Security challenges in multi-modal communication

Karin Bernsmed*, Per Håkon Meland*, Egil Wille*, Ravi Borgaonkar*, and Guillaume Bour*
*SINTEF Digital, Software Engineering, Safety and Security, Trondheim, Norway

***Abstract*—Emerging maritime services rely more on digital message exchanges and less on voice communication. This requires proper implementation of mechanisms that provide robust and appropriate security for the technology that is used for ship-ship and ship-shore communication, both near shore and in open waters. This paper presents the concept of multi-modal communication, which encompass digital message exchange over different types of technologies and between sectors. We point to security challenges for existing technologies, and suggest how we can address these using an example from Search and Rescue operations that involves the maritime and additional sectors.**

***Index Terms*—cyber security, maritime, VDES, communication, cross-sectoral**

I. Introduction

The maritime sector is undergoing rapid digitization. By transitioning from analogue voice to digital message exchanges over the upcoming VHF Data Exchange System (VDES) [1], the stress on the existing communication links will be reduced and new services can be introduced. Examples include distribution of maritime safety information, electronic port reporting through the maritime single windows [2], remote control of thugs and autonomous vessels, and improved search and rescue operations. The underlying drivers for digitization are not only the reduction of administrative workload on the involved parties, most importantly the seafarers, but also to improve the quality of information used to plan and execute the operations. However, the introduction of digital communication technologies will also bring new challenges that need to be addressed, including cyber security. There are standards and technical solutions designed to protect the integrity and authenticity of message exchanges, but the same mechanisms, which are replacing much of today's open communication links, may become a barrier and reduce the availability of information if they are not compatible with each other.

The digitization of maritime services should ideally enable more efficient information exchange with other sectors. An example could be a maritime traffic tracking service providing freight ship position data to a port logistics platform, which uses it to coordinate ground-based transport. However, to the best of our knowledge, there are no ongoing efforts on addressing cross-sectoral security issues; instead, every sector is developing its own solutions.

In this paper, we present the concept of *multi-modal communication*, by which we mean digital communication that relies on different types of communication technologies and/or that includes the exchange of information between sectors. These can be used either in parallel at the same time, or through a link of serial connections.

As an example to demonstrate our modal concept, we use coordination of future Search and Rescue (SAR) operations. Under such circumstances, failure of the communication equipment can have severe consequences. According to Loukas et al. [3], there are concerns about the potential of cyber-attacks to cause physical disasters, or to maximize the impact of existing ones by intentionally disturbing and/or interfering with the coordination of such operations. Fig. I outlines a scenario where a man overboard (wearing a SAR transponder) is located by nearby vessels, assisted by a SAR aircraft and helicopter. The SAR operation is coordinated by a Maritime Resource Coordination Centre (MRCC), which exchanges search coordination data, search patterns and status information with the actors on the scene (vessels, helicopter, and aircraft), using the network connectivity provided by the VDES ground (VDES-TER) and VDES space (VDES-SAT) segments, and/or by cellular networks (4G/5G). The MRCC also collects position data using the Automatic Identification System (AIS) from vessels in the nearby area and methodology data about the current sea conditions from an Aid to Navigation (AtoN) beacon. The MRCC may also need to exchange information (in the form of data or voice) with stakeholders from other sectors, such as the coastguard, the police, the red-cross, the armed forces, medical communication centres and hospitals [4]. Thanks to the introduction of digital communication technologies, including VDES, the rescue process can be streamlined by means such as better coordination of the involved entities and visualization of the search patterns on an electronic map.

In this paper, we present existing solutions rooted in the maritime sector that are relevant for digital message exchanges in multi-modal cross-sectoral scenarios. Further, we identify and discuss security challenges that need to be addressed and suggest a strategy for the road ahead.

II. Existing solutions and their security

Since 1897 radio transceivers have been used for communication at sea [5], and even today legacy VHF radios are the dominant form of close-range ship-ship and ship-shore communication. Analogue radios are also used in shore-based application, e.g., police, construction site or emergency communication, but with different sets of frequencies/channels within the MF/HF/VHF/UHF bands. These systems tend to

Corresponding author: K. Bernsmed (email: https://www.sintef.no/en/all-employees/employee/3807/).

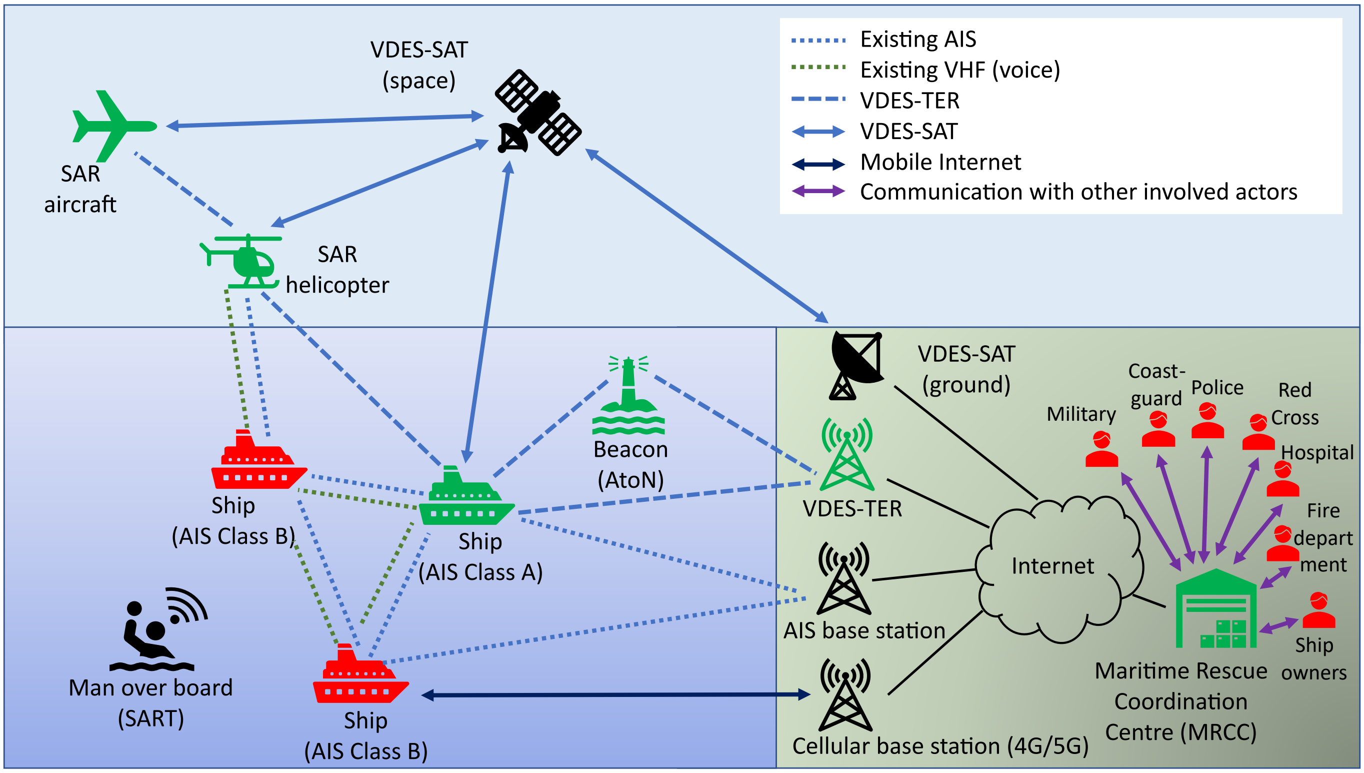

Fig. 1. Coordination of Search and Rescue operations.

be legacy systems that have not been designed with security in mind. The lack of integrity protection makes it easy to tamper with the analogue signals and the information is open to anyone listening in. If someone wants to make the signals unavailable, jamming is an inherent challenge with any wireless system [6]. Furthermore, there are seldom strong authentication mechanisms in place, making it difficult to determine who is on the other side of the line. Even with the relatively new Digital Selective Calling (DSC) features for distress calls, it is up to the user to program the correct nine-digit Maritime Mobile Service Identity (MMSI) number for the vessel into the radio equipment. In practice, any number can be programmed and the vessel can impersonate any other. Summarily, there is no guarantee that the sender of AIS signals is the ship it claims to be.

When ships are so close to shore that they can utilize terrestrial infrastructure, there are many communication options [7]–[9], including Mobile Data Services (MDS) (e.g., 3G/LTE/4G/5G), WiMAX/WiFi or more proprietary systems, e.g., Maritime Broadband Radio (MBR) [10]. Many of these systems are already cross-sectoral, but have limited maritime range and can be difficult to combine with each other as the security mechanisms are specific for each. Allal et al. [11] have benchmarked maritime communication technologies in term of security, and consider WiMAX to be the most secure compared to the others. However, they only include a limited range of technologies, whereas some are outdated today, and the analysis takes the context of autonomous and conventional ships in the Detroit of Gibraltar.

For long-range communication off-shore, different Satellite Communication (SATCOM) systems are frequently used for shipping, aviation, emergency and military applications. These typically include [12], [13]: Maritime VSAT, Inmarsat (BGAN, FleetBroadband, Fleet One, Global Xpress), Iridium (first generation, NEXT), Globalstar, BeiDou, SES (Broadband for Maritime (previously ASTRA2Connect Maritime Broadband), O3b mPower), Intelsat, OneWeb (under deployment), Telesat Lightspeed (planned), Kuiper (planned) and Starlink (under deployment). The different SATCOM systems vary greatly in terms such as bandwidth, coverage, latency and jitter, which is due to their age, distance to earth, beam width, effect, antennas and other physical characteristics. They are designed for a wide range of use cases [12]–[14], including voice and data transmission, radiodetermination (tracking, homing) and monitoring, and hence they have different criticality. All of these factors have resulted in different security requirements and implementations, and Pavur et al. [15] argue that there has to be a balance between satellite network performance and security robustness. Unfortunately, many of these systems have proven to contain numerous vulnerabilities, such as backdoors, hardcoded credentials for the terminals, and insecure protocols, misconfiguration or lack of encryption for segments of the network [15]–[17]. As pointed out by Caprolu et al. [18], it is generally difficult to assess the security of privately run SATCOM systems since the involved protocols are mostly closed source and undocumented.

As argued by Wozniak et al. [7] and Raulefs et al. [19], there are no SATCOM or shorter ranged transmission technologies that fully meet today's requirements for broadband maritime systems. Hence, there has been research on other approaches, such as multihop maritime communication systems, which essentially is data forwarding using mesh topologies. Røste et al. [9] have proposed the Wireless Coastal Area Network (WiCAN) concept which combines different mobile communications technologies SATCOM systems using an intelligent router onboard the ship, however, how to achieve appropriate security when mixing technologies is not addressed. Mu et al. [20] have proposed an integrated wireless Communication Architecture for Maritime Sector (CAMS), in which a secure tunnel on top of various data links can be setup between a ship and the home network. However, this does not solve the challenge of ship-ship and cross-sectoral security compatibility. VDES [1] is a new standard that provides two-way communication and an extension to AIS. It operates over VHF for ship-ship and ship-shore communication, but has also a satellite component (VDE-SAT) that extend the terrestrial component (VDE-TER) to provide global coverage [21]. Though VDES has data verification mechanisms, there is no real built-in data protection.

It is also feasible to establish dynamic 5G private networks for maritime applications, which connect to onshore base-stations (coast-5G [8]) using Integrated Access and Backhaul (IAB) or Non-Terrestrial Networks (NTN) technology [22]. This is still on a conceptual stage, but is expected to provide a broad range of security features for multiple industry segments, including authentication in public and non-public networks, user plane integrity protection and Virtual Network Functions (VNF).

Caprolu et al. [18] have analysed vulnerabilities in communication technologies used within large vessels. They found that the major security challenges are related to GNSS and AIS spoofing detection, jamming as a part of electronic warfare, lack of SATCOM security standardization, insufficient bridge systems assessments, poor mitigation of malware spreading and outdated, closed-source communication protocols.

When we extend the problem domain to also cover additional sectors, we run into further challenges. The ones that we consider most obvious can be summed up as:

- The sectors mainly rely on different communication technologies and standards. This is especially evident between terrestrial and non-terrestrial infrastructures. Just as within the maritime sector alone, it is therefore unlikely that we can rely on a single solution, and we have to see how technologies and security can be combined.
- There are legacy issues in all sectors, and it is not feasible to quickly replace or upgrade technologies that is already in place. Instead, we might foresee a security convergence that can take decades.
- There are different authorities and trusted third parties that manage each sector. In addition, sectors that operate globally may suffer from political conflicts and disgruntlement between national states. This can result in situations where e.g., cryptographic algorithms in one area not allowed to be used in others due to import restrictions and lack of trust.

In the next section, we revisit the SAR example to show a possible road forward, despite these numerous challenges.

III. The road ahead

To protect the exchange of digital messages independent on the underlying communication infrastructure, the establishment of an international Public Key Infrastructure (PKI) is a feasible solution [23], [24]. This is basically the way our modern Internet works today. By issuing certificates to sea- or shore-based actors, they can use public key cryptography to ensure confidentiality, integrity, authenticity, and non-repudiation of the information exchanged. Such a PKI solution has already been considered by the International Maritime Organization (IMO) and brought into the ongoing standardization by the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) [25]. It is also the approach suggested by the Maritime Connectivity Platform (MCP) Consortium [26].

The maritime PKI can enable security in a scenario like the one outlined in Fig. I, by providing authenticity and integrity protection of the information that is exchanged and by allowing the communicating actors to establish a secure link for the exchange of information. Those actors are marked with green in the figure. Enabling security means that the actors can make sure that no unauthorized persons and/or organizations are interceptions and/or disturbing the communication. However, one needs to make sure that also:

- Actors with outdated technology, for example a nearby leisure ship with "old fashioned" AIS equipment (Class B, marked with red in the figure), must be able to send and receive relevant information, but by using the existing AIS and VHF (voice) communication channels.
- Actors without VDES connectivity, for example a nearby ship with a mobile Internet connection (also marked with red in the figure), must be able to send and receive relevant information, but by using their existing network connection.
- Actors from other sectors, such as the coastguards, police or red-cross (also marked by red in the figure), must be able to collaborate and exchange relevant information.

Ideally, a security solution should be able to function properly also under such circumstances, thereby providing a holistic way of securing communication in multi-modal scenarios. To achieve this goal, we foresee the following possible and practical paths forward:

A All actors are enrolled in the same (maritime) PKI, managed by the same Certificate Authority (CA). If there are several PKIs for each sector, entities can have multiple certificates (one for each for PKI). For the representation of the identities of these actors, the Maritime Resource Name (MRN) [27], which is a naming scheme that can uniquely identify any maritime resource on a global scale, could be a starting point. This naming scheme covers all kinds of maritime resources that has an identity of some kind, however, resources from other sectors are not included here. Hence, MRN could be extended to also allow for non-maritime resources.

B Establishing trust between the CAs of the different sectors. Each CA manages its own "forest" of entities. It is possible to use cross-forest enrolment to issue certificates to entities in one forest from a CA in another forest (see Cooper et al. [28]). Cryptographic protocols, algorithms and key lengths must be compatible.

C Establishing trust between the CAs of the different sectors using Blockchain [29] is an alternative. A Blockchain, by definition, can create trust where there is none, and could thus be used to allow secure cross-sectoral communication. This solution is less mature than the cross-forest enrolment (proposed in B), but would allow the use of different cryptographic protocols, algorithms, and key lengths.

D Fallback to an insecure channel for a short period of time. For example, in an emergency, actors can choose to ignore signature and/or disable encryption. After such event, there should be a thorough post-event analysis looking for possible misuse of the system. Eventually, a discussion regarding possible vulnerabilities (e.g. downward compatibility) and the effects of lacking security is needed.

E When messages are relayed through different sectors, using different communication technologies, use wrapping/tunnelling to protect the information where possible.

F When messages are relayed through different sectors, using different communication technologies and different message formatting (e.g., data - voice), rely on point-to-point security solutions. This requires an evaluation of the existing security levels to make sure that there are no security downgrades along the chain that can be exploited.

These paths may not be sufficient to take us all the way to our goal, but will at least allow us to explore the terrain of security for multi-modal communication further.

Acknowledgement

This work has been partially supported by the Research Council of Norway through the projects "Cyber Security in Merchant Shipping - Service Evolution" with contract number 295969 and "Digital Ecosystems for Smart and Autonomous Ships" with contract number 309255. Support has also been received from "CyberSec4Europe", Grant Agreement No. 830929, and "AEGIS", Grant Agreement No. 859992, both belonging to the European Union's Horizon 2020 Programme.

References

[1] IALA, "VHF Data Exchange System," 2021, accessed: 2021-07-09. [Online]. Available: https://www.iala-aism.org/technical/connectivity/vdes-vhf-data-exchange-system/

[2] EU, "European Maritime Single Window environment (EMSWe)," 2020, accessed: 2021-07-09. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A4407248

[3] G. Loukas, D. Gan, and T. Vuong, "A review of cyber threats and defence approaches in emergency management," *Future Internet*, vol. 5, no. 2, pp. 205–236, 2013.

[4] N. Andreassen, O. J. Borch, and A. K. Sydnes, "Information sharing and emergency response coordination," *Safety Science*, vol. 130, p. 104895, 2020.

[5] F. Bekkadal, "Future maritime communications technologies," 06 2009, pp. 1 – 6.

[6] K. Grover, A. Lim, and Q. Yang, "Jamming and anti–jamming techniques in wireless networks: a survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.

[7] J. Wozniak, K. Gierlowski, and M. Hoeft, "Broadband communication solutions for maritime itss: Wider and faster deployment of new e-navigation services," in *2017 15th International Conference on ITS Telecommunications (ITST)*, 2017, pp. 1–11.

[8] C. Yu, J. Li, C. Zhang, H. Li, R. He, and B. Lin, "Maritime broadband communications: Applications, challenges and an offshore 5g-virtual mimo paradigm," in *2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*. IEEE, 2020, pp. 1286–1291.

[9] T. Røste, K. Yang, and F. Bekkadal, "Coastal coverage for maritime broadband communications," in *2013 MTS/IEEE OCEANS - Bergen*, 2013, pp. 1–8.

[10] Kongsberg, "Maritime Broadband Radio - MBR," 2021, accessed: 2021-07-09. [Online]. Available: https://www.kongsberg.com/maritime/products/bridge-systems-and-control-centres/broadband-radios/maritime-broadband-radio/

[11] A. A. Allal, K. Mansouri, M. Youssfi, and M. Qbadou, "Toward a new maritime communication system in detroit of gibraltar where conventional and autonomous ships will co-exist," in *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2017, pp. 1–8.

[12] D. S. Ilcev, "The development of maritime satellite communications since 1976," *International Journal of Maritime History*, vol. 31, no. 1, pp. 145–156, 2019.

[13] F. Bekkadal and K. Yang, "Novel maritime communications technologies," in *2010 10th Mediterranean Microwave Symposium*, 2010, pp. 338–341.

[14] IMO, "Convention on the International Maritime Satellite Organization," 1976, accessed: 2021-07-09. [Online]. Available: https://www.imo.org/en/About/Conventions/Pages/Convention-on-the-International-Maritime-Satellite-Organization.aspx

[15] J. Pavur, D. Moser, V. Lenders, and I. Martinovic, "Secrets in the sky: on privacy and infrastructure security in dvb-s satellite broadband," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 277–284.

[16] R. Santamarta, "SATCOM terminals: Hacking by air, sea, and land," *DEFCON White Paper*, 2014.

[17] ——, *Last call for SATCOM security*. IOActive, 2018. [Online]. Available: https://ioactive.com/wp-content/uploads/2018/08/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf

[18] 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.

[19] R. Raulefs, M. Wirsing, and W. Wang, "Increasing long range coverage by multiple antennas for maritime broadband communications," in *OCEANS 2018 MTS/IEEE Charleston*, 2018, pp. 1–6.

[20] L. Mu, R. Kumar, and A. Prinz, "An integrated wireless communication architecture for maritime sector," in *Multiple Access Communications*, C. Sacchi, B. Bellalta, A. Vinel, C. Schlegel, F. Granelli, and Y. Zhang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 193–205.

[21] SpaceNorway, "VHF Data Exchange System (VDES)," 2021, accessed: 2021-07-09. [Online]. Available: https://spacenorway.no/vhf-data-exchange-system-vdes-page-under-development/

[22] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5g evolution: A view on 5g cellular technology beyond 3gpp release 15," *IEEE Access*, vol. 7, pp. 127 639–127 651, 2019.

[23] C. Frøystad, K. Bernsmed, and P. H. Meland, "Protecting future maritime communication," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–10.

[24] G. Bour, K. Bernsmed, R. Borgaonkar, and P. H. Meland, "On the certificate revocation problem in the maritime sector," in *Secure IT Systems: 25th Nordic Conference, NordSec 2020, Virtual Event, November 23–24, 2020, Proceedings 25*. Springer, 2021, pp. 142–157.

[25] IALA, "G1139 – The Technical Specification of VDES," International Association of Marine Aids to Navigation and Lighthouse Authorities, Tech. Rep., 6 2017. [Online]. Available: https://www.iala-aism.org/product/g1139-technical-specification-vdes/

[26] MCC, "Maritime Connectivity Platform," 2021, accessed: 2021-07-09. [Online]. Available: https://maritimeconnectivity.net/

[27] IALA, "Maritime Resource Name," 2021, accessed: 2021-07-07. [Online]. Available: https://www.iala-aism.org/technical/data-modelling/mrn/

[28] M. Cooper, Y. Dzambasow, P. Hesse, S. Joseph, and R. Nicholas, "Internet x. 509 public key infrastructure: Certification path building," *Network working group, RFC*, vol. 4158, 2005. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4158#page-30

[29] Ø. J. Rødseth, P. H. Meland, C. Frøystad, and O. V. Drugan, "PKI vs. Blockchain when Securing Maritime Operations," *European Journal of Navigation*, 2019.