Vessels Cybersecurity: Issues, Challenges, and the Road Ahead

Maurantonio Caprolu, Roberto Di Pietro, Simone Raponi, Savio Sciancalepore, Pietro Tedeschi
Division of Information and Computing Technology
College of Science and Engineering, Hamad Bin Khalifa University - Doha, Qatar
{ssciancalepore, rdipietro}@hbku.edu.qa, {mcaprolu, ptedeschi, sraponi}@mail.hbku.edu.qa

***Abstract*— Vessels cybersecurity is recently gaining momentum, as a result of a few recent attacks to vessels at sea. These recent attacks have shacked the maritime domain, which was thought to be relatively immune to cyber threats. The cited belief is now over, as proved by recent mandates issued by the International Maritime Organization (IMO). According to these regulations, all vessels should be the subject of a cybersecurity risk analysis, and technical controls should be adopted to mitigate the resulting risks. This initiative is laudable since, despite the recent incidents, the vulnerabilities and threats affecting modern vessels are still unclear to operating entities, leaving the potential for dreadful consequences of further attacks just a matter of "when", not "if".**

In this contribution, we investigate and systematize the major security weaknesses affecting systems and communication technologies adopted in modern vessels. Specifically, we describe the architecture and main features of the different systems, pointing out their main security issues, and specifying how they were exploited by attackers to cause service disruption and relevant financial losses. We also identify a few countermeasures to the introduced attacks. Finally, we highlight a few research challenges to be addressed by industry and academia to strengthen vessels security.

I. Introduction

Vessels are likely the oldest long-range transportation means used by humans to reach physically far locations, and it is still the preferred one in many cases, including the movement of goods—over 90% of the world's trade is carried by sea—and luxury entertainment, such as cruise experiences. Thus, large vessels carrying thousands of tonnes of goods (e.g. oil tankers, containers carriers) or a few thousand people definitively can be considered as *critical systems*, requiring reliable and secure computing and communication systems.

However, vessels cybersecurity issues historically have received only minimal attention from both the shipowners and the scientific community. The reasons are manifold, and can be found in the late *digitization* of the maritime sector, the heterogeneity of operators, the focus on availability rather than security, and, finally, the widespread belief that cyber-attacks to vessels offshore are technically difficult and hard to succeed.

Given the above scenario, the International Maritime Organization (IMO) first generally highlighted the major cyber-threats in the maritime sector (*MSC-FAL.1 /Circ.3*, 2017). Then, in the 98th session (June 2017), it took action, adopting the "Resolution MSC.428/98", namely, "Maritime Cyber Risk Management in Safety Management Systems". This document forces shipowners to address cyber risks and cyber-security attacks in the design and the deployment of existing safety management systems [1]—these objectives to be attained by January 2021. Since this latter date, any vessel not conforming to this regulation would not be authorized to sail—implying relevant economic loss, as well as a threat to global trade.

Despite this mandate, the IMO did not clearly define the attack surface of a modern vessel. Indeed, while shipowners are currently oriented towards the strengthening of the management systems, other areas are overlooked. For instance, severe weaknesses implicit to the communication protocols used by the ships are unknown to operating entities, hence potentially nullifying the efforts to implement secure-by-design vessels.

To the best of our knowledge, this is the first contribution investigating, in a comprehensive and structured manner, the cybersecurity issues associated with modern vessel systems. Specifically, we analyze the communication technologies and computer systems used within large vessels, pointing out several security issues rooted in their design and operational mode. We also relate these vulnerabilities with recent incidents and attacks involving vessels, and we identify the weak points that any modern vessel needs to mitigate towards the enforcement of the latest IMO resolutions. Finally, we indicate mitigating countermeasures to the highlighted threats, as well as future research directions to be addressed by industry and academia to strengthen vessels cybersecurity.

The rest of this paper is organized as follows: Section II discusses the security vulnerabilities of communication technologies on vessels, Section III illustrates the vulnerabilities associated with the computer systems on-board, while Section IV focuses on the technologies used to improve people' safety. Section V highlights challenges, countermeasures, and future directions towards the realization of cyber-secure vessels. Finally, Section VI tightens conclusions.

II. Vessel Communication Systems Security

Traditional inland communication systems have not been designed to guarantee network coverage offshore. Thus, only a limited set of technologies are available for vessel communications. Figure 1 provides a graphical overview. While GNSS technologies enable location estimation (Section II-A), critical bidirectional communication services include the Automatic Identification System (AIS) protocol

This article has been accepted by IEEE Communications Magazine. Publication expected in June 2020.

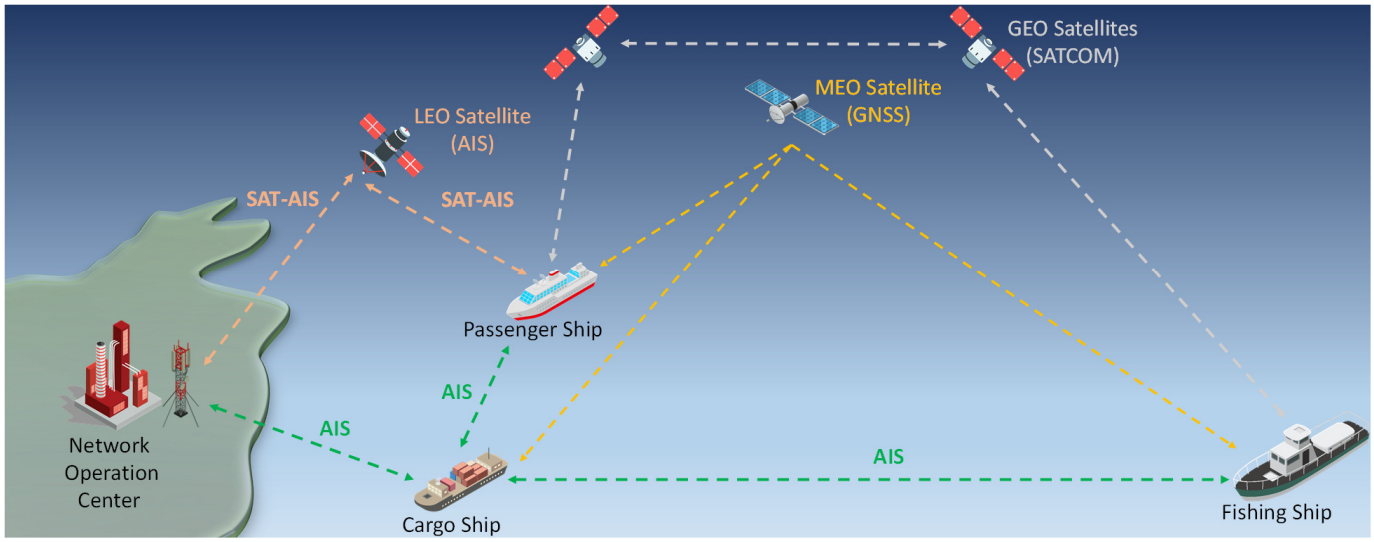

Figure 1. Overview of technologies used by modern vessels.

(Section II-B) and Satellite Communications (SATCOM)—this one supporting higher data rates (Section II-C).

A. Global Navigation Satellites Systems (GNSS)

A key element of modern vessel systems is the real-time location awareness provided by Global Navigation Satellites Systems (GNSS) technologies. Any modern vessel is equipped with a GNSS module, that can receive RF signals originated from Medium Earth Orbit (MEO) satellites, located $[19,000 - 23,000]$ km above Earth. GNSS data, guaranteeing earth coverage, are broadcasted unidirectionally at a frequency of 2 Hz. Each satellite is synchronized to the exact system time, thanks to atomic clocks, and transmits a navigation signal containing the message delivery time and additional information, including the deviation of the satellite from its expected trajectory.

A receiver equipped with omnidirectional antennas detects a combination of signals from different satellites and can identify the single contributions. For each of them, based on the exact Time of Arrival (ToA) (synchronized with the clock reference of the transmitters), knowing the propagation speed of the signal (the speed of light), it is possible to obtain the distance from the satellites. A minimum of four satellites are required to efficiently multi-laterate distances and obtain a location. Given that perfect time synchronization is not possible, a localization error is generally present, usually not exceeding 5 meters in outdoor conditions with clear sky visibility [2]. Note that, when employed for military use (access is restricted to authorized parties), the GNSS can reduce the error to less than 1 meter. Several GNSS technologies are available, based on the community responsible for operating and maintaining the satellites. Despite the most famous is the Global Positioning System (GPS) operated by the USA, there are equivalent systems, e.g., the Russian Global Navigation Satellite System (GLONASS), the European GALILEO, and the Chinese BEIDOU.

From the security perspective, commercial vessels rely on civilian GNSS signals. Unfortunately, to boost message availability at the receivers, the civilian GNSS was designed to transmit messages in clear-text, without relying on any confidentiality nor authentication mechanism. Moreover, since GNSS signals are used as the timing source of many synchronization technologies, the trajectories of the satellites are publicly available. Therefore, they can be easily spoofed using commercially available Software Defined Radios (SDRs). These relatively cheap devices can be tuned on the operating frequency of the GNSS technology, and configured via freely-available, open-source tools to transmit messages that are indistinguishable from authentic GNSS signals. As shown in Figure 2, since the legitimate signals are very weak at the ground level, the forged messages can be easily super-imposed to the legitimate ones, leading the receivers to estimate fake locations [3].

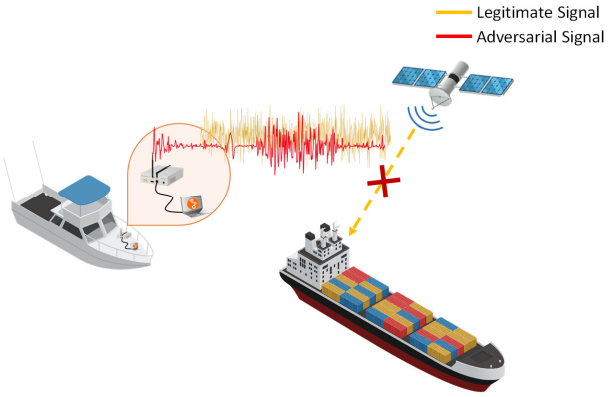

Figure 2. Logic of jamming and spoofing attacks against vessels.

Despite these weaknesses are well-known, the vulnerability of vessels to GNSS spoofing attacks received worldwide attention only recently, due to anomalies detected in the Black Sea area [4]. In June 2017, at least 20 ships located

in the Black Sea region reported anomalies to their GNSS systems, with their receivers signaling either unstable locations or positions on the ground, close to a nearby airport area. Thus, vessels were forced to switch to manual navigation systems and to resort to outdated systems to maintain their routes and avoid collisions. GNSS is extremely sensitive also to jamming attacks. Vessels can be easily approached by moving entities carrying a device emitting noise on the GNSS communication frequency. The power of the noise adds up to the power of the legitimate signal, thus compromising the operation of any GNSS technology.

B. Automatic Identification System (AIS)

AIS, proposed by the International Association of Lighthouse Authorities (IALA) and part of the Vessel Traffic Service (VTS), is a coastal tracking system mandatory on ships of over 300 tonnes, but widely adopted also over ships of smaller weight. It aims to broadcast the position, speed, movements, and route of the vessels, to help them avoiding collisions [5]. AIS operates in the Very High Frequency (VHF) band, using the Gaussian filtered Minimum Shift Keying (GMSK) scheme, and it guarantees a horizontal transmission range of up to 74 Km, with a bitrate of 9600 bit/s. AIS uses two channels: the 161.975 MHz, for ship-to-ship communication, and the 162.025 MHz, for ship-to-shore communications. AIS transceivers consist of: (i) a VHF transmitter; (ii) two VHF Time Division Multiple Access (TDMA) receivers; (iii) a VHF Digital Selective Calling (DSC) receiver; (iv) a positioning module supporting GNSS capabilities; and (v) sensors connected via standard marine electronic communications links. The data are periodically broadcast, allowing all the compatible vessels to enforce situation awareness and avoid collisions.

To overcome coverage issues, AIS has been extended further to a space-based version, namely Space-Based AIS. Leveraging AIS receivers located on Low Earth Orbit (LEO) satellites, the messages can be relayed to the ground, extending the range up to 400 Km.

While the intended purpose of AIS was to avoid vessel collisions, today AIS is used for several cyber-physical applications, including identification, search and rescue operations, accident investigation, remote tracking, ocean currents estimation, and the protection of marine Critical Infrastructures (CIs).

However, being designed in the 80s, AIS does not support any security property, such as authentication and confidentiality. As discussed in [6], the protocol is vulnerable to different attacks, including spoofing, hijacking, data manipulation, and Denial of Service (DoS). An attacker could: (i) create fake vessels; (ii) inject false ship details (e.g., position, speed, and Mobile Maritime Service Identity (MMSI)); (iii) impersonate vessels or port authorities; (iv) inject false information (e.g., false man-in-water alarms); and, finally, (v) send false collision warning alerts.

C. Satellite Communications

SATCOM services are the roots of many services used on vessels to guarantee safety and security. A generic SATCOM system consists of four elements: (i) several space-based satellites; (ii) many ground-based gateway earth stations; (iii) a Very Small Aperture Terminal (VSAT) antenna installed outdoor; and, (iv) a Network Operation Center (NOC).

The satellites are the key elements of the networking infrastructure. They are typically located in a Geostationary Earth Orbit (GEO) (height $35,786$ Km) above the equator, and they are equipped with multiple communication technologies to communicate with earth-based equipment and other satellites. Typically, a GEO satellite exchanges data using the Ka-band, in the frequency range $[26.5 - 40]$ GHz, using narrow-band modulation schemes. This allows re-using the frequency band, compared to traditional wideband technologies. Alternatively, the *bent-pipe* architecture is used, where the satellites act as relays in *Amplify-and-Forward* mode, relaying the signal between two gateways located on the ground. The satellites can also use dedicated optic technologies to transfer data to each other, as for LEO satellites operated by GlobalStar and Iridium providers.

In maritime applications, the gateway earth stations and the VSAT antenna reside together on the vessel, and enable direct communication with GEO satellites at high speed, up to 506 Mb/s when using the most recent Ku-band (frequency range: $[12 - 18]$ GHz). To guarantee Line-Of-Sight (LOS) connection to the satellites, the VSAT antenna is installed outdoor, in a clear view of the sky with a given angular view, expressed in terms of azimuth, polarization, and skew. This setup is typically realized by the operator at the deployment time. Motors and sensors on-board are used to orientate the antenna towards the satellite. Finally, the NOC is maintained by the satellite operator and provides coordination and maintenance tasks to the satellite network. Thus, each ship is typically a node in a network including also vessels of the same shipowner and same satellite operator. Many maritime satellite providers are available, including Iridium, GlobalSat, and INMARSAT. INMARSAT, operating 13 satellites, is the most adopted operator, as it is the only approved provider for the Global Maritime Distress and Safety System (GMDSS) technology.

The GMDSS specification, established in 1980 by the IMO, evolved to include several systems, protocols, equipment, and procedures useful to ease the rescue of vessels in distress. It includes: (i) transmission of ship-to-shore distress communications via multiple communication technologies on multiple frequencies; (ii) reception of shore-to-ship alerts; (iii) transmission of maritime safety information; (iv) transmission of vessel location; and, (v) exchange of generic navigation information.

Overall, the degree of security offered by SATCOM strongly depends on the specific protocols and operations deployed by the operator. Since operators are private companies, the details of the security protocols and procedures are always protected by intellectual property rights, thus being hard to evaluate. To name a few cases of vendor-specific security issues, a recent study [7] discovered unencrypted connections between the VSAT antenna and the gateway in DVB-S SATCOM networks. Thus, when insecure services are used (i.e., POP3 e-mails or HTTP browsing), privacy issues arise.

In the specific context of vessels, recent reports published

by the security firm IOAlliance discovered that the GMDSS operations enforced by INMARSAT are affected by severe weaknesses [8]. The root cause of the vulnerabilities has been found in the *thraneLink* protocol, a proprietary solution within the SAILOR 6000 communication suite. Specifically, the consulting firm found a backdoor enabling the installation of an unauthenticated firmware update and malicious software. Moreover, additional protocol-level vulnerabilities were discovered in the Mini-C INMARSAT Terminal. Using specially crafted messages, an attacker aware of these vulnerabilities could disable the Ship Security Alarm System (SSAS), used by vessels to signal piracy and terrorism attempts offshore. Besides, additional physical attacks are possible, by simply modifying the orientation of the VSAT antenna, thus denying a reliable SATCOM link.

III. Vessels Computer Systems Security

Computer systems integrated into modern vessels include specific hardware and software solutions to automate dedicated functions, including navigation, propulsion, and fuel supply. On the one hand, they provide the crew with a real-time and reliable view of the state of the vessel, improving reaction time and decreasing personnel costs. On the other hand, these technologies increase the vessel attack surface, leading to additional security concerns.

The automated systems operating on-board, summarized in Figure 3, include a variety of elements [9]. The core is the *bridge*, providing a unified view of all the systems operating on-board. The bridge acts as the central point of a logical star network, where information coming from peripheral systems are integrated to provide a comprehensive view of the vessel. Another important system is the Electronic Chart Display and Information Systems (ECDIS), a computer-based navigation information system used by officers to establish and maintain the route, as an alternative to legacy paper nautical charts. The ECDIS provides crucial services, including navigational safety, automatic route planning, route monitoring, navigation time, and route update management.

Additional peripheral management systems connected to the bridge include: (i) the *Cargo Management System*, in charge of managing goods loading and unloading operations; (ii) the *access control systems*, including cameras and microphones for surveillance purposes, alarm systems, and electronic devices for the on-board personnel security; (iii) *on-board machinery management*, automating the monitoring of mechanical systems, including propulsion and steering systems; and, finally, (iv) the *communication systems*, including SATCOM, AIS, and GNSS modules.

Moreover, the ECDIS provides continuous data recording features, thanks to the interaction with the Event Data Recorder (EDR). The EDR is an event logger allowing forensic investigations when serious malfunctions and incidents occur. According to Safety of Life at Sea (SOLAS) regulations, the EDR should provide minute-by-minute recording for the past twelve hours of the voyage and the record of four hourly intervals of voyage track for a period of six months. These systems could be connected to shore-side networks for data downloading and software updates.

Other computer systems are available, even if they are mostly physically disconnected from the bridge. To name a few, they include the *crew welfare systems*, integrating several third-party computing systems used for ship administration and crew welfare, and the *passenger services management*, including the devices in possession by the crew and the passengers and used for boarding, access control, billing services, luggage tracker, and entertainment.

From the security perspective, being vessels Cyber-Physical Systems, the physical and the digital components of the system are interrelated. Thus, attacks on the digital infrastructure impact on the physical context of the vessel, and, at the same time, physical attacks can disrupt the digitized systems maneuvering and coordinating vessel operations. In particular, the *bridge* is the most critical component. Gaining full access to this system would enable the attacker to definitively control the vessel, performing maneuvers, and altering the input from peripheral systems. Severe service disruption could occur also if the attacker takes full control of crucial peripheral systems, including the EDR, cargo management systems, and the on-board machinery management systems. For instance, a ransomware controlling the vessel could block any door or movement toward the land, holding passengers as hostages at sea until a ransom is paid. On the physical perspective, an attacker could tamper the sensors of the automatic docking system, leading the automatic navigation systems to run the ship into natural formations (e.g., underwater rocks), or human infrastructures like bridges, ports, and other ships, using the very same mass and speed of the vessel as a weapon [10].

News about attacks on vessel computer systems are widely available. For instance, the "Guidelines on Cyber Security onboard Ships" reported that a vessel designed for paperless navigation was delayed from sailing for days after a malware blocked its ECDIS system [9]. The crew members did not realize the failure as a cyberattack, but simply as a technical issue, and its resolution took significant time and efforts, leading to relevant financial losses. Several shipowners also reported that their ICT network was infected by ransomware, causing service breakdowns [11]. Despite the involved companies revealed the least possible details (a disappointingly diffused habit, theoretically reducing bad publicity, but practically preventing to assess the scale and impact of the phenomenon), unofficial news reported unwitting ship agents as the source of the malware, causing issues in several ports.

IV. Safety On-board

Vessels are technically sophisticated systems, characterized by a considerable size. Thus, they need several crew members on-board, holding critical roles to safeguard the passengers, the vessel, and the goods.

Several use-cases are possible for the above scenario. For instance, during the ship's docking maneuver, failing of the automatic systems could occur. In these cases, specialized crew members are typically in charge of solving the problem. However, if these people have any issue, the vessel does not have any technology enabling a timely communication of the event or the automatic handling of the emergency.

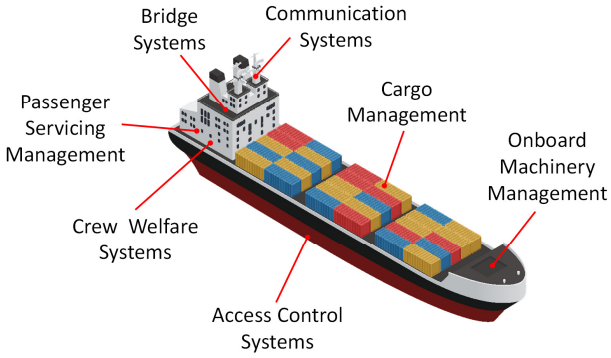

Figure 3. Main systems integrated into modern vessels.

Similarly, the unexpected absence of any crew member during critical real-time vessel operations could not be automatically detected. At this time, the control room where the bridge is located is mostly unable to realize personnel absence and undertake a critical maneuver without being supported by specialists.

To the best of our knowledge, the safety on-board is currently addressed by relying on both introductory training courses and legacy communication protocols. During the training courses, the crew members acquire general information, such as reaction behaviors in case of fire, safety equipment usage, and alarm signals meaning. However, no information about the operation of communication systems is provided.

As per the communication protocols, the National Marine Electronics Association (NMEA)-2000 is the wired communication standard adopted by vessels. It is a plug-and-play technology (IEC 61162-1), allowing the connection of marine sensors within vessels and their management through the bridge. The standard is compatible with the Controlled Area Network (CAN-BUS), currently employed in many vessels to manage several peripheral systems, including the steering and the alarm systems.

The implementation of a standard communication protocol on-board allows automating many of the tasks that, until a few decades ago, were purely manual. However, the CAN-BUS was designed in the 80s; thus, the technology proves not to be up to today's cyber-security challenges. Among the many limitations, the protocol provides neither authentication nor confidentiality of messages. Thus, as shown in Figure 4, any compatible receiver attached to the system could read the unencrypted content of the messages and inject fake messages—e.g., shutting down the systems, causing DoS attacks [12].

V. Challenges and Road Ahead

Table I summarizes the security properties enjoyed (or missing) by the communication technologies used on vessels. Despite the vulnerabilities highlighted in the above table have been addressed in other contexts, their integration in modern vessels leads to several challenges (summarized in Table II), due to the constraints peculiar to the vessel context. Detailed motivations, challenges, and future directions stemming from discussions with major players in the vessels production domain are provided below.

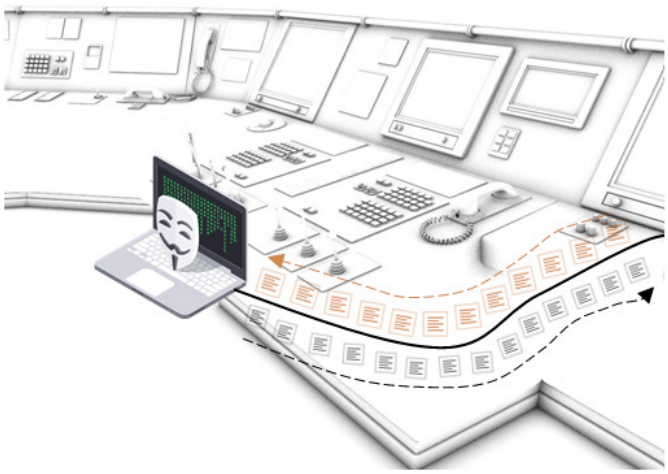

Figure 4. CAN-BUS attacks. Compatible receivers connected to the system can read and inject fake messages.

Table I
Security properties of vessels communication technologies.

Technology	Confidentiality	Authentication	Availability
GNSS	✗	✗	✗
AIS	✗	✗	✗
SATCOM	✗	✓	✓
CAN-BUS	✗	✗	✓

Table II
Overview of security issues and possible countermeasures.

Security Issue	Countermeasure
GNSS Spoofing	Cross-Technology Location Estimation (GNSS, SATCOM)
Electronic Warfare	Anti-jamming Protocols
Non-Standardized SATCOM Protocols	Standardization Efforts
AIS Spoofing	Software Security Frameworks
Bridge System Assessment	Standardized Security Assessment Procedures
Malware Attacks	Containerization
Automatic Safety Systems	Wireless Sensing and ML
Wired Communication Protocols Security	Physical Security Strategies, Access Control

GNSS Spoofing Detection. The lack of message authentication in civilian GNSS technologies exposes vessels to GNSS spoofing attacks, leading them to estimate inconsistent locations. Several strategies are available to detect GNSS spoofing attacks. These techniques rely either on multiple antenna schemes or on the analysis of the *raw* GNSS signals, or on the cross-validation of GNSS-derived locations with information from additional communication technologies (i.e., cellular networks) [2]. However, these schemes are hardly applicable to vessels. On the one hand, they require hardware modifications on systems already deployed, leading to consistent hardware installation and maintenance costs. On the other hand, vessels located off-shore could hardly leverage positioning technologies other than the GNSS. Therefore, future GNSS Spoofing detection schemes on vessels should target non-invasive solutions, requiring little (if any) hardware change to the already operational expensive ships.

Electronic Warfare Mitigation. Electronic Warfare scenarios involve several powerful attacks, where adversaries use sophisticated tools to disrupt the operation of the communication infrastructure of a given entity. In the maritime domain, jamming vessels could have disastrous consequences. Indeed, without access to the GNSS infrastructure and to the SATCOM network, a vessel could easily lose situational awareness and the capability to communicate with landline systems, not relying on any further help than its personnel and past generations equipment (e.g., physical maps). Despite the availability of several anti-jamming schemes, vessels require the adoption of non-invasive protocols, that should be thoroughly assessed and contextualized in order not to require expensive and time-consuming hardware change operations, while providing seamless integration with current technologies and ease of use.

SATCOM Security Standardization. The recent attacks over SATCOM networks have revived the interest of industries and academia towards the security of the satellite communication links. To date, the high costs derived from the manufacturing, deployment, and maintenance of satellites have motivated the development of proprietary solutions. Thus, the involved protocols are (despicably) mostly closed-source and undocumented, and their security cannot be evaluated from the scientific community—it may be worth remembering that security through obscurity, while providing a transient competitive advantage, in the long-run has been shown to lead to critical breaches. Indeed, these limitations indicate the need for standardization activities towards the definition of secure datalinks for vessels SATCOM security. While programs specific for other CIs are starting to arise (see [13] for civil aviation), to the best of our knowledge, no initiatives are scheduled for the maritime domain.

AIS Spoofing Detection. The AIS protocol provides neither message authentication nor encryption, thus being exposed to replay and spoofing attacks. Similar issues existing for other wireless communication technologies have been addressed thanks to application-layer frameworks, able to provide authenticity, integrity, and confidentiality to the messages. These cited strategies can be integrated into the applications using AIS, leveraging the lessons learned by other similar communication technologies (see IEEE 802.15.4 in the IoT context). However, conjoint initiatives by shipowners and operators in the vessel domain are needed to agree on application-layer design guidelines and technical details, such as the setup of a dedicated Public Key Infrastructure.

Bridge Systems Assessment. Considering the critical role played by the bridge and the catastrophic consequences that could arise in case of attacks, protecting the bridge software against cyber-attacks must be a priority for shipowners. Research efforts are needed in this field to standardize the security assessment procedures, inheriting experience from other CI domains (e.g., smart grids, aircraft), and contextualizing the maritime requirements in security frameworks characterized by a high level of automation.

Mitigating Malware Attacks. Similarly to other digitized CIs, malware infections to vessel management and computing systems could have a high pay-off for an attacker. Protecting the security perimeter of a CI has been extensively studied in the literature [14], and similar solutions could be integrated into vessel systems as well. Given that the effective physical separation and logical isolation among all the on-board systems are imperative to contain the spread of potential threats and the extent of damages in case of malware attacks, global regulations and technical guidelines specifically tailored to vessel systems are needed, to standardize interfaces and interconnections among integrated systems.

Automatic Safety Systems. Although technological innovations proceed at a high pace, their integration into modern vessels is still in its infancy. Unlike other moving assets (e.g., aircraft), vessels still largely rely on human intervention to manage emergencies. This leads to the necessity of introducing automatic emergency systems, allowing responsive monitoring of goods and humans onboard. Wireless sensor-based systems relying on wearable embedded devices could provide a valuable solution to the above issues. Thanks to short-range wireless communication technologies, smart sensors can monitor the physical conditions of the crew, enabling real-time personnel localization and tracking. Moreover, optimized deployment strategies can improve situational awareness during critical maneuvers. For instance, a central computing system relying on artificial intelligence could collect and analyze the measurement, react to emergencies, and provide significant advantages in terms of prevention, detection, and management.

Wired Communication Protocols Security. The rapid obsolescence of the current technologies makes protocols introduced decades ago no longer fit to mitigate modern cyber threats. Specifically, being proprietary protocols closed-source and protected by intellectual property rights (e.g., the CAN-BUS), their security evaluations is difficult, to say the least.

Hence, there could be hidden security threats getting along for decades, as it has been recently shown [15]. This scenario could lead to perilous use-cases where, besides cargo and physical resources, even the safety of the crew members and passengers is at stake. Thus, securing the interactions between the centralized computing equipment and the mechanical peripheral devices, as well as employing standardized and secure (ideally wired) communication protocols, become crucial security requirements, where their deployment could rely on the results already available in the scientific literature.

VI. Conclusion

The mandatory adoption of cyber-security risk analysis and related technical controls on all vessels by January 2021 forces shipowners to start reflecting on a few key security elements, including the threat model affecting the maritime domain, the attack surface, and possible countermeasures. In this paper, to the best of our knowledge, we highlight for the first time the main weaknesses affecting the communication technologies and systems used in modern vessels, shading lights on their relationship with mainstream attacks carried out over the last few years. We also summarize the most important research challenges, directions, and countermeasures, to be addressed by maritime operators towards the development of secure vessel systems.

Despite the widely known security issues of wireless and wired technologies are even amplified in the vessel domain, we believe that vessels integrate a suitable variety of technologies and the computational power to overcome such limitations, meeting standard, and evolving towards more secure operational conditions. Though, this can only be achieved via a stricter collaboration among maritime sector, industry, and academia.

Acknowledgments

The authors would like to thank the anonymous reviewers for their comments and suggestions, that helped improving the quality of the manuscript. This publication was partially supported by awards NPRP 11S-0109-180242, UREP 23-065-1-014, and NPRP X-063-1-014 from the QNRF-Qatar National Research Fund, a member of The Qatar Foundation. The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the QNRF.

References

[1] International Maritime Organization, "Maritime Cyber Risk Management In Safety Management Systems," https://tinyurl.com/yc3xszxa, Jun. 2017, (Accessed: 2019-10-20).

[2] G. Oligeri, et al., "Drive Me Not: GPS Spoofing Detection via Cellular Network: (Architectures, Models, and Experiments)," in *ACM Conf. on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 12–22.

[3] G. Baldini et al., "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 355–379, 2011.

[4] The Maritime Executive, "Mass GPS Spoofing Attack in Black Sea?" https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea, July 2017, (Accessed: 2019-10-20).

[5] E. Tu et al., "Exploiting AIS Data for Intelligent Maritime Navigation: A Comprehensive Survey From Data to Methodology," *IEEE Trans. on Intelligent Transportation Sys.*, vol. 19, no. 5, pp. 1559–1582, May 2018.

[6] M. Balduzzi et al., "A Security Evaluation of AIS Automated Identification System," in *Proc. Annual Computer Security Applications Conference*, 2014, pp. 436–445.

[7] J. Pavur et al., "Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband," in *ACM Conf. on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 277–284.

[8] R. Santamaria, "A Wake-up Call for SATCOM Security," IOActive, Technical Report, 2014, (Accessed: 2019-10-20). [Online]. Available: https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

[9] BIMCO, "The Guidelines on Cyber Security Onboard Ships," BIMCO, Technical Report, 2016, (Accessed: 2019-10-20). [Online]. Available: https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=20

[10] K. Jones et al., "Threats and Impacts in Maritime Cyber Security," *Engineering & Technology Reference*, vol. 1, no. 1, Jan. 2016.

[11] L. Mathews, "Another Shipping Giant Falls Victim To Ransomware," https://www.forbes.com/sites/leemathews/2018/07/26/another-shipping-giant-falls-victim-to-ransomware/, July 2018, (Accessed: 2019-10-20).

[12] P. Carsten et al., "In- Vehicle networks: Attacks, vulnerabilities, and proposed solutions," in *Proc. Annual Cyber and Information Security Research Conference*, 2015.

[13] K. Bernsmed et al., "Security requirements for SATCOM datalink systems for future air traffic management," in *IEEE/AIAA Digital Avionics Systems Conference*, Sep. 2017, pp. 1–10.

[14] D. Puthal, et al., "Building Security Perimeters to Protect Network Systems Against Cyber Threats [Future Directions]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 4, pp. 24–27, Oct 2017.

[15] M. Lipp, et al., "Meltdown: Reading Kernel Memory from User Space," in *27th USENIX Security Symposium*, 2018.

Biographies

- Maurantonio Caprolu is PhD student at HBKU-CSE-ICT, Doha-Qatar. He received his Master's Degree with honors in Computer Science at Sapienza, University of Rome, Italy. His research interests include security issues in Blockchain-based systems, Edge/Fog architecture and Software-Defined-Networking.

- Dr. Roberto Di Pietro, ACM Distinguished Scientist, is full professor of cybersecurity at HBKU-CSE, Doha-Qatar. His research interests include Distributed Systems Security, Wireless Security, OSN Security, and Intrusion Detection, leading to 220+ scientific publications and patents. As for Google Scholar, he has been totaling 8400+ citations, with h-index=44, and i-index=120.

- Simone Raponi is PhD Student at HBKU-CSE-ICT, Doha-Qatar. He received both his Bachelor and Master Degree with honors in Computer Science at Sapienza University of Rome, Italy. His research interests include cybersecurity, Privacy, and Artificial Intelligence.

- Dr. Savio Sciancalepore is Post-Doc at HBKU-CSE-ICT, Doha-Qatar. He received his bachelor and master degrees from the Politecnico di Bari, Italy. His research interests cover security issues in Internet of Things and Cyber-Physical Systems.

- Pietro Tedeschi is PhD Student at HBKU-CSE-ICT, Doha-Qatar. He received his Master's degree with honors in Computer Engineering at Politecnico di Bari, Italy. He worked as Security Researcher at CNIT, Italy, for the EU H2020 SymbIoTe. His security research interests lie in Drone, Wireless, IoT, Applied Cryptography.