of the vessel, to ensure non-repudiation.

For example, assume that Vessel A wants to preserve its anonymity when sending AIS signals. In more detail, the steps to be followed are:

1. **Prerequisites:**
  - a. We assume that Vessel A has already obtained from its corresponding National mIBC-PKG authority its distinctive maritime mIBC Key pair: Private key, and Public key that derives from its MMSI.
  - b. The vessel may produce the public key of its corresponding National mIBC Private Key Generator authority that derives from the (publicly available) official name of the National mIBC Private Key Generator authority.
  - c. The vessel may send/receive messages (data) by means other than AIS.
  - d. There is a communication means (e.g. satellites) between the vessel and its corresponding National mIBC Private Key Generator authority.
2. **The vessel sends a signed Request to its National mIBC Private Key Generator (National-mIBC-PKG) authority indicating its desire to validate new Pseudo-MMSIs.** The vessel sends a signed, encrypted, and time-stamped, "Request for Pseudo-MMSIs" to its National-mIBC-PKG.
3. **The National mIBC Private Key Generator authority creates a pack of Pseudo-MMSI numbers:** These numbers have the following properties:
  - a. A standard prefix (e.g. "000-") to be distinguished from real MMSIs
  - b. The expiration date of the Pseudo-MMSI
  - c. Random digits
  - d. They are nine digits long, to ensure compatibility with the existing AIS protocol.
4. **For each Pseudo-MMSI number a new valid mIBC Public key is produced by the National-mIBC-PKG.** The mIBC infrastructure dictates that the public key of each vessel derives from the MMSI of the vessel. Consequently, for each Pseudo-MMSI number we can produce a new valid, distinctive, public key for our mIBC infrastructure. Hence, each vessel can generate as many pseudo-MMSIs it wishes, along with their derivative public keys.
5. **The National mIBC Private Key Generator authority securely sends back to the vessel the generated private keys of the pseudo-MMSIs.** The National-mIBC-PKG authority sends back to the requesting vessel timestamped, signed and encrypted messages with:
  - a. The new pseudo-MMSIs, (the vessel can produce the corresponding public keys).
  - b. The corresponding private keys.
6. **AIS broadcasts a pseudo-MMSI instead of the real MMSI of the vessel.** The vessel that uses pseudo-MMSIs preserves its anonymity and at the same time proves that is a legitimate vessel, registered with the mIBC infrastructure. This is because only a legitimate National mIBC Private Key Generator authority can generate the corresponding private keys of the pseudo-MMSIs.
7. **Non-repudiation:** The National mIBC Private Key Generator authority will preserve encrypted records of real MMSIs and of the corresponding pseudo-MMSIs. Upon official request, the National-mIBC-PKG will provide official law enforcement organizations with the real identity of the vessel behind each pseudo-MMSI.

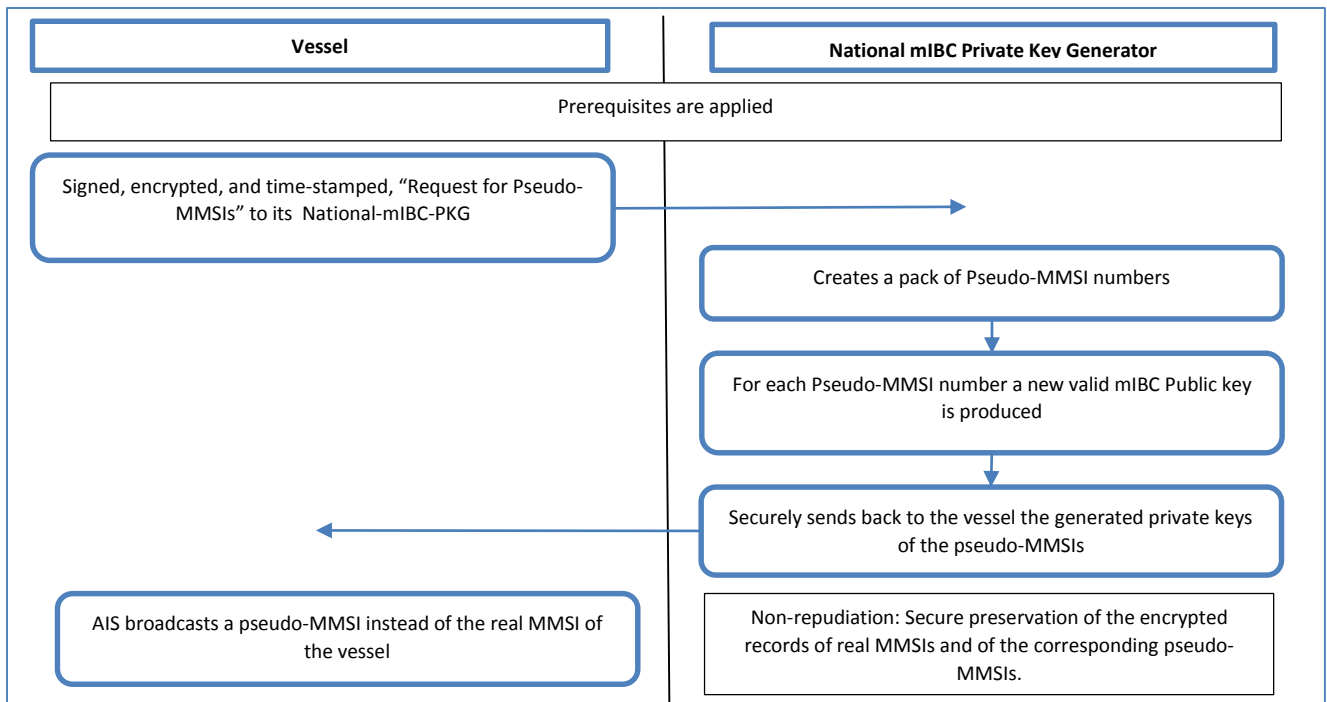


Figure 7: Preserving privacy: Anonymous-AIS usage mode using pseudonymous MMSIs

#### 4.3 ENCRYPTED-AIS MODE AND SYMMETRIC CRYPTOGRAPHY IN INSECURE SEA AREAS

Our goal is to give a secure navigational alternative to switching off the AIS, as the IMO guidelines dictate, when there are concerns about the security of the vessel. AIS broadcasted data may be a honeypot for lawless activities (e.g. piracy) in insecure sea areas (e.g. Somalia coast, etc.). Our aim is, in insecure sea areas, the AIS navigational data broadcasted by legitimate vessels to be received only by legitimate vessels and not by not-legitimate vessels in the area. We propose the on demand encryption of the legitimately broadcasted AIS data. No one should be able to decrypt the broadcasted data, except those entities (vessels, shore-bases, authorities) that have the right to do so.

However, it is impossible to pre-determine all the legitimate vessels, because the assumption that a registered ship is also a lawful ship is unrealistic. Thus, we propose to focus the use of the encrypted-AIS only in officially declared “insecure sea areas”. Inside these areas, it is possible for a law-enforcement authority (e.g. a military patrol ship) to distinguish the legitimate vessels (e.g. cargo vessels) from the suspicious ones (e.g. sea-pirates). This will allow the use of encrypted-AIS only between the designated as legitimate vessels, whilst the suspicious ones will receive only useless encrypted AIS data. This approach raises a number of issues: How do we define an “insecure” sea area; who should declare these areas; who and how can distinguish the vessels in an “insecure” sea area between legitimate and suspicious; and finally how all this may be implemented by Encrypted-AIS?

##### 4.3.1 DEFINITION OF AN “INSECURE” SEA AREA

- 1) **How do we define an “insecure” sea area?** IMO allows the AIS to be switched-off “if the master believes the continual operation of AIS might compromise the safety or security of his /her ship or if security incidents are imminent” [2]. We use this as a definition of an “insecure sea area,” and we highlight some additional properties of such areas:
  - a) An “insecure sea area” may have specific or abstract geographic boundaries. (e.g. the sea area off the Somalia coasts, some coastal areas in West Africa, the Malacca Straits)
  - b) An “insecure sea area” may be defined ad-hoc, in a periodical fashion when “security incidents are imminent.” (e.g. the coastal area out of a heavy-traffic when a terrorist attack is imminent)

- c) An “insecure sea area” may be partitioned ad-hoc in smaller sea areas. (e.g. safe pathways where law enforcement units are patrolling)
- 2) **Who has the right to declare a danger “insecure” sea area?** We propose that the maritime community must adopt procedures to officially declare, define and label the “insecure” sea areas globally. Nevertheless, we presume that this should be a co-responsibility of the international maritime authorities (e.g. IMO, IALA) along with the national maritime authorities and the ship owners.

#### 4.3.2 DEFINITION OF AN AD-HOC TRUSTED THIRD PARTY IN AN “INSECURE” SEA AREA

In our concept, the ability to distinguish at all times between the “good”-legitimate vessels and the “bad”-suspicious ones inside each “insecure” sea area is the backbone of the encrypted-AIS. The role of the Trusted Third Party that will make the distinction may be assigned to a representative of a law-enforcement authority in the region. In practice, this TTP may be a military boat of a United Nations force, a port authority or other official shore base, a coast guard boat, a coast guard patrolling airplane, a drone, a micro-satellite, or even a new global specialized maritime authority. The task of the TTP is firstly, to at all times distinguish between the “good”-legitimate vessels and the “bad”-suspicious ones; and secondly (as we shall see later on) the symmetric-key escrow of the AIS on the legitimate vessels inside each “insecure” sea area.

#### 4.3.3 ENCRYPTED-AIS WITH SYMMETRIC CRYPTOGRAPHY, SYMMETRIC KEY ESCROW WITH MIBC

Traffic in these insecure sea areas is neither pre-agreed nor pre-determined; a number of vessels might get inside an “insecure” sea area while others leave the area. Furthermore, the AIS range of each vessel does not cover completely the insecure sea-area; each ship receives and transmits AIS messages inside its AIS range. In these sea areas, variable and temporary AISANETs are created and dispatched as described earlier. Note that the mIBC is a public-key cryptography variant, and thus it is ideal for one-to-one authentication and encrypted communication without any pre-agreement. On the contrary, it is a nightmare for broadcasting encryption, because each message should be separately encrypted and retransmitted to each recipient. On the other hand, symmetric cryptography is ideal for encrypted broadcasting messages. Yet, everyone must share, somehow, the same symmetric key. Symmetric cryptography is already in use in commercial AIS products [37], and some coast guards around the world. However, these implementations, as far as we know, are used for secure AIS communication between pre-determined vessels (“blue-forces”), e.g. the vessels of the coast guard. On the contrary, we are interested in using the encrypted AIS among non-pre-determined vessels, with or without any pre-agreement. The latter is very important because our approach allows the use of the Encrypted-AIS mode between unknown vessels in an area, in an ad-hoc manner. To this end, we propose the use of hybrid cryptography, i.e. to use the mIBC to distribute the symmetric key to the entities that would like to encrypt their communications with a symmetric cryptographic algorithm.

In more detail, the steps to be followed to use Encrypted-AIS are:

1. **Prerequisites:**
  - a. A sea area official classified as “insecure” a sea area. (e.g. “Coast-of-Somalia”). Because some areas are too large, further partitioning may be required.
  - b. At least one Trusted Third Party (TTP) as defined earlier (e.g. a Military Patrol Boat, a micro-satellite) is present and can create keys for symmetric encryption and distribute them, encrypted with the public keys (mIBC) of the recipients.
  - c. The vessels can use mIBC to exchange encrypted-AIS messages.
  - d. The vessels in the area may broadcast encrypted AIS messages and decrypt received AIS messages.
  - e. The vessels in the area are registered with the maritime-IBC infrastructure (mIBC), and thus they have a valid mIBC key pair and a valid MMSI number.
  - f. We assume that the suspicious vessels are also registered with the maritime-IBC infrastructure (mIBC) and thus they have a valid mIBC key pair and a valid MMSI number.
2. **One or more law-enforcement units are assigned as the official Trusted Third Parties (e.g. a Military Patrol Boat, a micro-satellite) on the specific “insecure” sea area.**

3. **Classification of the vessels in the specific “insecure” sea area to legitimate and suspicious ones.** The TTP in the “insecure” sea area receives reports of suspicious movements from a vessel. The vessel is classified as “Suspicious-Vessel” and an alarm is triggered. The criteria and the procedures to characterize a vessel as “Legitimate” or “Suspicious” are beyond the scope of this paper.
4. **Legitimate and suspicious vessels classification in the specific “insecure” sea area.** The TTP classifies the vessels in the area in two groups, namely the legitimate vessels and the suspicious ones. The TTP collects the MMSIs of all the legitimate vessels.
5. **Symmetric key generation.** The TTP broadcasts an alarm AIS message and an AIS call to prepare to change to Encrypted-AIS with specific cryptographic properties (e.g. symmetric cipher name, symmetric key length). The TTP generates a symmetric key with an expiration date/time that will be valid for Encrypted-AIS in this specific “insecure” Sea area only.
6. **Key escrow, of the symmetric key. Only the legitimate vessels in the area obtain the symmetric key.** The TTP encrypts and transmits the AIS symmetric-key with the mIBC-public-key of each legitimate vessel in the area. Each legitimate vessel receives a message that contains the AIS symmetric key, encrypted with its mIBC-public key and uses its corresponding mIBC-private key to decrypt it. Thus, after a while, all legitimate vessels expected to have the symmetric key ready to use for the Encrypted-AIS broadcast.
7. **Suspicious vessels never obtain the symmetric key of the Encrypted-AIS in this area.** The TTP never transmits the symmetric key encrypted with the mIBC public-keys of the suspicious vessels. Since the suspicious vessels do not have the private key of any of the legitimate vessels in the area, they cannot decrypt the TTP messages and they cannot obtain the symmetric key for the Encrypted-AIS broadcast.
8. **The legitimate vessels use Encrypted-AIS mode, and only those who have the right symmetric key can decrypt the broadcasted data.** The legitimate vessels and the law-enforcement authorities have access to all the AIS navigation data; encryption/decryption of the AIS messages is transparent to the end users and the e-navigation systems.
9. **The suspicious vessels cannot decrypt Encrypted-AIS data, and they cannot use AIS information to attack their targets.** The suspicious vessels are unable to obtain any AIS information for this specific “insecure” sea area.
10. **The TTP continuously monitors the specific “insecure” sea area for new vessels entering.** When a new vessel enters the specific “insecure” sea area, the TTP decides in which group to classify it. If it is classified as a legitimate vessel, it automatically becomes a member of the Encrypted-AIS ad-hoc network of the specific sea area. Then it receives a message, encrypted with its mIBC public-key, which contains the symmetric key of the specific Encrypted-AIS ad-hoc network. Hence, the newly entered legitimate vessel may start also to use the Encrypted-AIS.

Figure 8a depicts the attacker’s point of view when using the AIS as is today, whilst figure 8b when the Encrypted-AIS is in use. In the former case the e-navigation monitor of an attacker displays detailed information on all the vessels in the area, by receiving their plaintext AIS data. In the latter case, all AIS communication between legitimate vessels is encrypted. Since the attacker is unable to decrypt these messages, the vessels in the area are hidden from them.

Similarly, figure 9a depicts the legitimate vessel’s point of view when using the AIS as is today, whilst figure 9b when the Encrypted-AIS is in use. In the former case, the legitimate vessel’s master was forced to switch off the AIS, thus degrading the level of domain/situation awareness and, accordingly, navigation safety. In the latter case, both the level of domain/situation awareness and navigation safety remains intact.

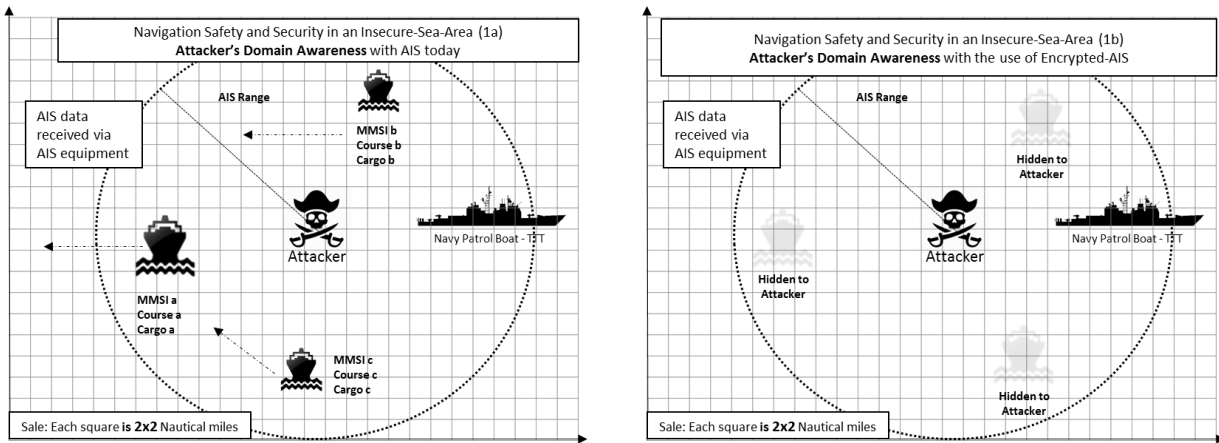


Figure 8: Unencrypted (1a) versus Encrypted-AIS (1b): The attacker's view

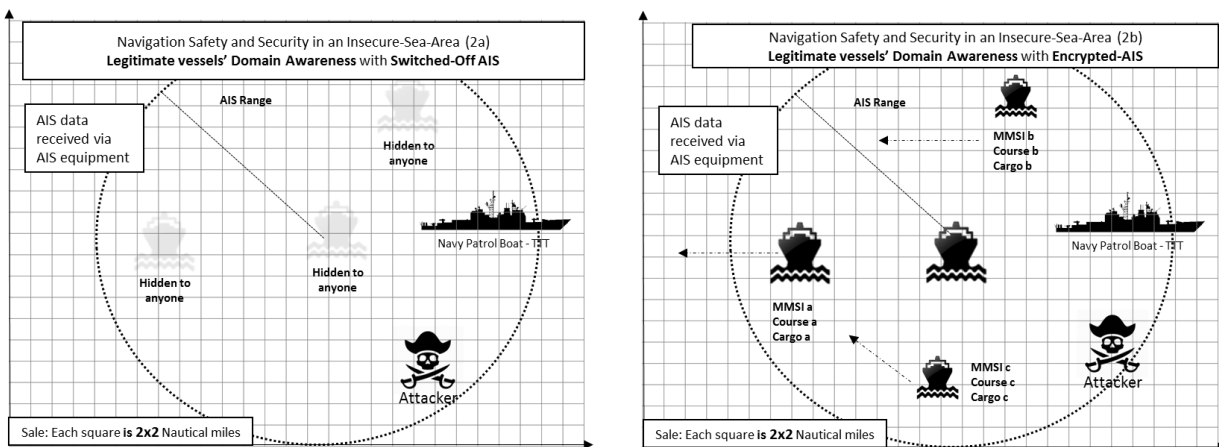


Figure 9: Unencrypted (2a) versus Encrypted-AIS (2b): The legitimate vessel's view

#### 4.3.4 EVALUATION AGAINST THE REQUIREMENTS FOR A SECURE AIS

In this subsection, we evaluate the concept of the maritime IBC/Pseudo-MMSIs scheme against the requirements for a security enhanced AIS of section 2. As we do not propose a specific implementation, our evaluation is based on the general security properties of Identity-Based Cryptography, Symmetric Cryptography, and Hybrid Cryptosystems.

1. **AIS Message Confidentiality (AIS Usage mode 4: "Encrypted AIS").**
  - a. **Ad-Hoc, one-to-one AIS message confidentiality.** The proposed maritime-IBC provides each vessel with a private key where the public key is easily derived from the distinctive MMSI number of the vessel. Therefore, AIS messages can be encrypted with the public key of the intended receiver. This gives the ability to a vessel to choose specific receivers to send partially or fully encrypted messages. (E.g., a vessel with sensitive cargo that wants to inform real-time for its navigational data only the law enforcement authorities and its shipping company.)
  - b. **Group AIS Message confidentiality with hybrid cryptosystems in insecure areas under the supervision of a Trusted Third Party.**
2. **Privacy/Anonymity capabilities for AIS (AIS Usage mode 3: "Anonymous AIS").** Our proposal satisfies the two conditions about the legitimacy and the non-repudiation of the anonymous vessel. An official authority, the National-mIBC-PKG, which creates the pseudo-MMSIs and their corresponding private keys, guarantees the legitimacy of the vessel under the pseudo-MMSIs.

3. **AIS Source Authentication and AIS data integrity (AIS Usage mode 2: “Source authentication and data integrity AIS”).** When each entity has an mIBC key pair, there are numerous methods to choose from to implement this mode. In brief, AIS data can be “signed” with the real or pseudo-MMSI private key of the vessel and then broadcasted. Part of the AIS broadcasted data is the MMSI number (or the corresponding analog in Pseudo-MMSI) from which the vessel’s public key is derived. Therefore, each vessel which receives the AIS message can use the received public key (MMSI number/ Pseudo-MMSI analog) to authenticate the source and check the data integrity.
4. **A scalable AIS information dissemination is feasible on all four main AIS usage modes.** It is possible to implement a partial encryption of AIS data with the public keys (MMSI-numbers) according to the information that the sender-vessel wants to disclose in public and in private. For example, a vessel may broadcast unencrypted all the AIS data and encrypt only its cargo data with the public key of a coast guard vessel. Thus, everybody has the sender-vessel navigational data, whilst only the coast guard may access its cargo data.
5. **Because we are proposing alternatives to switching-off the AIS, the availability of the AIS service is increased.** The pseudo-MMSIs and the scalable authorized AIS information broadcasting give the opportunity to the vessel’s crew to use these methods to keep their anonymity and to control information dissemination. Therefore, it is unlikely that the crew switches off the AIS to preserve the anonymity of the vessel or the privacy of the passengers. Unfortunately, this does not affect the ability to launch DoS attacks on AIS.
6. **Non-repudiation of broadcasted AIS messages.** The “signing” of the AIS data with the MMSI number provides the needed non-repudiation capabilities to the AIS. On the other hand, when the vessel uses pseudo-MMSIs for anonymity, the only way to ensure non-repudiation is to keep records of the real identity of the vessels and of their given pseudo-MMSIs. In this case, we are highly dependent on the trustworthiness of the third party, which is the official authority (the NMA-PKG in our case) that creates and disseminates the Pseudo-MMSIs.

## 5. IMPLEMENTATION ISSUES

We based our conceptual proposal on related works for AIS and similar systems in transportation sectors, e.g. ADS-B in aviation, and VANET systems in vehicular transportation. In this section, we highlight some issues related to the implementation of such a scheme.

**Equipment upgrade:** When a large number of vendors offer a variety of AIS equipment that is already on-board a vast number of vessels, a practical, economical and flexible solution must be found to upgrade to the security-enhanced version. We propose a Secure-AIS-Middle-ware equipment that may be a single PC with special software installed. It is a middle-ware between the AIS equipment and all the other devices (GPS, Speedometer, Steer, Digital map, AIS monitor, keyboard, etc.). It will process and forward to AIS, the data corresponding to GPS, speed, location, cargo, etc. and the AIS will just broadcast them according to the AIS specifications. Similarly, the received AIS messages will be forwarded to the Secure-AIS-Middle-ware equipment for processing and then will be forwarded to the e-navigation equipment of the ship.

The Secure-AIS-Middle-ware equipment would be responsible at least for the followings actions:

- 1) Directly receives, distinguishes all the inputs/outputs from the navigational equipment that are usually communicating with the AIS.
- 2) Processes the data received from AIS and forward them to other devices.
- 3) Receives data from vessel equipment, processes them, and forwards to AIS.
- 4) Stores the public keys of the authorities.
- 5) Manages the received private key that may be stored in a smart token plugged in the middle-ware.
- 6) Communicates, independently of AIS, with the authorities of mIBC.
- 7) Reads the MMSI number from an AIS message and uses it to compute the corresponding public key.
- 8) Checks the authentication and integrity of received AIS messages.
- 9) Encrypts/decrypts part of an AIS message, when requested, and sends it to the appropriate output.
- 10) Sends requests to obtain pseudo-MMSIs, obtains them and uses them.

Additionally, the Secure-AIS-Middle-ware equipment is the enabler of the four AIS Usage Modes.

**mIBC Private Key Compromise:** If a private key is compromised, then the corresponding key pair should be revoked and added to the Revoked Keys List. This can be complicated, as the public key is the distinctive MMSI number of the vessel. Therefore, to generate a new private key, the vessel must obtain a new MMSI number; this is a resource-demanding task. On the other hand, the MMSI number of a ship changes every time the ship changes flag; MMSI change is not uncommon and official procedures are applied. Thus, in case of mIBC Private Key compromise we may follow the existed procedures to change the MMSI of the ship and issue new mIBC key-pair.

**Public Key Revocation List** (actually MMSIs revocation list). Each time a vessel is in port, it can download the latest Revocation Lists. In open seas, the vessels that have the required resources can download the latest Public Keys Revocation List via a wireless communications mean (ex. Satellite) and forward it to vessels in range. We note that the Public Keys Revocation List is actually the MMSIs Revocation List. Thus, it is not something new to maritime community.

## 6. CONCLUSIONS

We examined the security of AISANETs as a special case of MANETs, with properties similar to those of VANETs and closely related to the ADS-B system in aviation. As such, in order to satisfy the requirements of confidentiality, source authentication, data integrity, and anonymity in AIS, we proposed the use of certificate-less Identity-Based Cryptography (IBC) along with pseudo-MMSIs and described the architecture of such a solution.

## REFERENCES

- [1] International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), "An overview of AIS," International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), Saint Germain en Laye, 2016.
- [2] International Maritime Organization, "AIS transponders," International Maritime Organization, 2017. [Online]. Available: <http://www.imo.org/en/OurWork/safety/navigation/pages/ais.aspx>. [Accessed 5 November 2017].
- [3] US Coast Guard, "Vessel Requirements for Notices of Arrival and Departure, and Automatic Identification System," *Federal register*, 30 January 2015.
- [4] European Union, "Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EE," *Official Journal of the European Union*, pp. L208/10-L208/27, 5 August 2002.
- [5] European Union, "Directive 2009/17/EC of the European Parliament and of the Council of 23 April 2009 amending Directive 2002/59/EC establishing a Community vessel traffic monitoring and information system," *Official Journal of the European Union*, pp. L131/101-L131/113, 28 May 2009.
- [6] European Union, "Commission Directive 2011/15/EU of 23 February 2011 amending Directive 2002/59/EC of the European Parliament and of the Council establishing a Community vessel traffic monitoring and information system," *Official Journal of the European Union*, pp. L49/33-L49/36, 24 February 2011.
- [7] F. Mazzarella, A. Alessandrini, H. Greidanus, A. M. A. P. N. D. and L. Ziemba, "Data fusion for wide-area maritime surveillance," in *Workshop on moving objects at sea*, Brest, France, 2013.
- [8] F. Mazzarella, V. F. Arguedas and M. Vespe, "Knowledge-based vessel position prediction using historical AIS data," in *Sensor data fusion: Trends, solutions, applications (sdf)*, Bonn, Germany, 2015.
- [9] G. Pallotta, S. Horn, P. Braca and K. Bryan, "Context-enhanced vessel prediction based on ornstein-uhlenbeck processes using historical AIS traffic patterns: Real-world experimental results," in *17th international conference on information fusion (FUSION), 2014*, Salamanca, Spain, 2014.
- [10] G. Pallotta, M. Vespe and K. Bryan, "Vessel pattern knowledge discovery from AIS data: A framework for anomaly detection and route prediction," *Entropy*, vol. 15, no. 6, p. 2218–2245, 2015.
- [11] F. Mazzarella, M. Vespe, D. Damalas and G. Osio, "Discovering vessel activities at sea using AIS data: Mapping of fishing footprints," in *17th international conference on information fusion (FUSION), 2014*, Salamanca, Spain, 2013.

- [12] F. Natale, M. Gibin, A. Alessandrini, M. Vespe and A. Paulrud, "Mapping fishing effort through AIS data," *PLoS ONE*, vol. 10, no. 6, pp. 1-16, 2015.
- [13] M. Vespe, M. Gibin, A. Alessandrini, F. Natale, F. Mazzarella and G. C. Osio, "Mapping EU fishing activities using ship tracking data," *Journal of Maps*, vol. 12, no. sup1, pp. 520-525, 2016.
- [14] D. O. D. Handayani, W. Sediono and A. Shah, "Anomaly detection in vessel tracking using support vector machines (SVMs)," in *2013 International conference on advanced computer science applications and technologies (ACSAT '13)*, Washington D.C., USA, 2013.
- [15] R. Laxhammar, F. G. and E. Sviestins, "Anomaly detection in sea traffic - a comparison of the gaussian mixture model and the kernel density estimator," in *12th international conference on information fusion (FUSION '09)*, Seattle, Washington, USA, 2009.
- [16] B. L. S. B. Ristic, M. Morelande and N. Gordon, "Statistical analysis of motion patterns in AIS data: Anomaly detection and motion prediction," in *11th international conference on information fusion (FUSION '08)*, Cologne, Germany, 2008.
- [17] Z. Ou and J. Zhu, "AIS database powered by GIS technology for maritime safety," *The Journal of Navigation*, vol. 61, p. 655-665, 2008.
- [18] F. Xiao, H. Ligteringen, C. van Gulijk and B. Ale, "Comparison study on AIS data of ship traffic behavior," *Ocean Engineering*, vol. 95, pp. 84-93, 2015.
- [19] R. Van Dorp and J. Merrick, "On a risk management analysis of oil spill risk using maritime transportation system simulation," *Annals of Operational Research*, vol. 187, p. 249-277, 2011.
- [20] F. Goerlandt, H. Goite, O. Valdez Banda, A. Höglund, P. Ahonen-Rainio and M. Lensu, "An analysis of wintertime navigational accidents in the Northern Baltic sea," *Safety Science*, vol. 92, p. 66-84, 2017.
- [21] J. Chen, F. Lu and G. Peng, "A quantitative approach for delineating principal fairways of ship passages through a strait," *Ocean Engineering*, vol. 103, p. 188-197, 2015.
- [22] W. Zhang, F. Goerlandt, P. Kujala and Y. Wang, "An advanced method for detecting possible near miss ship collisions from AIS data," *Ocean Engineering*, vol. 124, p. 141-156, 2016.
- [23] X. Qu, Q. Meng and L. Suyi, "Ship collision risk assessment for the Singapore strait," *Accident Analysis & Prevention*, vol. 43, p. 2030-2036, 2011.
- [24] J.-P. Jalkanen, L. Johansson and J. Kukkonen, "A comprehensive inventory of the ship traffic exhaust emissions in the Baltic Sea from 2006 to 2009," *Ambio*, vol. 43, p. 311-324, 2014.
- [25] N. Merchant, M. Witt, P. Blondel, B. Godley and G. Smith, "Assessing sound exposure from shipping in coastal waters using a single hydrophone and Automatic Identification System (AIS) data," *Marine Pollution Bulletin*, vol. 64, p. 1320-1329, 2012.
- [26] R. Shelmerdine, "Teasing out the detail: how our understanding of marine AIS data can better inform industries, developments, and planning," *Marine Policy*, vol. 54, p. 17-25, 2015.
- [27] B. Elliso, "Panbo: The marine electronics hub," 17 April 2009. [Online]. Available: [https://www.panbo.com/archives/2009/04/mandated\\_ais\\_an\\_aid\\_to\\_pirates.html](https://www.panbo.com/archives/2009/04/mandated_ais_an_aid_to_pirates.html). [Accessed 5 November 2017].
- [28] A. Palmer, *The New Pirates: Modern Global Piracy from Somalia to the South China Sea.*, I.B.Tauris, 2014.
- [29] L. Trask, "Captain raises AIS privacy concerns," 25 September 2013. [Online]. Available: [http://www.superyachtnews.com/business/captain\\_raises\\_ais\\_privacy\\_concerns](http://www.superyachtnews.com/business/captain_raises_ais_privacy_concerns). [Accessed 5 November 2017].
- [30] M. Balduzzi, K. Wilhoit and A. Pasta, "A Security Evaluation of AIS," Trend Micro.
- [31] 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.
- [32] 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.
- [33] S. H. Oh, D. Seo and B. Lee, "S3 (secure ship-to-ship) information sharing scheme using ship authentication in the e-navigation," *International Journal of Security and its Applications*, vol. 9, no. 2, pp. 97-110, 2015.
- [34] 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.



- [35] 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.
- [36] 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.
- [37] 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].
- [38] 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.
- [39] 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.
- [40] 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.
- [41] IEEE, 1609.2-2016 - *IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages*, IEEE, 2016.
- [42] A. Yang, X. Tan, J. Baek and D. Wong, "A new ADS-B authentication framework based on efficient hierarchical identity-based signature with batch verification," *IEEE Transactions on Services Computing*, vol. 10, no. 2, pp. 165 - 175, 2017.
- [43] V. Yadav, S. Misra and M. Afaque, "Security in Vehicular Ad Hoc Networks," in *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, Auerbach Publications, 2010, p. 227–250.
- [44] M. Gerlach and F. Guttler, "Privacy in VANETs using Changing Pseudonyms - Ideal and Real," in *IEEE 65th Vehicular Technology Conference, 2007*, Dublin, Ireland, 2007.
- [45] G. Calandriello, P. Papadimitratos, J.-P. Hubaux and A. Lioy, "Efficient and Robust Pseudonymous Authentication in VANET," in *4th ACM international workshop on Vehicular ad hoc networks (VANET'07)*, Montréal, Québec, Canada, 2007.
- [46] Y. Xiao, X. Shen and D.-Z. ( . Du, *Wireless Network Security*, Springer US, 2007.
- [47] H.-Y. Lin, Y.-M. Huang and T.-I. Wang, "Resilient Cluster-Organizing Key Management and Secure Routing Protocol for Mobile Ad Hoc Networks," *IEICE Transactions on Communications*, vol. E88–B, no. 9, pp. 3598-3613, 2005.
- [48] The Nautical Institute, "AIS Issues," [Online]. Available: <http://www.nautinst.org/en/forums/ais/ais-issues.cfm>. [Accessed 5 November 2017].
- [49] H. Smith, "Understanding the Maritime Transport Ecosystem," MONA LISA 2.0, Kingston, Ontario, Canada.
- [50] M. M., G. L., M. P. and H. T., "Towards an Understanding of Security, Privacy and Safety in Maritime Self-Reporting Systems," in *IFIP International Conference on Trust Management*, Gothenburg, Sweden, 2007.
- [51] A. Shamir, "Identity-Based Cryptosystems and signature schemes," in *CRYPTO '84*, 1984.
- [52] D. Boneh, B. Lynn and H. Shacham, "Short Signatures from the Weil Pairing," in *7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2001)* , Gold Coast, Australia, 2001.
- [53] Y. Fang, X. Zhu and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," *IEEE Wireless Communications*, pp. 24-30, 2009.
- [54] 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.
- [55] 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.
- [56] D. Chaum, "Security without identification: transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, no. 10, p. 1030–1044, 1985.



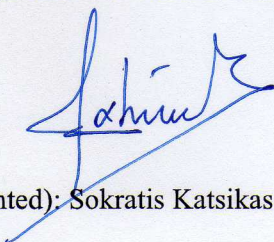
Journal of Marine Science and Technology  
CERTIFICATION FOR MANUSCRIPT SUBMISSION

The author warrants that the manuscript is the author's original work and has not been published before. (If excerpts from copyrighted works are included, the author will obtain written permission from the copyright owners and show credit to the sources in the manuscript.)

If the work was prepared jointly, the author agrees to inform coauthors of the terms of the agreement and to sign on their behalf.

Manuscript title: TOWARDS A SECURE AUTOMATIC IDENTIFICATION SYSTEM (AIS)

Signature

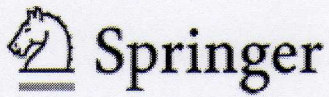


Name printed): Sokratis Katsikas

Affiliation: Norwegian University of Science and  
Technology, Center for Cyber and Information Security

Date: 28 December 2017

*If the paper is rejected this assignment is null and void.*



<http://www.springer.com/journal/773>

Journal of Marine Science and Technology  
Official Journal of the Japan Society of Naval Architects  
and Ocean Engineers (JASNAOE)

Editor-in-Chief: Takagi, K.

ISSN: 0948-4280 (print version)

ISSN: 1437-8213 (electronic version)

Journal no. 773

Signature  
Name (printed): Kimitaka Kawanishi

Affiliation: Norwegian University of Science and  
Technology, Center for Cyber and Information Security

Date: 28 December 2017

If the paper is rejected this assignment is null and void