SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures

Christian Hemminghaus*°, Jan Bauer*, Konrad Wolsing*•

*Fraunhofer FKIE
Cyber Analysis & Defense
Wachtberg, Germany

°University of Bonn
Security and Networked Systems
Bonn, Germany

•RWTH Aachen University
Communication and Distributed Systems
Aachen, Germany

{christian.hemminghaus, jan.bauer, konrad.wolsing}@fkie.fraunhofer.de

***Abstract*—Distributed maritime bridge systems are customary standard equipment on today's commercial shipping and cruising vessels. The exchange of nautical data, e.g., geographical positions, is usually implemented using multicast network communication without security measures, which poses serious risks to the authenticity and integrity of transmitted data. In this paper, we introduce digital SIGnatures for MARitime systems (SIGMAR), a low-cost solution to seamlessly retrofit authentication of nautical data based on asymmetric cryptography. Extending the existing IEC 61162-450 protocol makes it is possible to build a backward-compatible authentication mechanism that prevents common cyber attacks. The development was successfully accompanied by permanent investigations in a bridge simulation environment, including a maritime cyber attack generator. We demonstrate SIGMAR's feasibility by introducing a proof-of-concept implementation on low-cost and low-resource hardware and present a performance analysis of our approach.**

***Index Terms*—Maritime Cyber Security; Authentication; Integrity; IEC 61162-450; NMEA 0183**

I. Introduction

The vast majority of goods transported by many countries travel by sea. As an important driver of the global economy, but also because of the national supply of essential goods and the transport of dangerous cargoes, the shipping industry must be classified as critical infrastructure. Like all branches of industry, the shipping industry has been revolutionized by digitization. Furthermore, the emergence of civil global navigation satellite systems (GNSSs), primarily the Global Positioning System (GPS), has fundamentally changed navigation in shipping. Today's vessels heavily depend on cyber-physical systems with highly interconnected sensors and actors that are integrated into so-called maritime systems. Those systems greatly support navigation by integrating and cross-validating nautical data. An electronic chart display and information system (ECDIS) displays nautical data in an optimized format, which enables the changeover to electronic nautical charts (ENCs) and brings considerable advantages in decision support and automation, not only with regard to navigation [15]. At the same time, however, certain dependencies from a functioning and available maritime infrastructure arise, which is by no means immune to cyber attacks [16].

Unlike technologies in other economic sectors, vessels come with a long operation time and, as maritime systems are strongly embedded, accordingly outdated technologies are used. Hence, in practice, they are very vulnerable and lucrative targets to cybercrime. This vulnerability becomes an increasingly threatening challenge with national interest.

In the context of Maritime Cyber Security (MCS), research has recently revealed various attack surfaces [5], [6], [16], such as GNSS [3], the automatic identification system (AIS) [2] or very-small-aperture terminals (VSATs) [12]. Other attacks try to undermine the security of integrated bridge systems (IBSs) [1], [10], [11] by manipulating the communication of sensitive data for situational awareness. Because bridge crews are usually unaware of cyber risks and not trained to respond appropriately, the integrity and authenticity of data transferred to an ECDIS are of utmost importance, from an MCS perspective. For this reason, we present a security framework enabling a cost-effective approach for retrofitting authentication and integrity of nautical data to maritime systems. Overall, the contribution of this paper can be summarized as: i) a cyber security threat analysis for inside attacks on the IBS in maritime systems, ii) *SIGMAR*, a holistic framework tailored to retrofit digital *SIGnatures for MARitime systems*, and iii) a qualitative security assessment, as well as, a feasibility study of our approach including a technical performance evaluation.

The remainder of the paper is organized as follows. Section II provides a brief background on maritime systems. Then, a cyber threat analysis is conducted including related work (Sec. III), before our security framework is introduced along with a discussion of its security features (Sec. IV). Afterward, in Section V, a performance analysis of SIGMAR is conducted. Finally, the last section concludes the paper.

II. Maritime Background

Maritime systems onboard modern vessels provide up-to-date situational awareness and decision support through a distributed sensor network. Such aids, in part already combined with automation, enable a significant reduction in the number of crew members of today's vessels while increasing maritime safety. Maritime systems of commercial shipping, e.g., cargo ships and tankers, but also of cruising vessels, usually consist of information technology (IT) and operational technology (OT) networks. While the latter are generally traditional industrial control systems, e.g., for control of the engine and ballast water systems, the former enable IBSs and rely on IEEE 802.3 Ethernet as a well-established standard for the communication of nautical data.

 DOI: 10.1109/ISNCC52172.2021.9615738

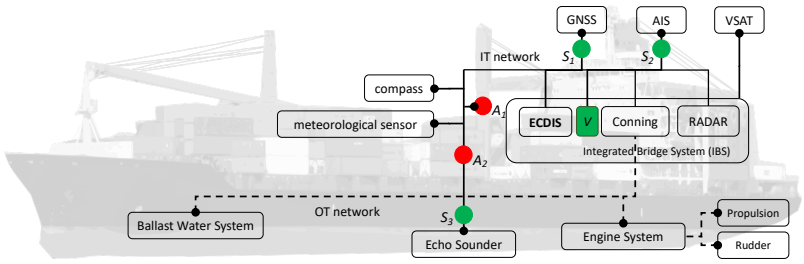


Fig. 1. An exemplary architecture of a typical maritime system onboard commercial vessels, cf. [3], [11], [15]. A distributed IEC 61162-450 IT network connects various sensor and actor devices distributed across the vessel to the IBS. Due to the lack of physical protection of long cable runs, there is a risk of cyber attacks, either as PotS (A_1) or PitM (A_2), which can be mitigated by SIGMAR components (S_i and V).

Typical components connected within suchlike IT networks comprise: i) computer-based navigation systems, known as ECDISs, GNSS receivers, an AIS transceiver, a maritime radar system for collision avoidance, echo sounders, meteorological sensors, and numerous other advanced electronics, ii) the conning workstation also connected to the OT network with engine and ballast water systems, which possibly has an interface for autopilot features offered by the IBS, and iii) a voyage data recorder (VDR). Furthermore, VSATs provide permanent Internet connectivity not only for the mentioned components but often also for additional services such as crew welfare and passenger entertainment systems. Many of these components are defined as mandatory for vessels of a certain size by the International Maritime Organization (IMO) [14]. For this reason, such vessels usually have maritime systems, which are built according to the scheme shown in Fig. 1.

The serial exchange of nautical data between marine electronics within the IT network is usually done using NMEA 0183, a standard that was initially defined in the 1980s by the National Marine Electronics Association and specifies a set of ASCII-based datasets to encode nautical information, so-called NMEA sentences with a maximal length of 82 characters. Nowadays, NMEA sentences are widely established as an encoding format even beyond shipping, e.g., also for data transfer from standard GPS receivers to PCs. To make use of common network technology in maritime systems, manufacturers started to use NMEA sentences to provide nautical information via TCP or UDP. This gave rise to the Lightweight Ethernet (LWE) protocol which was standardized in IEC 61162-450 [8] in 2011 and enables multi-sender, multi-receiver communication in maritime systems.

From a technical perspective, IEC 61162-450 bases on the UDP/IP stack. It uses IPv4 multicast with individual receiver groups according to the equipment type. However, because of the assumption of air-gapped systems, IT security initially did not play any role in designing the standard. Thus, the communication, even of sensible nautical information for ENCs, route planning, and autopilot commands, is not protected. Only in a recent version of the standard (2018) [8], a simple message authentication code (MAC) option was added, suggesting MD5 as the default hash algorithm which is known to be insecure for digital signatures [17].

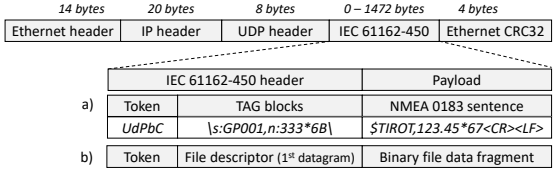


Fig. 2. PDU format of IEC 61162-450 datagram encapsulated in an Ethernet frame a) of an NMEA 0183 sentence and b) of a *binary* message.

The payload sent by the IEC 61162-450 is encapsulated in UDP datagrams, cf. Fig. 2. There are basically two types of payloads: *NMEA sentences* and *binary* files, which are distinguished by a token in the header. For NMEA sentences, one or more transport annotate and group (TAG) blocks are added for additional information (separated by \), before the actual data. Each TAG has a maximum size of 80 bytes and contains comma-separated key-value pairs, e.g., `s:GP0001` for source identification (ID). A two-digit XOR-based checksum is included at the end of each TAG block. The NMEA sentence begins after the last TAG block and starts with the typical `$`.

Compared to NMEA sentences, binary files can be of arbitrary length and, thus, are typically fragmented into a sequence of several IEC datagrams due to the maximum transmission unit of Ethernet. The first binary fragment in a sequence includes a *binary file descriptor* that, among others, contains information about the number of fragments (Fig. 2).

III. Cyber Threat Analysis

In practice, no two vessels are alike. Even the vessels of the same shipping company, manufactured in the same shipyard, are unique. Thus, their onboard maritime systems are also individual, which poses challenges to generic MCS. Nevertheless, as mentioned in the previous section, there are common similarities in their network architecture, cf. Fig. 1. This architecture and its components reveal different attack surfaces for cyber attacks as surveyed, e.g., in [6], [16]. Cyber threats in the maritime domain are not new. From various historical incidents, it is known that maritime systems are not immune to attacks [1], which attracted the attention of security research and produced comprehensive risk analysis [4], [16].

Cyber attacks can have different motivations. They can be carried out by generic hackers, activists, competitors, or even terrorists for economic or idealistic reasons [4]. According to [16], the three top categories of cyber risks are IT, OT, and human elements. Furthermore, attacks can generally be executed by *external* or *internal* attackers. External attackers could remotely attempt to mislead the navigation, e.g., by spoofing GPS signals [3] or to eavesdrop VSAT traffic, as recently demonstrated in [12]. The latter can pave the way for the attacker to get illegitimate access to sensible information enabling further attacks and eventually gaining full access to internal networks, thus, bridging the air gap.

Once having access to the maritime IT system, an attacker can pursue various objectives. To eavesdrop (passive), actively craft nautical messages, or carry out replay attacks, solely network access is required, i.e., a Person-on-the-Side (PotS) position. In case the attacker could gain a Person-in-the-Middle (PitM) position, further more powerful attacks are possible, which intercept, drop, delay, or even manipulate legitimate datagrams (impersonating its origin or forging its content). By this means, the attacker can make the vessel unmaneuverable or mislead the navigation, which can lead to collisions and serious damage. Therefore, the unprotected delivery of nautical messages via IEC 61162-450 poses a great danger.

Conventional countermeasures comprise *physical security* preventing intruders from entering a vessel, *perimeter security* blocking external cyber attacks, and generic *network security* [5]. In this paper, we focus on preventive security measures in case those conventional countermeasures are overcome. Hence, we consider internal attacks against the IT network, i.e., by both PotS (A_1) and PitM (A_2) attackers, as sketched in Fig. 1. Therefore, we propose a security framework that adds authenticity and integrity to nautical datagrams of the IEC 61162-450 standard by retrofitting specific low-cost hardware components (S_i and V). However, it should be noted that our framework cannot prevent Denial of Service (DoS) attacks that jam the shared medium.

The latest version of the IEC 61162-450 [8] standard introduces optional authentication, which is a simple MD5 MAC for a message m that is concatenated with a key k, i.e. $\texttt{MD5}_k(m) = h(k||m)$. However, MD5 is generally considered broken [17] and suchlike simple implementations are vulnerable to collision and length extension attacks. Thus, authenticity cannot be guaranteed by the standard.

To the best of our knowledge, there is no related work directly addressing the authenticity of nautical data exchange in maritime systems. However, with respect to the automotive sector that is exposed to similar security challenges, there are many approaches to retrofit authentication to Controller Area Networks (CANs), mainly based on keyed-hash MACs (HMACs) [7]. HMACs use cryptographic hash functions and depend on pre-shared keys. They are not prone to length extension attacks, but non-repudiation cannot be ensured because of common keys.

Intrusion Detection Systems (IDSs) represent a complementary method, often achieving a reasonable resource requirement without additional communication overhead. Content-based multi-sensor anomaly detection, for instance, can protect against manipulated messages. In addition, IDSs can also be used for sender identification, as recently demonstrated in the automotive sector [9]. Both methods can prevent external attacks, but they do not necessarily offer sufficient protection against sophisticated insider attacks.

A. Attack Scenario

The design of our framework is based on the following assumptions. We assume that all devices at the bridge, particularly the ECDIS and at least important nautical sensors, are deployed in a physically protected environment. However, due to the vessel's physical size, long cable runs cannot be considered secure and are potentially exposed to network attacks. Thus, we focus on PotS and PitM attacks exploiting unsecured cable runs, cf. Fig. 1. External attackers purposely interfering with sensors from outside the vessel, e.g., physical GPS spoofing, are out of scope.

IV. Adding Authenticity to Nautical Datagrams

A. Security Goal

As a fundamental preventive security measure to ensure authenticity and integrity of message transfer in general and nautical datagrams in particular, it is inevitable to incorporate cryptography into the communication. However, maritime systems are strongly embedded. A replacement of existing devices is difficult, labor-intensive, and time-consuming. Thus, particularly from an economic perspective, a replacement is usually simply too expensive. Moreover, because many devices in maritime systems, such as highly optimized sensors and actors, have only limited computing power and resources, the execution of computationally intensive operations might not always be possible with regard to time-critical transmissions. Therefore, our main goal is to design an inexpensive yet effective approach to retrofit cryptographic security into existing legacy maritime systems. The retrofitting should be minimally invasive, i.e., with minimal changes with respect to their underlying network and existing communication protocols.

B. Concept

As already discussed in Section III, authenticity and integrity can be ensured either by MACs using symmetric keys for cryptographic hash functions or by digital signatures using asymmetric cryptography. Both, if carefully implemented, ensure that attacks on the authenticity and integrity of datagrams are detectable. The crucial advantages of our decision to rely on signatures are threefold: the easier key distribution and management, a lower risk in case individual devices are compromised, and the non-repudiation property, providing a considerable added value for the recording in VDRs.

1) Requirements for Cryptographic Algorithm: To integrate digital signatures into IEC 61162-450, it is necessary to distinguish between NMEA and binary payloads. Regarding NMEA messages, TAG blocks in the IEC header can be leveraged by defining new TAGs, especially for signatures. The IEC PDU has a maximal length of 1472 bytes (cf. Fig. 2), while the maximum length of NMEA sentences is only 82 bytes. Even taking into account already existing IEC TAGs, the maximal PDU length leaves enough room for common signatures. However, one has to consider that additional signatures will increase the communication overhead and that the length of each TAG block is restricted to 80 bytes, already including 5 bytes for control characters and a checksum. Hence, to maintain compatibility with the standard, a signature size ≤ 75 bytes is desirable. Concerning binary transmissions, we identified the *status and information text* field in the first fragment's

header to be a reasonable candidate to retrospectively include the signature. It allows for a string of arbitrary length.

Besides the signature size, an important requirement for the cryptographic algorithm is a low computational effort, at least for signing due to low-resource adapters. In contrast, the verification is assumed to be performed centrally by a single, more powerful device and, thus, does not need to be computationally efficient. Finally, the algorithm should achieve a NIST security level of 128 bits for symmetric cryptography (comparable to a 3072 bits RSA).

2) Cryptographic Algorithms: We compared available cryptographic algorithms with regard to their suitability in maritime systems concerning the metrics above. Only two of these algorithms that fulfill the requirements are presented here. Multivariate cryptography is considered efficient, especially for signing, and achieves short signatures. Signatures generated by Rainbow with a 128-bit security level, for instance, have a size of 372 bits only. Another approach is offered by elliptic curve cryptography, which is successfully applied even in the context of Wireless Sensor Networks. The elliptic curve digital signature algorithm (ECDSA) is an established algorithm of this class. It is also characterized by short signatures and moderate performance, even on devices with limited resources.

For the NIST recommendation of a 128-bit security level, ECDSA (P-256) provides comparable security with a signature size of 512 bits. The comparative performance evaluation in [13] shows that depending on the implementation, ECDSA is significantly faster than Rainbow. For this reason, we consider the former to be the most reasonable choice for being retrofitted to maritime systems, although the communication overhead will be slightly higher due to longer signatures.

3) Signing and Verification: The digital signature is generated using the hash of the original IEC message, which already contains a source ID TAG that is crucial for the later validation of authenticity. However, to prevent replay attacks, sequence numbers or timestamps are furthermore needed. Since timestamps allow a stateless implementation that is more flexible, particularly in multicast systems, we use this altering information for replay mitigation. Timestamps are implemented by an additional TAG in the IEC message.

Once the signature is computed, it is Base64 coded, which is required to avoid possible conflicts with control characters. As a result, the signature size is increased to 680 bits, which exceeds the maximum length of a TAG. Thus, for NMEA datagrams, signatures need to get split into two successive TAGs. Although there are no such length limitations for signatures in binary datagrams, our NMEA TAG format (source `s:`, timestamp `t:`, and signature `y:`) is adopted for the sake of consistency. However, in the likely case, a binary transmission is fragmented into several IEC datagrams, the adapter first needs to receive all fragments until it can proceed with signing or verification processes, which implies a certain latency.

In the verification process, the integrity is initially checked by all checksums and then the validity of the timestamp, i.e., if the datagram is received within a certain threshold (currently 10 s). Finally, the actual signature is validated using the public key belonging to the source ID found in the message.

C. System Architecture

The network architecture of our approach is sketched in Fig. 1 based on a simplified maritime system. SIGMAR extends an existing system consisting of various IEC 61162-450-compliant sensor and actuator devices connected to one (or more) ECDISs by three additional components: i) a *SIGMAR adapter* (S_i) that is responsible for signing the messages of source devices, ii) a *SIGMAR verifier* (V) handling the verification of signatures, and iii) a *SIGMAR certificate authority (CA)* including a certificate repository that provides the system's public key infrastructure (PKI). All components are assumed to be physically protected against unauthorized access and, thus, to be trustworthy. Therefore, *SIGMAR adapters* are placed in the close vicinity of certain sensors transmitting IEC 61162-450 datagrams that are worth protecting, e.g., GNSS or AIS devices. To this end, adapters (S_i) are added to the network as gateways, directly "behind" the sensor, cf. Fig. 1. To minimize potential interferences with the existing system, adapters retain original IP addresses in outgoing packets. Whereas multiple adapters can coexist in a retrofitted maritime system, only a single verifier and a single CA is required, unless for redundancy reasons. Unlike adapters, both components are connected to the network like usual devices and can run on a shared physical host system.

To secure the maritime system, individual key pairs and the CA's root certificate are pre-installed on each component prior to its deployment. When a certain adapter is installed on a sensor, it has to be initially registered at the verifier. For this purpose, the IDs of both, adapter and sensor, and its *scope*, i.e., the type of IEC 61162-450 datagrams the sensor creates, are transferred to the verifier, already along with a valid signature.

As a regular network device, the verifier operates in parallel. Hence, verifications of signatures do not cause latency to the system and do not affect existing receivers. A verifier continuously monitors the entire network traffic. Whenever a datagram of any registered device is observed, the datagram is immediately inspected regarding its signature. If the datagram is signed, its authenticity and its validity are further checked as described above. Missing public keys can be inquired from the CA on demand. In case the verification process fails, i.e., the signature is falsified, the integrity is violated, the datagram is outdated, or the sensor data are out of a registered scope, a potential attack is detected. Thus, a corresponding alert is triggered, including information about its cause and all devices involved. The same holds for the observation of illegally unsigned datagrams from registered sensors. Moreover, the initial registration of scopes also enables the validation of the sender's authorization for communicating certain data. Hence, datagrams containing data that is out of the scope of the corresponding sender can be classified as unauthorized transmissions and will be reported as well.

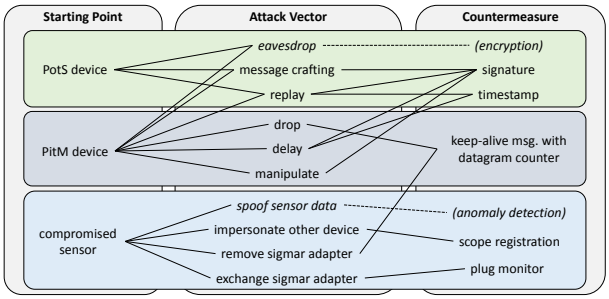


Fig. 3. Threat model of internal network attacks on nautical communications originating from various starting points and our preventive countermeasures.

D. Security Considerations

Concrete reactive countermeasures against such attacks are out of the scope of this paper and are also generally difficult to define or even to automate. In practice, therefore, the primary goal is to alert the crew and provide adequate situational information. Hence, the latency introduced by the verifier's processing (time-to-alert) is negligible because of its parallel operation that does not affect the original data flow between senders and receivers. However, in future autonomous maritime systems, adequate and timely countermeasures have to be considered and implemented. In suchlike scenarios, multiple verifiers in gateway positions, similar to the adapters, or integrated verifier software implementations within receiving devices would be a reasonable option.

Furthermore, despite the assumption of physically protected environments for trustworthy sensors and their adapters (cf. Sec. III-A), (un)plugging events of Ethernet cables are monitored and reported by adapters. Moreover, periodic and signed keep-alive messages are foreseen for SIGMAR adapters that include the number of outgoing datagrams within the last period. In this way, not only can the presence of an adapter be monitored, but attacks that specifically intercept and drop individual messages can also be detected. However, those features shift SIGMAR towards an IDS. As they are not our focus, details are not discussed further here.

In conclusion, the security features enabled by SIGMAR are summarized in Fig. 3 and confronted with the possible cyber attacks from the threat analysis in Section III. Note that the risk of eavesdropping could be mitigated by encryption. However, this risk is assumed to be uncritical, since the security goal of confidentiality, if at all, plays only a minor role in maritime systems, at least for civilian and commercial shipping. Furthermore, bogus information generated by a compromised sensor cannot be counteracted with our approach.

E. Implementation

The proof-of-concept implementation of SIGMAR is deliberately lightweight, modular, and open-source. It is based on Python 3 using *Scapy* for packet-level processing and *OpenSSL* for cryptography. Thus, SIGMAR components can be executed on standard Linux systems, also on low-cost system-on-a-chip platforms, such as the Raspberry Pi family. It is developed using a special virtualized testing environment allowing distributed setups according to Fig. 1. Also, the execution of various simulated attacks on the network layer is possible, enabled by a comprehensive attack framework ranging from simple replay attacks to sophisticated GPS spoofing beyond SIGMAR's scope. Moreover, real-world network traces from the maritime domain can be imported for simulation purposes. By doing so, we used a trace collected from a research vessel (Deneb) to continuously evaluate SIGMAR's security countermeasures during the development with regard to potential attacks mentioned in Section III.

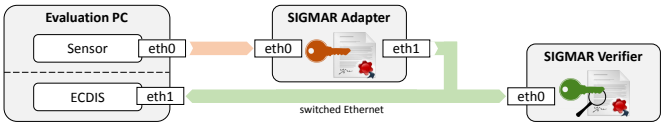


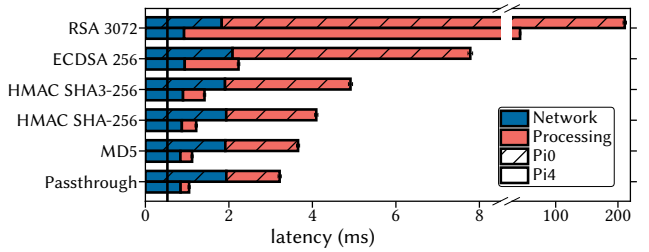
Fig. 4. Setup used for the performance analysis. The originally insecure communication between *sensor* and *ECDIS* is extended by a SIGMAR adapter as a sensor gateway that adds digital signatures to nautical datagrams. A dedicated verifier monitors message authentication and sensors' authorization.

V. Performance Evaluation

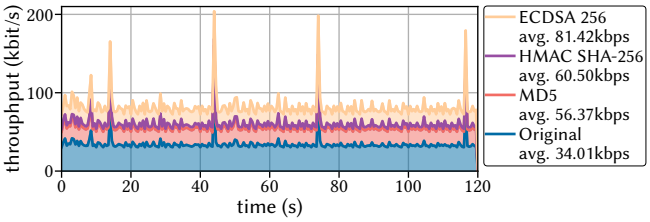
A. Evaluation Setup & Methodology

The performance evaluation is focused on two relevant metrics: the *latency* caused by the SIGMAR adapter and the resulting *communication overhead*. It was conducted using a simplified evaluation setup shown in Fig. 4. It consists of a bundle of representative sensors that are aggregated in a single IEC 61162-450-compliant sender and an ECDIS acting as a corresponding receiver. Initially, the communication between both devices is inherently insecure because of the lack of authentication. According to the system architecture described in Section IV-C, a SIGMAR adapter is added to the sensor. It operates as a signing gateway that adds signatures using its private key while forwarding datagrams from the ingress (eth0) to the egress (eth1) network interface (100Base-TX). Next, a SIGMAR verifier complements the setup, which is responsible for signature verifications using the adapter's corresponding public key. Technically, to bypass time synchronization issues, a fully-equipped computer is used as an evaluation PC running both instances, sensor and ECDIS assigned to individual network interfaces, cf. Fig. 4. The adapter is installed on a small, low-cost commercial off-the-shelf device, namely a Raspberry Pi zero (1 GHz CPU, 512 MB RAM). We also used a less resource-constrained Pi 4 (4x1.5 GHz CPU, 4 GB RAM), particularly recommended for the central verifier.

Two setups are considered, each with NMEA 0183 datagrams (captured from Deneb) and synthetic binary transmissions. First, the original maritime system without additional security instances serves as a baseline for the evaluation (*original*), measuring latency and throughput from sensor to ECDIS. Second, this setup is extended by SIGMAR. We differentiate between pure datagram forwarding (*passthrough*) and actual authenticated forwarding. The processing delay, including the cryptographic signing process, is also separately recorded. In these setups, we compare our solution against the MAC approaches (IEC's MD5 and a common HMAC) and also include RSA as an ECDSA alternative for comparison.



(a) Latency of NMEA datagram transfer induced by SIGMAR adapters.



(b) The impact of additional signatures on communication overhead.

Fig. 5. Evaluation results regarding different cryptographic methods used for authentication of IEC 61162-450 datagrams.

B. Results

The results concerning the latency induced by SIGMAR adapters to the original IEC 61162-450 network are visualized in Fig. 5(a). It is successively measured for 100 NMEA datagrams for different authentication approaches. The original delay for the transmission of datagrams from sensor to ECDIS (≈ 0.53 ms) is included as a vertical baseline. The figure shows the inherent network delay (blue) caused by the addition of the adapter and the processing delay (red). The latter contains latencies of datagram processing and of cryptographic operations. As expected, increasing cryptographic complexity leads to a significant increase in the overall latency. The preferred ECDSA, with its advantages, turned out to be very efficient and, compared to the MAC variants, achieves a reasonable tradeoff between latency and cryptographic security. Regarding its RSA counterpart, ECDSA is orders of magnitude faster. Furthermore, the more performant Pi 4s are suitable for higher workloads (in the verifier). However, the results of the Pi zero are considered to be sufficient in practice.

The corresponding latencies evaluated for binary transmissions and the verifier are similar but not further discussed due to space limitations. Instead, the overhead is investigated. Fig. 5(b) shows the throughput exemplary extracted from the traffic of the Deneb trace. It can be seen that the additional overhead increase is relatively constant, depending on the signature size of the respective authentication method. Apart from that, the traffic pattern remains very similar. Even with SIGMAR, only a low network capacity is required. Overall, it can be concluded that, even with low-cost hardware, the cost of our approach is acceptable and justifies the security gains.

VI. Conclusion

In this paper, we presented SIGMAR, a holistic security framework for retrofitting authentication to nautical communication in the context of onboard maritime networks. It is designed to remain compatible with the existing IEC 61162-450 standard and extends it with digital signatures. Using ECDSA, it is demonstrated to achieve reasonable performance even with low-cost hardware. In our future work, we plan to deploy our framework on a real vessel. We are also considering investigating the feasibility of our approach regarding NMEA 2000 that is relevant for leisure marine applications.

Acknowledgments

The work in this paper was partially funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) as part of the ACTRESS project. Additionally, the authors thank the German Federal Maritime and Hydrographic Agency (BSH) for giving us access to their research vessel.

References

[1] M. S. K. Awan and M. A. Al Ghamdi, "Understanding the Vulnerabilities in Digital Components of An Integrated Bridge System (IBS)," *Journal of Marine Science and Engineering*, vol. 7, no. 10, pp. 1–20, Oct 2019.

[2] M. Balduzzi, A. Pasta, and K. Wilhoit, "A Security Evaluation of AIS Automated Identification System," in *Proc. of the Computer Security Applications Conf. (ACSAC)*, New Orleans, LA, USA, 2014, pp. 436–445.

[3] J. Bhatti and T. E. Humphreys, "Hostile Control of Ships Via False GPS Signals: Demonstration and Detection," *Journal of the Institute of Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[4] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos, "A novel cyber-risk assessment method for ship systems," *Safety Science*, vol. 131, pp. 14, art. no. 104 908, 2020.

[5] D. Bothur, G. Zheng, and C. Valli, "A critical analysis of security vulnerabilities and countermeasures in a smart ship system," in *Proc. of the Australian Information Security Management Conf. (AISM)*, Perth, Australia, 2017, pp. 81–87.

[6] M. Caprolu, R. D. Pietro, S. Raponi, S. Sciancalepore, and P. Tedeschi, "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead," *IEEE Communications Magazine*, vol. 58, no. 6, pp. 90–96, 2020.

[7] B. Groza and P. Murvay, "Security Solutions for the Controller Area Network: Bringing Authentication to In-Vehicle Networks," *IEEE Vehicular Technology Magazine*, vol. 13, no. 1, pp. 40–47, 2018.

[8] IEC 61162-450:2018, "Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection," International Electrotechnical Commission (IEC), Tech. Rep., 2018.

[9] M. Kneib, O. Schell, and C. Huth, "EASI: Edge-Based Sender Identification on Resource-Constrained Platforms for Automotive Networks," in *Proc. of the Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, USA, 2020, pp. 1–16.

[10] M. S. Lund, J. E. Gulland, O. S. Hareide, Ø. Jøsok, and K. O. C. Weum, "Integrity of integrated navigation systems," in *Proc. of the Conf. on Comm. and Network Security (CNS)*, Beijing, China, 2018, pp. 1–5.

[11] M. S. Lund, O. S. Hareide, and Ø. Jøsok, "An attack on an integrated navigation system," *Necesse*, vol. 3, no. 2, pp. 149–163, 2018.

[12] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "A Tale of Sea and Sky On the Security of Maritime VSAT Communications," in *Proc. of the IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2020, pp. 1384–1400.

[13] M. Sjöberg, "Post-quantum algorithms for digital signing in Public Key Infrastructures," Master's thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2017.

[14] SOLAS Chapter V – 1/7/02, "Safety of Navigation," International Maritime Organization (IMO), Tech. Rep., 2002.

[15] B. Sviličić, M. Kristić, S. Žuškin, and D. Brčić, "Paperless ship navigation: cyber security weaknesses," *Journal of Transportation Security*, vol. 13, pp. 203–214, 2020.

[16] K. Tam and K. Jones, "Factors affecting cyber risk in maritime," in *Proc. of the Int. Conf. on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Oxford, United Kingdom, 2019, pp. 1–8.

[17] X. Wang and H. Yu, "How to Break MD5 and Other Hash Functions," in *Proc. of the Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, Aarhus, Denmark, 2005, pp. 19–35.