Keeping the Baddies Out and the Bridge Calm: Embedded Authentication for Maritime Networks

Lucca Ruhland[•°], Mari Schmidt[•], Jan Bauer[•], Elmar Padilla[•]
[•]Fraunhofer FKIE, Cyber Analysis & Defense [°]University of Bonn
Wachtberg, Germany Bonn, Germany
{forename.surname}@fkie.fraunhofer.de

***Abstract*—Integrated bridges of today's vessels are complex and distributed maritime systems that interconnect versatile electronic equipment. However, digitized vessels have long ceased to be isolated systems and are thus increasingly vulnerable to cyber attacks. In this context, integrity and authentication of the communication onboard is crucial. Therefore, we introduce *MARMAC*, a low-cost solution to retrofit authentication of nautical communication. *MARMAC* is based on symmetric cryptography and extends the prevalent IEC 61162-450 protocol enabling a backward-compatible solution which mitigates common attacks. Using a specific gatekeeper approach, *MARMAC* can prevent unauthenticated messages from being processed that could otherwise affect the nautical situational awareness on the bridge. Our approach is evaluated using real network traffic in a laboratory testbed with low-cost hardware, highlighting its feasibility and potential to secure existing maritime systems.**

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

I. Introduction

Maritime transportation is the main driver of world trade and the global economy. The shipping industry transfers the vast majority of goods across the entire globe. As it secures global supply chains and is responsible for the national supply of vital goods, it represents a critical infrastructure. This increases the need for operational safety in general and for cybersecurity in particular. Therefore, maritime infrastructures urgently need to be protected and hardened against existing threats from cyberspace. While the security of IT and industrial control systems in coastal infrastructures, such as ports and transshipment facilities, is addressed by traditional security measures in appropriate standards and guidelines [1], the protection of existing maritime systems onboard vessels lags behind. For far too long, ships have been seen as isolated systems. However, with increasing digitization and permanent connectivity to shore-based systems, they are confronted with public networks that inevitably close the original air gap. As a result, these rarely secured systems become lucrative targets for a plurality of cyberattacks [2], [3].

Looking at reported maritime cyber incidents [4], a threatening picture emerges for this sector. Although port and hinterland infrastructures are the main target, there have also been an alarming increase of attacks on maritime systems onboard. Consequently, security research is concerned with the identification of security vulnerabilities and the development of adequate countermeasures for those systems.

Today, modern maritime systems combine a variety of different embedded and highly networked nautical sensors and aggregate their rich information in a so-called integrated bridge system (IBS), which represents an important interface between the cyber (sensors) and the physical domain (actuators, i.e., propulsion systems and rudders). Inspired by the Internet of Things, it is increasingly networked with the outside world. In the IBS, an electronic chart display and information system (ECDIS) further processes nautical data enabling a precise situational picture providing decision support for navigators as well as automation benefits [5]. At the same time, however, there are certain dependencies on functioning, available, and reliable instruments on the bridge, which are currently still not sufficiently protected against cyberattacks [2].

Maritime security research has revealed various attack vectors against IBSs, including attacks on the global navigation satellite system (GNSS), the automatic identification system (AIS), and satellite communication [2], [3]. Further attacks aim to undermine security by disrupting and altering nautical data transmitted to the bridge at the network level in order to intentionally manipulate situational awareness [6]. If such attacks are carefully carried out, they are difficult to detect. Crews also often lack the necessary awareness of cyber risks and due to missing trainings cannot respond appropriately [7].

In addition to well-known security measures, such as regular installations of security updates to close existing vulnerabilities, ensuring the integrity and authenticity of data in transit is of utmost importance. However, vessels come with long operation times. Thus, often outdated technologies are used, which are highly embedded and cannot be exchanged without considerable effort. Hence, retrofittable, yet effective, security solutions are crucial, but also challenging.

To address this challenge, we present *MARMAC (MARitime multi-Message Authentication Code)*, a low-cost security solution to seamlessly retrofit nautical data authentication into existing maritime systems in a performant manner. Unlike previous approaches that only allow monitoring of authenticity [8], our goal is to develop a gatekeeper that prevents non-authenticated message delivery to the sensitive IBS (*keeping the baddies out...*). The advantage of this rigorous prevention over monitoring lies in safety, because instead of being warned, which may lead to irritations in already safety-critical situations, the crew is freed from manual, reactive measures by our holistic protection (*... and the bridge calm*). The gatekeeper approach is also in line with common recommendations of

 DOI: 10.1109/ISNCC55209.2022.9851819

network segmentation according to IEC 61162-460, the current security standard for maritime networks. Because of the further increase in digitization, which will, e.g., integrate a large number of environmental sensors in many cargo ship containers into the future situation picture on the bridge, a corresponding increase in the network load must be assumed, which is coped by our high-performant solution.

Starting with brief background information on maritime systems, on IBSs, and the nautical data communication (Sec. II), we analyzed cyber threats (Sec. III). These yield our attacker model, from which we derive requirements for a secure protocol extension that allows our backward-compatible solution. Based on available general approaches (Sec. IV), we select a suitable method that we adapt for maritime systems (Sec. V). Using an experimental hardware setup consisting of low-cost off-the-shelf hardware devices, we successfully evaluate our approach. Overall, our contributions comprise:

- *MARMAC*, a low-cost retrofitting of secure authentication for maritime networks using symmetric cryptography,
- a security gatekeeper in front of the IBS,
- a quantitative feasibility study of our approach based on a technical performance evaluation.

II. Maritime Systems & Networks

Progressive digitalization in shipping has led to complex maritime cyber-physical systems, which networks versatile sensors and actuators onboard with modern network technology and bundles the control systems in the IBS. Systems of commercial shipping, from cargo ships to cruising vessels, usually rely on common Ethernet-based technology (IEEE 802.3) for communication, which has also gained acceptance in many other areas due to its advantages in terms of data rate, cost efficiency, flexibility, and distribution.

Maritime systems include various devices, sensors, and receivers distributed over the vessel. These usually comprise several GNSS receivers for localization, marine radar and an AIS receiver. AIS is a periodic radio broadcast system used to exchange vessels' IDs, position, and course information with each other. Together with the radar, the received AIS signals forms a crucial basis for safe ship operation. Especially in difficult visibility conditions, they serve to prevent collisions with landmass and other ships and are, therefore, internationally mandatory in accordance with the SOLAS Agreement [9]. Additionally, there are further nautical sensors, such as an echo sounders, speed logs, compasses, as well as anemometers.

Via the shared network, the versatile data of those devices are transferred to the IBS. On the bridge, an ECDIS in combination with a radar display provides navigators with a precise and up-to-date nautical situation picture and supports them in their navigation decisions. The conning console and also an autopilot interface offered the by IBSs are responsible for controlling propulsion systems and ships' rudders. Finally, it should be mentioned that commercial IBSs are typically connected to the Internet via satellite communication and thus usually in constant contact with the associated shipping company's fleet operations center.

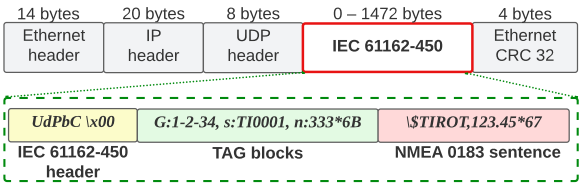


Fig. 1. IEC 61162-450 [10] datagram format of an NMEA 0183 sentence encapsulated in an Ethernet frame in the IP/UDP stack.

A. Maritime Communication Protocols

Ethernet as the basis for data transmission is supplemented by two well-established transport protocols, the connection-oriented TCP and the lightweight UDP. Sensor data is further translated into the NMEA 0183 format, developed in the 1980s. It defines NMEA sentences that are originally designed for serial data exchange between marine electronics and specifies a set of ASCII-based encodings with a maximal length of 82 characters. Due to its widespread use, even beyond the maritime domain, this legacy standard is still in use. Modern Ethernet-based maritime communication standards therefore encapsulate NMEA sentences in UDP messages, as is the case with IEC 61162-450 [10] that uses the traditional UDP/IP stack as shown in Figure 1. As a widely used maritime standard, it serves as a representative protocol in this paper. By using IPv4 multicasts with individual receiver groups according to the equipment type of the network device, it enables multi-sender, multi-receiver communication in maritime systems.

There are two basic types of IEC payloads which differ in their headers, i.e., *UdPbC \x00* for NMEA sentences transmitting nautical data (cf. Fig. 1) and occasional *binary* transfers for larger amounts of data like chart updates indicated by *RaUdP \x00*. Because we focus on securing the former, the following considerations refer solely to NMEA sentences for reasons of space. Similar to [8], however, our solution also works with binary transfer. NMEA sentences include one or multiple TAG blocks that contain additional information about subsequent payloads, which start is indicated by \$ or \!. Each TAG has a size of $\leq$ 80 bytes. They contain comma-separated key-value pairs, e.g., *s:TI0001* representing the source ID, and a two-digit XOR-checksum at the end of each block.

However, both NMEA 0183 and IEC 61162-450 do not take cybersecurity adequately into account. Hence, the communication, particularly of sensitive information, e.g., for navigation, is rarely secured, neither concerning confidentiality nor authenticity. The current version of the IEC standard [10] only optionally proposes a simple message authentication code (MAC). Its successor, IEC 61162-460, on the other hand, is dedicated to cybersecurity and specifies segmentation into different network zones based on the industrial security standard IEC 62443. In particular, critical IBSs shall be located in secured zones. However, this standard is currently only gradually being transferred into practice and is costly to retrofit. It can therefore be assumed that the majority of vessels will continue to operate without the specified security measures for decades.

III. Cyber Threats & Security Goals

The high level of support and automation provided by the many electronic devices in maritime systems is contrasted by an increased risk from cyberattacks. Potential threats can be divided into external and internal attacks. External attacks can be carried out remotely and include, on the one hand, attacks targeting the electromagnetic spectrum, such as spoofing attacks on GNSS [11] or AIS [12] and, on the other hand, cyberattacks that exploit external satellite communications [13], the human factor, or even physical access to inject malware into maritime systems [2], [3]. While the former are out of scope for this paper, the latter open the possibility for attackers to gain access to the internal network.

According to their network access point, attackers have different capabilities. Because multicast protocols are used and communication is not cryptographically secured, an attacker can effortlessly eavesdrop on communicated information. Recorded packets can then be replayed into the network, and it is also possible to craft and inject arbitrary messages. If attackers have a Person-in-the-Middle (PitM) position, they can also discard messages, delay or alter them during forwarding. Whereas eavesdropping in these systems is usually uncritical and discarding messages is easily recognized as an error, the threat posed by deliberately altered or injected false information is significantly higher as it has the potential to unnoticeably manipulate the situation picture and decision making on the bridge. This can lead to serious consequences such as groundings and collisions and, besides economic damage, also endangers the safety of humans and the environment.

In this paper, we focus on internal network attacks. We assume an extensive network that spans the entire vessel due to the distributed sensors. This provides an opportunity for attackers with physical access to gain network access (also PitM). However, we assume that the IBS and its components are protected from direct attackers by separate physical access protection, in addition to having a dedicated data link connecting the IBS to the outside. Furthermore, we assume that only individual important nautical sensors are physically protected, but general network participants are not, which means that their compromise cannot be excluded.

Based on the above assumptions, we define the security goal to be achieved as follows. It is mandatory to protect the integrity and authenticity of sensitive nautical data to prevent harmful stealthy attacks on IBSs. For this purpose, a security gatekeeper shall be implemented on the dedicated link to the IBS that enforces this requirement and completely prevents non-authenticated data injection into the critical system. To ensure that potentially compromised devices cannot spoof authentic data from other devices, unique source authentication is also required for each device to enforce authorization on device-level. However, a PitM attack that intercepts and drops messages cannot be prevented with our approach. Yet, these attacks are easily detectable by the crew, which has contingency plans to fall back on, so rather less monetary damage is expected. External attacks are also not considered.

IV. Multicast Authentication

The integrity of digital communication also requires message authenticity, i.e., a recipient must be able to verify the message's origin. Message authenticity is generally achieved by cryptography, either by digital signatures or by message authentication codes (MACs) [14]. The former are enabled by more complex asymmetric cryptography methods, such as RSA or ECDSA, and have a number of advantages, e.g., secure group communication assuming a corresponding public key infrastructure (PKI), but are more computationally and resource intensive. In contrast, traditional MACs, such as keyed-hash MACs (HMACs), rely on symmetric cryptography and, thus, generally have a better performance. However, their integrity checks are based on a pre-shared key (PSK) to authenticate messages. Because all participants in a group have the same PSK, a certain degree of group authenticity can be ensured, but not a unique *source authenticity* [14]. This is especially the case for MD5 authentication, optionally introduced in the latest IEC 61162-450 [10]. Besides MD5 is commonly considered broken [15], the proposed implementation is vulnerable to collision and length extension attacks.

To the best of our knowledge, there is no related work addressing the authenticity of nautical communication in maritime systems, apart from our prior work SIGMAR [8]. However, SIGMAR relies on asymmetric cryptography and appears not reasonable to be used for time-critical message forwarding required for a gatekeeper. Particularly in the context of resource-constrained sensor networks, many MAC-based techniques have been proposed, which are designed for multicast communication, address low hardware capacities, and compensate for the disadvantages of conventional MACs compared to signatures [14]. These resource-efficient approaches include, i.a., TESLA [16], Multi-MAC (MMAC) [17], or the Revised Nyberg's Fast One-way Accumulator [18].

TESLA is based on one-way chains. Messages are authenticated with conventional MACs but keys required for verification are published with a certain delay. The method promises low latency and high loss tolerance, yet assumes loose time synchronization between senders and receivers, which violates the assumptions of the maritime model. Nyberg's Accumulator was also developed for multicast authentication. MACs are computed by concatenating HMACs over session keys between sender and receivers, as well as the actual message. It is assumed that all network participants have negotiated secret session keys. The MAC, the message, and the user's own session key are required for verification. A MAC is authentic, if the user's own session key was used to create it. MMAC is a source authenticity method. To create a MMAC, a unique set of keys is initially assigned to each multicast participant. For each key in the set, a conventional MAC is calculated. The concatenation of these MACs yield the MMAC *tag*. The unique key sets of all participants overlap to some extent, so that each pair of participants share individual keys. In this way, a sufficient proportion of the MMAC can always be verified by each receiver, ensuring the detection of forged MMACs.

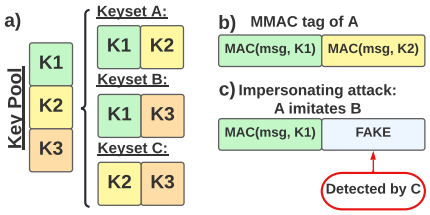


Fig. 2. Principle of MMAC, which assigns a unique key set from a secret key pool to each participant and thus enables an efficient source authentication.

V. MARMAC

To provide a fundamental level of security to maritime systems and to address the existing cyber threats identified in Section III, it is necessary to enforce source authenticity and integrity on all message transfers, in particular nautical datagrams. Due to the embedded nature of those systems, a replacement of existing devices is difficult, labor-intensive, and economically, not reasonable. As they consist of many devices, such as optimized sensors, the available computing resources are restricted, so that computationally intensive operations might not be possible regarding time-critical transmissions. Therefore, efficient yet secure cryptographic schemes to achieve the stated security goals (Sec. III) are used.

Since in our experimental comparison, MMAC performed significantly better than the Nyberg's Accumulator in terms of computational effort and communication overhead, it is selected as the method for further use in this work.

A. Multi-MAC in a Nutshell

The Multi-MAC (MMAC) scheme is a broadcast source authentication mechanism constructed from multiple MACs. Due to mutually intersecting keysets, all receivers detects attempted forgeries [17]. Figure 2 exemplarily illustrates this verification principle. Subfigure a) depicts the entire key pool, which (for simplicity of illustration) consists of three keys and the resulting keysets. Different colors represent the keys. Subfigure b) shows a valid MMAC *tag* by the owner of keyset *A* consisting of a MAC for each of its keys. Subfigure c) shows a possible MMAC forgery of *A*, who pretends to own keyset *B*. Due to the uniqueness of keysets, the adversary is still missing the key *K3* and thus has to create a fake value. Since the receiver *C* is in possession of shared key *K3*, it can easily detect the forgery by calculating the MAC using *K3* and compare it to the second MAC in the MMAC tag.

B. Adaptation of Multi-MAC

1) Modification of the Multi-MAC scheme: MMAC's size of keysets depends on the number of multicast participants. Hence, when increasing the number of participants, also the computational overhead for signing and verification increases. Thus, we propose to alter the scheme slightly to improve scalability. Divide all multicast participants into subgroups of equal size. Each subgroup uses the same key pool for creating keysets, but they have an additional and unique subgroup key, which is only issued to group members. MMAC's distribution scheme remains otherwise unchanged. This results into unique and overlapping keyset, which can be verified by all subgroup members, in particular the proposed gatekeeper.

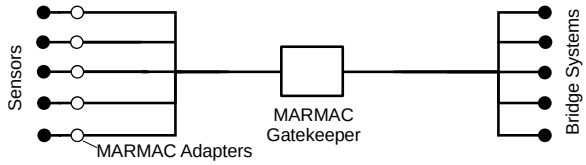


Fig. 3. *MARMAC*'s architectural concept. Dedicated adapters authenticate the output of nautical sensors and the gatekeeper prevents the forwarding of non-authenticated messages into the IBS.

2) Integration of Multi-MAC: MMAC is incorporated into IEC headers as new TAG blocks, using a custom TAG *x*, to remain backwards compatible with IEC 61162-450. This allows existing maritime devices to process the received information despite having a MMAC tag. As each TAG block holds a maximum of 80 bytes, a tag is split into multiple consecutive blocks if necessary. Since the protocol data unit (PDU) allows up to 1472 bytes and NMEA sentences are limited to 82 bytes, there is much room for an MMAC tag (cf. Fig. 1). To decrease communication overhead, it is however desirable to reduce the MAC size. Thus, an efficient MAC scheme is beneficial.

To achieve our stated security goals, these MMAC tags need to be applied to every nautical datagram. Because a replacement of maritime devices is impracticable, additional *MARMAC* adapters in between the sensors and the IBS are proposed, as shown in Figure 3. Acting as gateway, they apply MMAC tags to every IEC message before multicasting them.

3) Cryptographic Algorithms: In general, any cryptographically secure MAC can be used for MMAC. We consider a MAC suitable for usage in a retrofitted maritime system, if it holds: (i) The MAC should produce a reasonably short tag, to decrease the communication overhead, (ii) the MAC algorithm should perform moderately on resource constraint devices.

Our research has yield two suitable MAC algorithms: SipHash and HMAC-SHA-256. SipHash is a pseudorandom function (PRF) that can be used as a secure MAC if combined with a secret and provides a 128-bit security level. We propose to use the SipHash-4-8 variant with a 128 bit tag size. The resulting MMAC tag, consists in our concept of 9 individual MACs and thus has a total length 144 bytes. Additionally, SipHash is considered as very performance-efficient [19]. Since SipHash is not standardized by the NIST, as a more conservative choice, we also consider the popular HMAC-SHA-256 that also provides a 128-bit security level regarding hash collisions [20]. Due to SHA-256 producing a 256 bit hash value, the resulting MMAC tag is 288 bytes.

4) Tag Generation and Verification: MMAC tags are generated using a hash of the original IEC message. The already contained source ID TAG is later used for authenticity validation. To mitigate replay attacks, a timestamp as an additional TAG is included into the IEC message in advance. This allows a stateless verification. To avoid possible network latencies affecting the timestamp-based replay protection, a validity period of 1 s is chosen, during which timestamps are accepted by the MAC verification. In this short period,

replay attacks remain possible, but nautical datagrams delayed by this period are considered harmless, since the motion of ships is relatively inert. After computation of the MMAC tag, it is encoded in Base64 to avoid possible conflicts with reserved control characters. The tag is then also included as an additional TAG into the IEC message as described above.

On receiving an authenticated message, the receiver checks the MACs in the MMAC tag for all keys it shares with the sender. If even a single MAC is invalid, the receiver triggers an alarm. Otherwise, the receiver considers the message to be authentic and also the integrity to be valid.

C. System Architecture: Adapters & Gatekeeper

We assume a simplified maritime system as shown in Fig. 3, consisting of at least one IBS that is connected to various IEC 61162-450-compliant sensor and actuator devices. *MARMAC* extends this system by two major components, which are assumed to be physically protected and therefore trustworthy. The *MARMAC* adapters are necessary due to the impracticability of replacing existing devices. They act as a gateway and are placed in close vicinity of the sensors. Their responsibility is to incorporate MMAC tags into nautical datagrams of the source device before forwarding them.

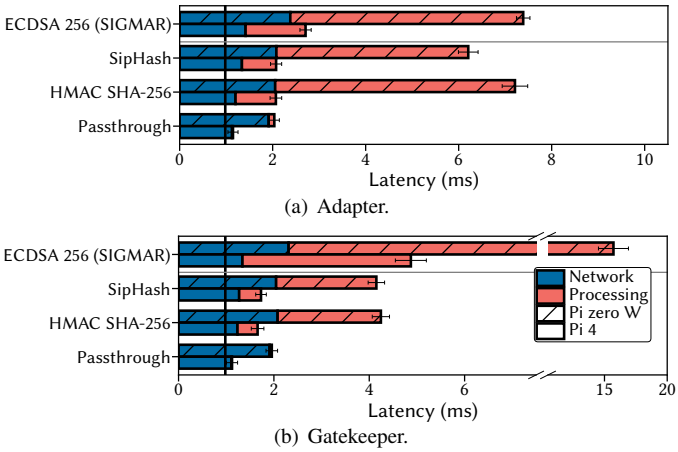
The *MARMAC* gatekeeper is responsible for actively preventing harmful stealthy attacks against the IBS by verifying MMAC tags and discarding any message with an invalid tag, such that it enforces authenticity and integrity on all nautical datagrams. Only valid messages are relayed to the IBS for further processing. Hence, *MARMAC* ensures a separation of the maritime network, so that the IBS has only access to valid data directly originating from its gatekeeper. Note that multiple adapters and gatekeepers can coexist in a retrofitted system.

VI. Performance Evaluation

A. Evaluation Setup & Methodology

The proposed concept has been prototypically implemented in Python and its performance is evaluated on low-cost hardware in terms of latency and communication overhead (Sec. VI-B) as well as maximum throughput of nautical data transfer (Sec. VI-C). The widely used single-board computer Raspberry Pi (Pi zero W and Pi 4 for a contrasting performance range) is used as these devices are assumed to have comparable resources as typical maritime network equipment and sensors. Furthermore, due to their low costs, an efficient retrofitting to secure authentication is possible.

The evaluation setup consists of the proposed *MARMAC* entities (cf. Fig. 3) and a measuring PC which represents both sensor and ECDIS and determines timestamps of in- and egress messages. For an isolated evaluation of adapter and gatekeeper, a single Raspberry Pi is sufficient. First, it is used as an adapter whose authenticated messages are stored afterwards on the PC. In a second step, it acts as gateway that validates incoming messages replayed from the PC.



(a) Adapter.

(b) Gatekeeper.

Fig. 4. Transmission delay induced by *MARMAC* entities for different cryptographic methods. Using symmetric cryptography, *MARMAC* significantly outperforms *SIGMAR* [8] (using asymmetric ECDSA 256) for the time-critical gatekeeper. The black vertical line furthermore indicates the original delay and confirms that the additional delay of our approach is quite tolerable.

B. Latency & Communication Overhead

Real-word IEC/NMEA network traffic captured from the research vessel *Deneb*[1] (39,355 messages, 11:04 min) is used in our evaluations. As a baseline, a setup modeling the original maritime system without additional security instances is considered and the latency from sensor data transit to the ECDIS is measured. Then, the setup is extended by *MARMAC* and the additional latency induced by either adapters or gatekeepers is determined. Here, we differentiate between pure datagram forwarding (*passthrough*) and actual authenticated counterparts. Moreover, processing delays, including cryptographic operations, are measured separately. Besides the passthrough, we compare our solution against the more complex asymmetric *SIGMAR* [8] and, furthermore, consider SipHash and HMAC-SHA-256 as candidates for *MARMAC*'s cryptography.

The results regarding the latency induced by *MARMAC* to the original IEC 61162-450 communication are shown in Figure 4. It is successively measured for 100 NMEA datagrams in the *Deneb* trace for different variants. The original delay for the datagram transmission from sensor to IBS (≈ 0.98 ms) presents the baseline. The figure shows the inherent additional network delay (blue) caused by the *MARMAC* entities and the processing delay (red), which results from latencies of datagram processing and cryptographic operations.

As expected, *MARMAC*'s symmetric cryptography, i.e., SipHash and HMAC (SHA-256), significantly outperforms *SIGMAR* in both entities, adapters (Fig. 4(a)) and gatekeepers (Fig. 4(b)). Thus, our approach greatly reduces the overall latency, which is particularly essential for the latter. The preferred SipHash (cf. Sec. V-B3) furthermore turned out to be more efficient in terms of latency then HMAC with comparable level of security. Obviously, the more performant Pi 4 is better suited for higher workloads, i.e., as gatekeepers, whereas the results of the Pi zero W are considered to be already sufficient for *MARMAC* adapters in practice.

[1] https://www.bsh.de/EN/The_BSH/Our_ships/Our_ships_node.html

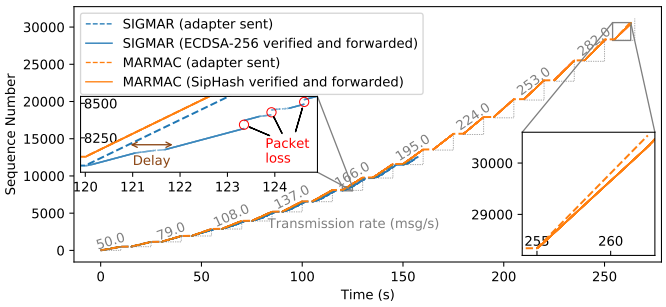


Fig. 5. *MARMAC*'s vs. *SIGMAR*'s gatekeeper performance (Pi zero W).

The communication overhead can be derived analytically from the additional data *MARMAC* introduces to each IEC/NMEA message. This overhead basically depends on the additional NMEA TAG, which in turn results from the size of the individual MACs. SipHash adds 237 and HMAC 424 additional bytes. Considering the *Deneb* trace with an average message size of 81 bytes, this results in an overhead factor of 3.93 and 6.23, respectively, whereas *SIGMAR* has a factor of only 2.39 [8], which is, however, compensated by the considerably better latency of *MARMAC*. SipHash is not only competitive to HMAC in terms of latency, but also requires significantly less overhead, thus, is the recommended variant.

C. Gatekeepers' Bottleneck Performance

The captured network traffic from *Deneb* was again utilized to evaluate *MARMAC*'s gatekeeper performance against the related *SIGMAR* [8] on the Pi zero W. While even the average traffic (43.2 msg/s) is already close to *SIGMAR*'s capacity, messages got delay up to 0.5 s during peaks ($\approx$ 80.0 msg/s). These bursts are short enough to recover during less intense periods ($\approx$ 39.6 msg/s). In contrast, *MARMAC* is found to be significantly more efficient and can handle roughly 4 times as much msg/s. Thus, with increasing traffic, which is expected in the future, *MARMAC* gains in importance.

In a second setup, we create synthetic traffic based on the *Deneb* trace and stepwise increase the transmission rate in order to evaluate the bottleneck performance of the gatekeeper. Again, *MARMAC* is compared against *SIGMAR*. The results are visualized as time-sequence plot in Figure 5 and confirm the significant performance increase of our approach. While a gatekeeper that relies on *SIGMAR* only achieves a maximal throughput of roughly 59 msg/s due to its latency (cf. Fig. 4(b)) and cause considerable delay and packet loss otherwise (at 125 s), *MARMAC* successfully copes with transmission rate of up to 250 msg/s. Overall, *MARMAC* represents an efficient solution with sufficient throughput suitable for low-cost hardware, thus enabling retrofitting into maritime systems.

VII. Conclusion

In this paper, we proposed *MARMAC*, a resource-efficient framework for a secure and safe communication of nautical data in integrated bridge systems of modern vessels. For that purpose, *MARMAC* retrofits authentication to the wide-spread IEC 61162-450 standard. It leverages the multicast-capable Multi-MAC and adopts it to maritime systems. We furthermore introduce a specific gatekeeper enabling network segmentation and enforcing communication integrity. Our framework is evaluated using low-cost hardware with trace-based simulation showing promising performance even on devices with low computational power. In our future work, we will investigate the potential of efficient MAC schemes [21] for maritime systems. We also plan to deploy and further improve *MARMAC* in practice, taking into account real-world maritime electronics.

Acknowledgments

The work in this paper was partially funded by the German Federal Ministry for Digital and Transport (BMDV) as part of the project SINAV with its partners BM Bergmann Marine and Fraunhofer CML. The authors thank the German Federal Maritime and Hydrographic Agency (BSH) for providing access to the research vessel Deneb and Michael Bergmann for discussions.

References

[1] A. Drougkas, A. Sarri, and P. Kyranoudi, "Guidelines - Cyber Risk Management for Ports," 2020, ENISA.
[2] K. Tam and K. Jones, "Factors Affecting Cyber Risk in Maritime," in *Proc. of Cyber SA*, Oxford, United Kingdom, 2019, pp. 1–8.
[3] 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.
[4] P. Meland, K. Bernsmed, E. Wille, O. Rodseth, and D. Nesheim, "A Retrospective Analysis of Maritime Cyber Security Incidents," *TransNav*, vol. 15, no. 3, pp. 519–530, 2021.
[5] 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.
[6] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation Data Anomaly Analysis and Detection," *Information*, vol. 13, no. 3, 2022.
[7] D. Heering, O. M. Maennel, and O. M. Venables, "Shortcomings in cybersecurity education for seafarers," in *Proc. of MARTECH*, Lisboa, Portugal, 2020, pp. 1–13.
[8] C. Hemminghaus, J. Bauer, and K. Wolsing, "SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures," in *Proc. of ISNCC*, Dubai, UAE, 2021.
[9] SOLAS Chapter V – 1/7/02, "Safety of Navigation," 2002, International Maritime Organization (IMO).
[10] IEC 61162-450:2018, "Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection," 2018.
[11] 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.
[12] M. Balduzzi, A. Pasta, and K. Wilhoit, "A Security Evaluation of AIS Automated Identification System," in *Proc. of ACSAC*, New Orleans, LA, USA, 2014, pp. 436–445.
[13] 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 S&P*, San Francisco, CA, USA, 2020, pp. 1384–1400.
[14] Y. Challal, H. Bettahar, and A. Bouabdallah, "A taxonomy of multicast data origin authentication: Issues and solutions," *IEEE Communications Surveys & Tutorials*, vol. 6, no. 3, pp. 34–57, 2004.
[15] X. Wang and H. Yu, "How to Break MD5 and Other Hash Functions," in *Proc. of EUROCRYPT*, Aarhus, Denmark, 2005, pp. 19–35.
[16] A. Perrig and J. Tygar, *Secure Broadcast Communication*. Springer, 2003, ch. TESLA Broadcast Authentication, pp. 29–53.
[17] T. Wu *et al.*, "A Fast and Efficient Source Authentication Solution for Broadcasting in Wireless Sensor Networks," in *Proc. of NTMS*, Paris, France, 2007, pp. 53–63.
[18] X. Yao, X. Han, X. Du, and X. Zhou, "A Lightweight Multicast Authentication Mechanism for Small Scale IoT Applications," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3693–3701, 2013.
[19] J.-P. Aumasson and D. Bernstein, "SipHash: A Fast Short-Input PRF," in *Proc. of INDOCRYPT*, Kolkata, India, 2012, pp. 489–508.
[20] NIST, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions," 2015, FIPS PUBS 202, DOI 10.6028/NIST.FIPS.202.
[21] E. Wagner, J. Bauer, and M. Henze, "Take a Bite of the Reality Sandwich: Revisiting the Security of Progressive Message Authentication Codes," in *Proc. of WiSec*, 2022, pp. 207–221.