

Review

Maritime Communications—Current State and the Future Potential with SDN and SDR

Nadia Niknami ^{1,*}, Avinash Srinivasan ^{2,*}, Ken St. Germain ² and Jie Wu ¹¹ Center of Networked Computing, Temple University, Philadelphia, PA 19122, USA; jiewu@temple.edu² Department of Cyber Science, United States Naval Academy, Annapolis, MD 21402, USA; stgermai@usna.edu

* Correspondence: tun03933@temple.edu (N.N.); srinivas@usna.edu (A.S.)

† These authors contributed equally to this work.

Abstract: The rise of the Internet of Things (IoT) has opened up exciting possibilities for new applications. One such novel application is the modernization of maritime communications. Effective maritime communication is vital for ensuring the safety of crew members, vessels, and cargo. The maritime industry is responsible for the transportation of a significant portion of global trade, and as such, the efficient and secure transfer of information is essential to maintain the flow of goods and services. With the increasing complexity of maritime operations, technological advancements such as unmanned aerial vehicles (UAVs), autonomous underwater vehicles (AUVs), and the Internet of Ships (IoS) have been introduced to enhance communication and operational efficiency. However, these technologies also bring new challenges in terms of security and network management. Compromised IT systems, with escalated privileges, can potentially enable easy and ready access to operational technology (OT) systems and networks with the same privileges, with an increased risk of zero-day attacks. In this paper, we first provide a review of the current state and modalities of maritime communications. We then review the current adoption of software-defined radios (SDRs) and software-defined networks (SDNs) in the maritime industry and evaluate their impact as maritime IoT enablers. Finally, as a key contribution of this paper, we propose a unified SDN–SDR-driven cross-layer communications framework that leverages the existing SATCOM communications infrastructure, for improved and resilient maritime communications in highly dynamic and resource-constrained environments.



Citation: Niknami, N.; Srinivasan, A.; St. Germain, K.; Wu, J. Maritime Communications—Current State and the Future Potential with SDN and SDR. *Network* **2023**, *3*, 563–584.

<https://doi.org/10.3390/network3040025>

Academic Editor: Martin Reisslein

Received: 30 October 2023

Revised: 22 November 2023

Accepted: 7 December 2023

Published: 14 December 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: autonomous underwater vehicles; IoT; maritime communication; software-defined networking; software-defined radio; unmanned aerial vehicles

1. Introduction

An Internet of Things (IoT) system involves the interconnection of devices using the Internet as a communication medium. A gamut of application domains have and continue to benefit from the emergence of IoT, including traffic management, critical infrastructure, and transportation sectors, such as the shipping industry. In the domain of ship technology, the IoT offers new opportunities to make use of interconnections between the physical and cyber layers, as well as the integration of all the ship's components with the cyber systems, including global navigation satellite systems (GNSS), automatic identification systems (AIS), and electronic chart display systems (ECDIS). Maritime communications are also crucial for IoT applications such as monitoring the environment and controlling climate change. While it is true that 4G and 5G can be installed in maritime environments, their application to onshore environments is restricted since base stations cannot be located offshore. Consequently, satellites are an essential component of maritime communication. Satellites are essential for providing connectivity to oceans that are sparsely connected operating areas, despite the high costs of proprietary terminals and the limited bandwidth availability [1].

Internet of Ships (IoS) and maritime IoT are becoming increasingly popular [2], and their numerous applications are presented in Figure 1. A more crucial aspect of the maritime industry and scientific research is the ability to connect devices in order to facilitate navigation and data collection. The maritime environment differs significantly from conventional land propagation environments since there are no physical barriers such as buildings or hills to obstruct the wireless signals. However, when considering wireless communications over inland waterways, it is important to account for potential obstacles such as buildings, bridges, and vessels passing beneath. These obstructions primarily impact large vehicles and buildings located near the waterways. It is also important to consider equipment located in offshore areas and vessels located in deep-sea regions when considering wireless communications over the sea. Furthermore, compared to terrestrial wireless communications, maritime wireless communications must take into account the combined air–water–land effects [1]. Furthermore, cities and areas bordering waterways and maritime traffic areas should expect customer demand in those regions as well as in their traditional terrestrial base. This demand will bring additional infrastructure requirements to include wireless coverage, network traffic, and power for supporting ancillary systems.

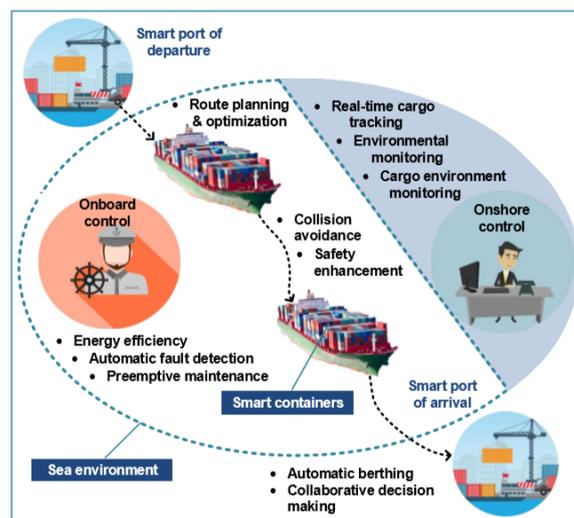


Figure 1. Key emerging applications of IoS [2].

The diverse set of platforms of maritime communications widely acknowledged and accepted in the current literature [3–5], shown in Figure 2, are as follows:

1. Land platforms consist of satellite stations, cellular towers, and UAV stations, among other things.
2. Water platforms can be categorized into three layers—seabed, underwater, surface. The seabed layer consists of various sensors; the underwater layer consists of AUVs and submarines, among other things; and the surface layer consists of ships, buoys, and USVs, among other things.
3. Air platforms consist of UAVs and Hawkeye aircraft that play a critical role in relaying air-to-air and ship-to-air radio communications.
4. Space platforms consist of two types of satellites—navigation satellites and communication satellites—in three possible orbits—low earth orbit (LEO), medium earth orbit (MEO), and geostationary orbit (GEO).

Software-defined radio (SDR) and software-defined network (SDN) are both examples of software-defined technologies that are revolutionizing traditional hardware-based networks and communications systems. SDR uses software to replace hardware in radio systems, while SDN uses software to abstract and automate the network control functions. Both SDR and SDN provide greater flexibility and programmability, enabling the development and deployment of more agile and adaptive systems. More importantly,

SDR and SDN can be integrated to create dynamic, software-defined radio access networks (SD-RANs), which can improve the overall network performance, reliability, and security [6].

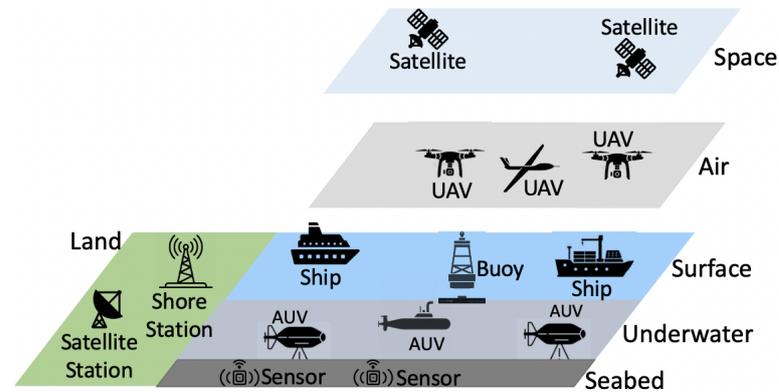


Figure 2. Diverse set of maritime communications platforms.

In the context of maritime communication, SDR and SDN can offer significant advantages over traditional hardware-based networks and communications systems. SDR can be used to create more flexible and adaptive radio systems, which are particularly useful in dynamic maritime environments [7]. In addition, SDR can be used to dynamically adjust radio frequency and modulation parameters to improve communication quality and reliability, even in very challenging environments. Similarly, SDN can be used to create more efficient and automated network management systems for maritime communication networks [8]. For example, SDN can be used to centralize network control and automate network configuration and monitoring functions. This can simplify the management of complex maritime communication networks, improve network efficiency, and reduce operational costs.

This research focuses on laying the groundwork for the modernization of maritime communications in the era of the IoT. It addresses the vital need to ensure the safety of crew members, vessels, and cargo in the maritime industry, which plays a crucial role in global trade. The adoption of advanced technologies, including unmanned aerial vehicles, autonomous underwater vehicles, and the Internet of Ships, offers opportunities for enhanced communication and operational efficiency. However, this technological evolution also introduces new security and network management challenges, necessitating a comprehensive evaluation of the current state of maritime communications and the impact of SDRs and SDNs as enablers of IoT in the maritime sector. This research seeks to address these critical issues to enhance maritime operations, safety, and security.

Our key contributions in this article are as follows:

- We provide an in-depth review of the current state and various modalities of maritime communications, providing a foundational understanding of the existing landscape.
- We assess the adoption and the potential impact of software-defined radios (SDRs) and software-defined networks (SDNs) in the maritime industry, focusing on their role as IoT enablers. The proposed framework leverages the flexibility of SDRs and SDNs for improved resiliency in maritime communications.
- The proposed maritime communications framework seamlessly integrates with existing satellite communication (SATCOM) infrastructure, for improved communication efficiency and resiliency.

The remainder of this paper is organized as follows: In Section 2, we provide the background and rationale for the proposed approach. Section 3 delves into the details of IoT, followed by discussions on security challenges in maritime networks in Section 4. Section 5 presents the proposed framework for SDN-SDR-based maritime communications, followed by conclusions and future research direction in Section 6.

2. Background and Definitions

It has become increasingly important to maintain maritime communication as oceanic activities have increased dramatically, including naval shipping and logistics, offshore oil exploration, wind farms, fishing, and tourism, among others [9]. There are three broad types of maritime communication systems: 1. radio communication, 2. satellite communication (SATCOM), and 3. shore-based mobile communication. Below are the three most significant communications challenges currently faced by the maritime industry:

- **Range:** A Wi-Fi signal can travel approximately 330 feet (100 m) from an on-land base station, but this may be affected by obstructions between the base station and the receiver, which limits their reliability. Even though Wi-Fi appears to be an economical and fast networking solution, its use is limited by its range of restrictions.
- **Latency:** There has been considerable effort toward solving the latency problem. While it is not possible to completely eliminate latency, significant improvements have been made to minimize the latency [8,10]. Using satellites requires sending data as radio waves from ground equipment (transmitter) to a satellite (in space), which is then re-transmitted by the satellite to a receiving ground equipment (receiver). While this process occurs at the speed of light, the distance the data must travel and a small amount of processing of signal at the satellite result in latency.
- **Service Demands:** With advances in networking, IoT, and smart technologies, the demand for data services is at an all-time high [11]. The provision of network connectivity on a cruise ship requires robust and flexible technology, not only for safety, communication, and navigational purposes but also for recreational and business purposes. As a result of this increase in service demands, reliable, flexible, robust, and agile maritime networks have become an essential component of maritime infrastructure [8].

2.1. Maritime Communication

The right communication protocol must be used for a vessel network to achieve a clear signal. Ensuring communication and navigational safety in maritime activities is paramount, and this is where maritime communications, spanning both inland waterway and sea communications, play a pivotal role as a critical technology [1]. In addition to waterway and sea communications, there are also aerial, space, and terrestrial communications. Developing a robust communication solution for IoT applications in the maritime environment is crucial to minimize external interference and ensure reliable data transmission from senders, such as smart containers, to receivers, such as cloud services. This is vital to maintain the integrity and efficiency of maritime IoT systems, enabling seamless connectivity and effective data exchange in the face of potential disruptions or signal disturbances. Communications technologies can be broadly categorized into the following categories:

- **Near Range**—The near range technologies are for short-range communications within a limited area or proximity, such as ship-to-ship or ship-to-shore communication over short distances.
- **Wide Area**—The wide area technologies are for long-range communication over larger geographic areas, often facilitated by SATCOM systems providing global coverage.
- **Narrowband**—Narrowband technologies are for communication systems operating within a narrow frequency range, typically used for transmitting small amounts of data, such as text messages or basic voice communication.
- **Broadband**—Broadband technologies are for high-speed data transmission allowing for transferring large amounts of data, enabling multimedia applications, video streaming, and high-quality voice communication. Examples include cellular networks, very-small-aperture-terminal (VSAT) systems, and dedicated maritime broadband services.

Due to the small amount of data typically transmitted by near-range communication devices, such as those utilizing NFC, the required battery size is small, enabling extended battery life. It is possible to send larger amounts of data using other near-range communi-

cation protocols. The Wi-Fi system, for example, can deliver a large amount of data, but the Wi-Fi signal range is generally limited to 100 m from a single access point [12]. To cover larger areas, such as an ocean vessel, multiple access points or repeaters are often necessary for Wi-Fi deployment. Bluetooth technology, on the other hand, has the capability to establish communication over extended distances, particularly with the advancements in Bluetooth 5. However, it typically operates at slower data rates compared to Wi-Fi. It is worth noting that Bluetooth can be a suitable choice for certain applications, even though it may have slower data transfer speeds when compared to Wi-Fi. Mobile cellular communication is a potential wide-area technology for the transmission of large amounts of data over large geographical areas, which maritime communications can benefit from. Mobile cellular services generally have the capability to send and receive larger amounts of data compared to Wi-Fi. The exact data capacity and speed of mobile cellular networks depend on various factors, such as the specific generation of cellular technology (e.g., 3G, 4G, 5G), network coverage, and available bandwidth. It is a licensed technology that requires mobile operators to obtain permission to operate a network within a specific geographical region. However, due to the higher power consumption of cellular technology, it can significantly impact the battery life of low-power devices.

While there are other communication protocols that are capable of transmitting data over a wide area, they do suffer from low data rates and can typically only transmit kilobytes of information instead of megabytes. Among these protocols is the long range (LoRa) protocol. LoRa is an unlicensed technology that employs spread spectrum modulation and enables the transmission of small amounts of data over long distances while consuming less power [13]. A typical application of the LoRa protocol would be monitoring water or gas meters over a large geographical area. Due to the small amounts of data transmitted, the battery life of the device running protocols such as LoRa is relatively long.

2.2. Unmanned Aerial Vehicles (UAVs)

An aerial network consists of multiple unmanned aerial vehicles (UAVs). Since UAVs are capable of flying, it is very attractive to deploy them as aerial base stations and relays [14]. The airborne UAVs can communicate directly with other airborne UAVs or with ground stations [15]. However, the management of UAV airborne networks poses significant challenges. These networks involve the exchange of vast amounts of information, including flight and control information, protocol stack information, sensing information, and data obtained from ground terminals. Furthermore, due to the constant motion of UAVs, wireless links and network topologies are continuously changing. As a result, managing and utilizing information, handling intermittent links, and maintaining a fluid topology have become highly challenging tasks [16,17]. In maritime environments, UAV communication also faces challenges to the channel characteristics, including temperature of troposphere above the ocean, pressure, waveguide impact due to humidity, signal attenuation due to climate change, and uneven scatterer effect on UAV-to-ship communication due to irregular sea waves [18]. Current 5G cellular networks mainly focus on the terrestrial scenarios and do not cover maritime areas, causing difficulties in developing maritime IoT [19,20].

Due to the difficulty of deploying communications infrastructure on the ocean, the performance of existing maritime communication networks (MCNs) is far behind 5G [19]. However, the ubiquitous deployment of UAVs for wireless communication purposes can offer a potential solution to bridge the 5G gap between networks in the air and those on ground. With agile UAVs, there is an opportunity to provide maritime coverage in fixed sea lanes, without relying on costly satellite systems or on-shore stationary base stations. By employing a hybrid architecture, UAVs can establish connections with terrestrial base stations along the coast while utilizing satellites for backhaul over long distances. To better optimize the UAV deployment in response to the sporadic presence of ships in shipping lanes, it can be tailored to address the specific needs and requirements of users [19]. The use of tethered UAVs and helicopters is an alternative option for large ships and cruise

ships. Tethering UAVs simplifies the provision of energy by allowing continuous power supply through the tether. This eliminates the challenge of limited battery life and enables the UAVs to operate for an extended duration [21,22]. Tethered UAVs provide a reliable and continuous power source for aerial operations, making them suitable for various applications in maritime contexts.

2.3. Autonomous Underwater Vehicles (AUVs)

The autonomous underwater vehicle (AUV) is a robot that travels underwater without the assistance of an operator. Underwater projects and mapping missions using AUVs can help commercial and recreational vessels detect and map submerged wrecks, rocks, and obstructions that may present navigational hazards [23]. Deep-sea data collection is a unique application of delay-tolerant networks (DTNs). There are several reasons for this, including the need for timely data reporting and the inevitable delay in acoustic transmissions in the ocean [24]. A AUV surfaces frequently to transmit the data obtained from sensors—in two-dimensional or three-dimensional search space—to surface stations. Whenever an AUV ascends to the surface to establish communication with the surface stations, an additional delay occurs in the data transmission process. In [25], the authors show that by optimizing the number and location of AUV resurfacing events, it is possible to minimize the average data-reporting delay.

Additionally, underwater wireless sensor networks consume a significant amount of energy and are unbalanced, which poses a substantial challenge for AUVs. AUVs receive data directly from nodes located near the trajectory, while those farther away send data to their neighbors. In order to overcome this problem, a trajectory adjustment mechanism can be used, but this would result in nodes near the trajectory of the AUV consuming energy more rapidly and dying earlier than expected. In order to adjust the trajectory, a data collection scheme based on the location prediction of the AUV is incorporated in [26], wherein the nodes follow a predefined trajectory in order to predict the location of the AUV. The nodes that are located near the trajectory of the AUV send data to the AUV after collecting it from other nodes. In order to minimize the effects of the harsh underwater environment, a reliable mechanism has been developed to improve the performance of the network and to balance the load on the nodes in order to extend the service life of the network [26].

2.4. Unmanned Surface Vessels (USV)

Unmanned surface vessels (USVs) and unmanned surface vehicles are autonomous vehicles capable of performing tasks in diverse and complex environments without human intervention. In maritime communications, the limitations of UAVs have prompted industry and academia to explore the potential of USVs as a competitive solution to achieving the vision of 6G networks with seamless coverage and autonomous capabilities [27]. USVs' robust, waterproof technology allows for long-term operation, even in challenging weather conditions. They possess the ability to autonomously sense and gather information from various maritime terminals, promptly identifying risks and responding accordingly. These USVs are dispatched to periodically collect maritime data from buoys and sensor nodes across vast areas. Equipped with high-gain antennas and computation units, USVs are well-prepared for future mobile communications in computing and caching-enabled networks. They can perform local computations or offload tasks to satellites or base stations as needed [11]. USVs offer numerous advantages for future maritime wireless communication systems. They can provide flexible wireless communication services to remote maritime devices, such as ships, buoys, beacons, sensors, and platforms, without the need for dedicated high-gain antennas or satellite infrastructure. This enables the expansion of communication coverage beyond terrestrial domains, facilitating commercial and military applications such as deep-sea sightseeing and broad-sea monitoring. They can undertake longer and more hazardous missions, incur lower maintenance costs, ensure greater personnel safety due to their unmanned nature, and possess enhanced maneuverability and deployability

in shallow waters where larger craft might struggle. Additionally, USVs have the potential for enabling deeper water depth monitoring and sampling compared to aircraft/UAVs and spacecraft [28].

3. IT, IoT, IIoT, IoUT, and OT

An IoT system is a gateway for the maritime industry. The gateway is used to communicate between the hardware components, such as sensors and machinery, and the cloud. Additionally, gateways can be configured to provide only selective information to each other and complete information only to the cloud. Information technology (IT) in maritime communication involves the use of computer systems, software applications, and networks to manage and process information related to maritime operations. This includes data storage; transmission; analysis; and communication between vessels, shore-based facilities, and other stakeholders involved in maritime activities. Operational technology (OT) refers to the specialized systems and technologies used to control and monitor devices, events, and processes in enterprise or industrial operations. With maritime operations, OT includes equipment; software; and networks that enable real-time communication, navigation, vessel control, safety systems, and other operational functions specific to the maritime industry.

The Industrial Internet of Things (IIoT) refers to the extension and use of IoT in industrial applications and sectors. In marine and underwater environments, the Internet of Underwater Things (IoUT) is an emerging communication ecosystem that connects underwater objects [29]. IoUT technology plays a crucial role in various aspects of the maritime industry, including smart boats, ships, shores, and oceans. It enables automatic marine transport, precise positioning and navigation, underwater exploration, and disaster prediction, and prevention, as well as intelligent monitoring and security [30]. Although IoUT devices generally do not generate new data at high frequencies, it is essential to establish connectivity through methods such as acoustic, magnetic induction, and onboard wireless communication. Maritime IoT and IoUT devices encounter the challenge of ensuring continuous power or managing battery replacements. Consequently, these devices need to be designed to harness energy from ocean-based renewable sources. Ships traveling on seas, along coasts, or through shipping channels are included in the maritime market. A major component of maritime demand is cargo tracking, telematics, asset monitoring, border control, safety, scientific research, fleet management, and ocean monitoring [31]. A further sub-category of IoT applications in maritime networks can be identified as follows:

- **Cargo:** In the maritime industry, one of the key applications of IoT technology is the monitoring and tracking of large items, such as shipping containers, as they move along shipping routes. Additionally, IoT devices can be utilized for fleet management, which can automate and improve the efficiency of logistics, supply, maintenance, and operations associated with the fleet [32].
- **Cruise/ferry:** The utilization of satellite technology is prevalent in various domains such as fishing, cruise, ferry, and leisure markets. As vessels incorporate specialized equipment for IoT sensor data and IoT connectivity, the use of satellite technology is projected to increase even further.
- **Fishing:** There has been a significant improvement in the efficiency of monitoring, controlling, and supervising fishing vessels as a result of vessel monitoring systems (VMS). The use of VMS has become mandatory in several countries in recent years to ensure that fishing vessels report their catches to fishery management agencies.

The maritime network is characterized by the involvement of nodes such as ships and buoys in the development of an IoT setup, which led to the idea of Internet of Ships (IoS). Through high-level virtualization of the core network, the IoS enables the coordination of node computation to achieve forecasting analysis by using machine learning and artificial intelligence methods. UAVs can also be used to collect information in addition to IoT maritime sensor nodes. The battery life of the UAVs may limit this method, particularly if the head node is mobile and gathers data from the sensor nodes. There are a number of

industrial and scientific applications that require the connectivity of underwater objects, including oil exploration, environmental monitoring, disaster prevention, and disaster recovery [2]. Ships, buoys, and autonomous surface vehicles can serve as data collection stations, or sinks, by gathering data from underwater sensor networks and transmitting them to a control center via radio waves. This approach allows for efficient and cost-effective data collection and monitoring in marine environments.

4. Current Security Challenges in Maritime Networks

There is no standardized cybersecurity strategy for maritime transportation, which is a safety-critical activity. Cybersecurity attacks on shipping lines may have severe consequences, such as maritime accidents and supply chain disruptions. Cyber-attacks can have the most severe consequences as autonomous vessels become more prevalent [33]. The threat of maritime cyber-attacks adds a level of complexity to the traditional maritime threats of piracy, illegal activities, maritime terrorism, and accidents at sea. Digitalization, automation, and connectivity are increasingly prevalent in the global maritime sector. In recent years, cyber threats have increased significantly. In the past few years, cyber-attacks on shore-based maritime-related systems have increased nine-fold, while GPS and AIS spoofing have frequently been observed [34]. Infiltrating and controlling a commercial vessel in order to capsize, collide, or cause environmental damage is now well within the realm of possibility [34]. A variety of complex automated systems are installed on modern and autonomous ships, including navigation systems, radio detection and ranging (radar), automatic identification systems (AISs), communication systems, and control systems to control a wide range of electro-mechanical systems, including the main engine, generator, and converter drive. In modern ships, the extensive use of automation and IT systems presents new opportunities for hackers and malicious actors to implement cyber-attacks that could have catastrophic consequences and cause major safety losses [35]. The main goal of the attackers is to gain remote access to ships and vessels, extract sensitive and valuable information for future attacks, or disrupt the ship's operations by tampering with crucial components and rendering automated systems non-functional [36]. Below are some potential vulnerabilities, the consequences of an attack, and actual incidents that have been reported:

- There is no authentication or integrity check on the AIS transponders, which makes them vulnerable to hacking, where they could be used to spread fake messages. Attackers use software-defined radios to transmit false man-in-the-water signals, enabling them to remain undetected and transmit false weather reports [35,36].
- Navigation and GPS technologies are actively used in the maritime sector, which is a target for a number of cyber-attacks that aim to exploit design flaws in order to destabilize services that rely on them [37]. By spoofing GPS signals, attackers are able to reroute a vessel without triggering an alarm or alert.
- Autonomous vessels depend on enhanced SATCOMs to transmit operational commands and sensor data, making them susceptible to cyber-attacks such as denial-of-service attacks and man-in-the-middle attacks [38].
- The maritime very-small-aperture-terminal (VSAT) is an essential component for high-speed data transmission during naval operations. However, it lacks authentication, encryption, security, or personal information verification, making all devices vulnerable to attacks at the implementation level. Attackers could send false signals or malicious codes to disable or compromise the system, potentially endangering the safe navigation of the vessel [39].
- It is common for the system to be run on old computers without security updates. It is possible to compromise the system when updating the maps by downloading them from the Internet or manually uploading them via USB. The use of this updated medium can expose the system to many security risks [40].
- Despite the fact that radar signals are harder to interrupt than satellite signals, they are still susceptible to interference and DDoS attacks. Radar can provide inaccurate

- information about nearby objects in the event of a cyber-attack due to false echoes caused by external radar waves. Inaccurate information can lead to ship collisions.
- In the maritime industry, several network types are used for the transmission of data collected and processed by networked information systems. These technologies include SHIPNET, SAFENET, C3I system, RICE 10, SHIP system 2000, Smart Ship, and TSCE. Several security vulnerabilities exist in these technologies, as the design and configuration of communication links between IT networks neglect to consider authentication and encryption methods, leading to potentially vulnerable and outdated systems being available on the Internet [41].

5. A Framework for SDN–SDR-Based Maritime Communications

SATCOM offers numerous advantages over traditional point-to-point terrestrial communications, with a wide geographical coverage being the most significant advantage. However, SATCOM's potential for providing extensive coverage across global regions, the high cost of implementation, and extended propagation delays pose significant hurdles to its deployment within the maritime sector [1]. The maritime industry largely relies on SATCOM systems, which are expensive and have a low data rate [42]. Frequent maritime activities, on the other hand, require high-speed and reliable data transmission in order to ensure smooth communication between vessels and the control center. Current maritime wireless communication systems, however, do not meet this demand. SDN and SDR have tremendous potential to revolutionize maritime communications. With the proper design, integration, and deployment of SDN–SDR-based wireless communications infrastructure with the existing SATCOM infrastructure, both network and physical layer complexities can be alleviated. Maritime communications can be better managed with the planned deployment of software at these two layers to meet the demands and constraints of constantly changing on- and off-shore maritime communication environmental conditions and jurisdictional regulations.

None of the current solutions in the literature have considered our proposed approach of leveraging SDN and SDR and the existing SATCOM infrastructure into a unified framework for robust maritime communications, especially offshore. An important element of introducing SDN and SDR into maritime communications is the simplification of the communication infrastructure onboard a vessel [7]. The introduction of SDN on top of SDR further bolsters the robustness of the communication infrastructure onboard a vessel, and together makes the management, maintenance, and troubleshooting much simpler. The remainder of this section focuses on the background of SDN and SDR and their potential to alleviate the challenges of maritime communications, followed by an intuitive use case for a unified SDN–SDR-based maritime communications framework integrated with existing SATCOM infrastructure.

5.1. The SDR Approach

The International Convention for the Safety of Life at Sea (SOLAS) requires maritime operators to comply with a host of requirements that specify certain constraints on shipboard radio equipment [43]. Likewise, the International Telecommunication Union (ITU) has specified equipment to comply with the SOLAS Convention requirements [44]. Among these requirements are two-way VHF voice communication and, depending on the vessel, could also include AIS, satellite equipment, and emergency-position-indicating radio beacons. The ITU also identified trends that include E-navigation, VHF data exchange systems, and VHF voice digitalization.

5.1.1. SDR Background

An SDR provides traditional hardware-based signal processing in a reconfigurable software environment [45]. Where each new iteration of a communication standard requires legacy radios to upgrade to the most recent chipset and transceiver components to take advantage of new features, an SDR can be adapted to incorporate the changes by

reprogramming the software that runs on programmable hardware [46]. Adopting the use of SDRs can allow for switching from one communication standard to another, or even using the same communication standard in countries that have differences in the physical layer protocols. Using the 5G spectrum as an example, countries in the Americas, Europe, and Asia are licensing different frequencies to operate equipment [47]. Instead of carrying on board and maintaining a multitude of radios, SDRs can be reprogrammed and use infrastructure common among varying implementations. While the use of a purpose-built radio for a globally agreed standard need not be discarded in favor of an SDR, there may be times or operating conditions when the SDR is superior. Marine VHF radios use analog modulation for voice, while AIS is also a VHF band system that uses a digital modulation [48].

A single SDR can take the place of both of these radios and implement further functionality, such as the translation of voice-to-text information or even communication similar to SMS messages. Additionally, the SDR allows for agility in transmitting or receiving signals and can be adapted for the wireless environment. Atmospheric ducting has a significant impact on electromagnetic wave propagation. Signals may travel well beyond expected distances and cause unintended interference. An SDR can be used to partially mitigate this interference and ensure that minimum data rate performance is met. In [49], O'Shea et al. used an SDR to understand the effects of a wireless channel. They then used machine learning to develop a non-standard modulation symbol constellation to minimize the detection error of the received signal.

5.1.2. SDR Adoption

SDR solutions exist and may be implemented in maritime communication systems and enhanced to keep up with the increasing demand for novel functionality. The US Navy has been developing SDRs for implementation on surface ships and submarines, saving space, reducing maintenance requirements, and adding functionality [50]. There are over 900 radios that have been initially delivered, and these systems are being improved with new features that also include National Security Agency-certified encryption for both voice and data [51]. The maritime industry can make ready use of the lessons learned from the US Navy's investment and enjoy the benefits of capable SDRs. While still meeting SOLAS Convention and ITU requirements, SDRs offer an opportunity to improve current data rate capabilities and remain flexible for future changes in communication protocols. In [52], the authors present a prototype for AIS and VDES that is implemented on a low-cost SDR platform. Their prototype platform specifically executes a selectable code for the AIS and VHF data exchange system (VDES) services in transmission and reception modes. The prototype has implemented an additional platform for filtering and amplification in the AIS and VDES bands to improve the performance of the SDR platform.

In [53], the authors propose the creation of a low-cost AIS transmitter using SDR technology and open-source software. Through tests, the authors confirm that SDR-based AIS transmitters are a feasible solution since the AIS messages they sent out were received by commercial AIS equipment. Table 1 provides a summary of various studies exploring the utilization of SDN and SDR in maritime communications.

Table 1. Summary of Research Papers.

Reference	Summary
[14]	SDN-based framework for stable and efficient communication strategies for UAVs, addressing intermittent links, changing network topology, power constraints, link switching, routing, and load balance.
[54]	SDN-based UAV network controller collects network statistics, uses data for decision-making, emphasizing controller responsiveness, load, and device proximity for enhanced cost reduction, reduced latency, and reliability.

Table 1. *Cont.*

Reference	Summary
[55]	Joint sleep scheduling and opportunistic transmission scheme in maritime wireless communication networks using SDN to balance energy consumption and delay.
[56]	Use of multiple controllers for reducing response delay.
[57]	Integration of SDR-based AIS receiver into AAUSAT3 satellite, noting versatility and adaptability of new detection algorithms.
[58]	CrossFlow approach for application development in SDR networks, combining SDR and SDN principles for flexibility and modular architecture in wireless radio networks.
[59]	Discussion of SATCOM bandwidths on ships, highlighting the cost-effectiveness of indirect communication.
[52]	Presentation of a prototype for AIS and VDES using a low-cost SDR platform, with additional filtering and amplification for improved performance.
[53]	Proposal for a low-cost AIS transmitter using SDR technology and open-source software, confirming feasibility through tests.

5.2. The SDN Approach

5.2.1. SDN Background

There has been an increase in the use of software-defined networks (SDNs) in recent years, which promise to solve the problem of bundling between the control plane and the data plane. In an SDN, the control plane decides how network traffic should be handled, and the data plane forwards the traffic by the control plane's decisions. Logically centralized controllers simplify policy enforcement, network (re)configuration, evolution, and scalability by implementing control logic [60]. Figure 3 depicts mapping SDN and SDR to an OSI model. Some of the key advantages of SDNs are as follows:

- **Host Multiple Connections:** The ability to host multiple connections means that combinations of Wi-Fi, satellite, and mobile communication networks can be utilized as a single connection to provide a more streamlined and less complex maritime network. This also provides a certain level of redundancy for other connections in that, should one connection falter or go down, multiple others could take any redirected traffic onward to its destination.
- **Intelligent and Application-Based Routing:** One of the lesser celebrated but essential benefits of SDN solutions are their application-based routing [61] and intelligence capabilities [62]. This allows operators to build intelligence into their networks in order to understand the applications they run and their particular bandwidth requirements. Using the multiple wide area network (WAN) links available, maritime software-defined WAN administrators are able to benefit from dynamic application-level routing as well as implement application-based intelligence to overlay traditional packet-based routing. This enables the network to intelligently allocate the best possible connection for each individual bit of traffic.
- **Remote Management and Updates:** Leveraging SDN technologies can also save enterprises money, space, and resources by allowing SDN networks at their customers' sites to be managed by service providers from a centralized location. This also allows for networks to be updated remotely through software, instead of needing to house an IT specialist for the duration of every trip.

In summary, SDN provides centralized control and management, allowing administrators to dynamically allocate and prioritize network resources based on real-time needs. This flexibility enables efficient traffic management, ensuring smooth and reliable communication between maritime assets. Additionally, SDN's programmability enables the implementation of advanced security measures [63]. It allows for fine-grained access control, enabling administrators to create and enforce security policies across the network.

Moreover, SDN's separation of control and data planes enhances security by reducing the attack surface and preventing unauthorized access, especially when used in critical infrastructure such as maritime communication networks.

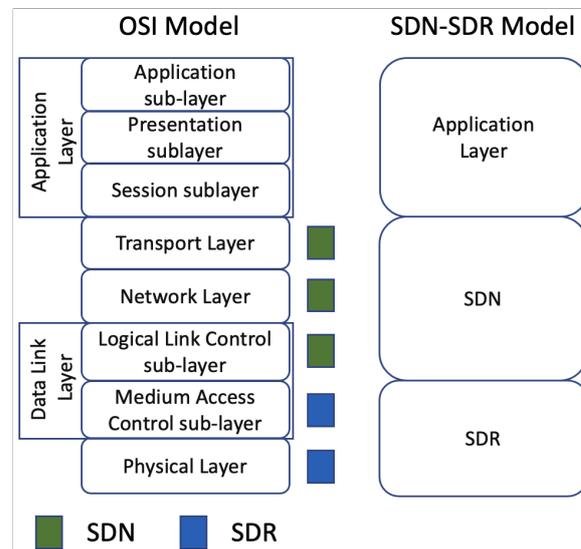


Figure 3. Mapping SDN and SDR to OSI model.

It should be noted that SDN, while offering unprecedented flexibility and efficiency in network management, can introduce challenges to system security. The centralization of control in SDN architectures creates a potential single point of failure, making the network vulnerable to targeted attacks. Additionally, the programmability of SDN controllers opens up new attack vectors, as malicious actors may exploit vulnerabilities in the software-defined infrastructure to manipulate network behavior. Moreover, the separation of the control plane from the data plane in SDN can expose communication channels between these components to security risks, potentially leading to unauthorized access or data breaches. As organizations increasingly adopt SDN to enhance their network capabilities, it becomes imperative to address these security concerns through robust encryption, access controls, and continuous monitoring to safeguard the integrity and confidentiality of network operations.

5.2.2. SDN Adoption

In maritime networks, establishing stable communication links is a significant challenge due to the constantly changing sea surface, which increases the risk of link fragility caused by sea waves. Therefore, finding a stable route is crucial to ensure network stability and minimize delays [64,65]. Recently, SDN has emerged as a solution to reduce the complexity of network management tasks [66–68]. By utilizing SDN, networks can be deployed and managed with greater flexibility, which reduces cost and increases availability. Additionally, the SDN controller integrates and learns from the information contained in the network itself to make intelligent decisions continuously.

In [14], the authors propose a solution for developing stable and efficient communication strategies for UAVs is an SDN-based framework that takes into account intermittent links, changing network topology due to UAV motions, and power constraints causing departures and arrivals of UAVs. Their framework also addresses the problem of link switching and routing to achieve load balance and extend the system's lifespan. In [54], a controller in the SDN-based UAV network collects network statistics and parameter information and uses the calculated results to make informed decisions. The efficacy of an SDN-based architecture is contingent on the responsiveness of the controller, which is heavily influenced by the controller load and the proximity of the SDN devices. The load imposed on a controller is determined by the volume of requests it receives from the

IoT devices it manages. SDN holds the potential for cost reduction, reduced latency, and enhanced network adaptability and reliability.

In [55], the authors present a joint sleep scheduling and opportunistic transmission scheme in delay-tolerant maritime wireless communication networks based on SDN to find a viable trade-off between energy consumption and delay. Another solution to reducing the delay of response is through the use of multiple controllers, as presented in [56]. Figure 4 presents an SDN with a maritime communications network.

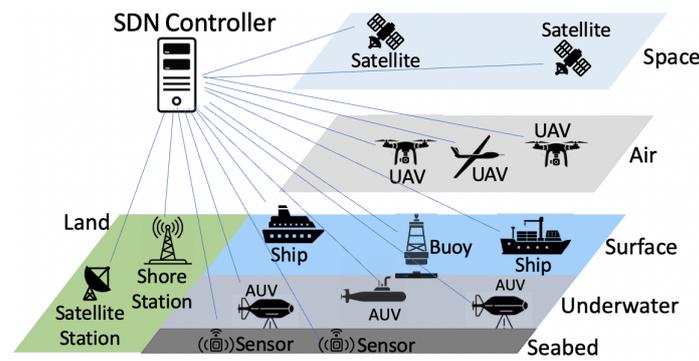


Figure 4. Maritime communications platforms with SDN.

Figure 5 depicts a potential maritime communications architecture leveraging SDNs and SDRs with multi-controllers. The proposed multi-controller SDN-based maritime network architecture has three planes—service, controller, and resource. This maritime network has a variety of aerial, space, ocean, underwater, and terrestrial IoT objects. Each controller controls a portion of the maritime network. The three controllers must work together to make the best decisions regarding the entire maritime network. This approach reduces both the response time and the load placed on a single controller. The sharing and load balancing of multiple SATCOM links in maritime networks, as well as the ability to overcome bandwidth constraints, are also challenges faced by SATCOMs in maritime networks. To solve these problems, each ship can be considered to be an SDN switch, and their management will be handled by a remote SDN controller [65].

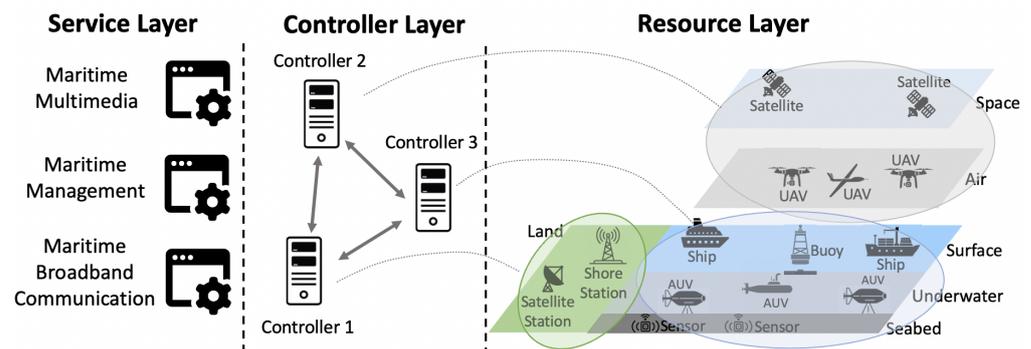


Figure 5. SDN-based maritime network.

5.3. Maritime Communications Security with SDN

An SDN-based framework can be used to mitigate attacks in an automated manner for improved resilience in the ship’s communication network [69]. There are sensors and actuators attached to the different components of the ship that are responsible for controlling the bridge, the engine, and the propulsion. The sensors transmit the data related to these physical devices to the controller for analysis. The controller, known as the Monitoring Controller, plays a crucial role in overseeing the operation of the ship’s components. It continuously monitors the data received from the sensors and analyzes them to ensure the proper functioning of the various ship components. Depending on the information

obtained from the bridge devices, the Monitoring Controller issues commands to start or stop the propulsion control system and can even reroute the ship on a different route if necessary.

With the help of the Detection Engine, the Monitoring Controller can quickly identify any anomalies or deviations from normal behavior. The Detection Engine examines the network traffic within the ship's communication network and detects suspicious or malicious activities by employing various techniques and underlying algorithms. It analyzes the network traffic patterns, protocols, and payload contents to identify potential threats or attacks. Once a suspicious activity is detected, the Detection Engine raises an alert and informs the Monitoring Controller about the potential security breach. Additionally, when the Detection Engine detects a fault or failure on the bridge device, it notifies the Mitigation Engine and the controller to divert the network traffic on a different route. The Mitigation Engine is responsible for initiating appropriate countermeasures to mitigate the impact of faults and/or failures. It collaborates with the controller to divert the network traffic onto a different route, ensuring that critical ship operations continue without disruption. By swiftly responding to faults or failures, the Mitigation Engine helps maintain the ship's communication network's reliability and availability.

Together, the Monitoring Controller, Detection Engine, and Mitigation Engine form integral components of the SDN-based framework, working in tandem to safeguard the ship's communication network against potential threats and ensure uninterrupted operation.

Figure 6 shows these components and the relations between them. Note that each of the three controllers within the controller layer, depicted in Figure 5, can have the Detection Engine and the Mitigation Engine, for more robust overall security.

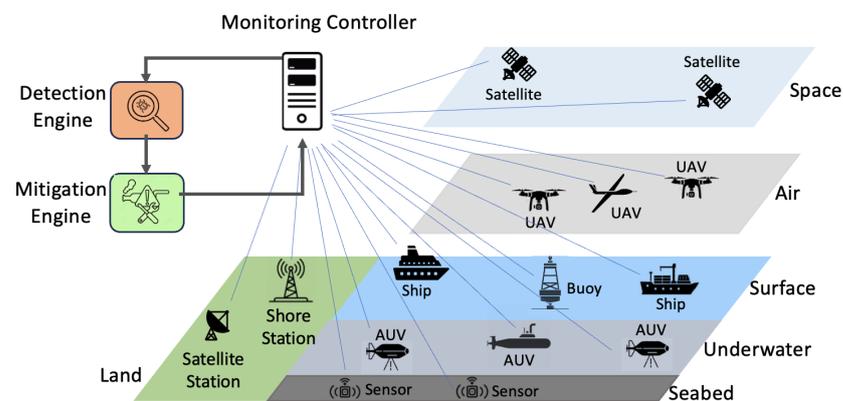


Figure 6. SDN-based framework for attack mitigation.

5.4. A Use Case

Merchants and cruise ships travel far and wide across the vast oceans between places. In the case of Navy vessels, they remain afloat for months at a time and may be required to anchor far offshore. In either case, the communications environment has physical and environmental challenges. More importantly, once away from the shore, the ships have no access to land-based high-bandwidth communications infrastructure. Furthermore, when ships want to pull up to ports in different parts of the world, they are often faced with differing communication standards. For example, countries may choose to operate wireless communications equipment across different spectrum allocations [47]. With dedicated equipment operating on a specific carrier for a given bandwidth, there is no guarantee of compatibility with another system's specifications.

While SATCOM is a viable solution in such scenarios, the cost can be prohibitive, and the latency and signal interference may not be acceptable for time-critical missions. Furthermore, the nature of the satellite constellation can introduce spatial or temporal communication gaps. For instance, a geosynchronous satellite in orbit approximately 35,000 km above the earth has a period of approximately 24 h. This results in the perception

to a user on the earth that the satellite stays relatively fixed at a given point in the sky. As a maritime vessel traverses east or west across the oceans, this point in the sky eventually will appear below the horizon, requiring the vessel to obtain coverage from an additional satellite to communicate.

Additionally, due to the curvature of the earth, geosynchronous satellite coverage above 70 degrees north latitude and below 70 degrees south latitude is greatly diminished [70]. While these issues can be overcome with different solutions such as using a polar or highly elliptical orbit, they bring their own complications, such as tracking and pointing requirements. In particular, Navy operations require connectivity among a diverse set of platforms, including submarines, surface ships, aircraft, and shore sites (see Figure 2). The links among these platforms support a wide range of applications supporting strategic and tactical C4ISR functions. While high bandwidth communications are available on large ships, small ships do not have the ability to leverage this bandwidth by dynamically selecting the most capable link available [59]. Consequently, ships do not efficiently utilize the available bandwidth within the strike group, limiting the ability for smaller ships to effectively gain access to services on the global information grid (GIG) [59]. SDN-SDR-based unified communications infrastructure can be very useful for deployment with the Navy's carrier strike groups (CSGs), which is composed of ships, submarines, aircraft, and personnel to support an extensive range of operations, all of which primarily rely on SATCOMs.

A more robust, low-cost, high-bandwidth, and low-interference communication infrastructure should be considered to address the afore-explained situations, especially for vessel-to-vessel (V2V) and vessel-to-aircraft-carrier (V2C) communications. With regards to a CSG, one possible solution is to fit the vessels in the CSG with an SDN-SDR-based unified communications framework integrated with the existing SATCOM infrastructure. It is important to note that today's satellites indeed leverage SDRs for more flexible and varied applications. In [57], the authors discuss how the SDR-based AIS receiver has been integrated into the AAUSAT3 satellite. The authors note that, due to its versatility, new detection algorithms can be easily deployed on an SDR-based AIS receiver, and they easily adapt to the new AIS transmission channels. As previously mentioned, SDN and SDR provide great flexibility to the network and physical layer functionalities of the communications stack. Several other works, including [71–76], have evaluated the integration of SDR in numerous satellite-based applications. With an SDN-SDR unified communications framework, the ship's crew can prepare for changing RF requirements based on the geographical region and regulations ahead of time by keeping the SDR infrastructure ready with the requisite physical-layer standards with simple software reconfiguration tasks. This will alleviate the burden of carrying several hardware components to meet the communications standards of different regions. In [58], the authors present CrossFlow, a principled approach for application development in SDR networks. CrossFlow provides a flexible and modular cross-layer architecture using the principles of SDR and a mechanism for centralized control using the principles of SDN. Through the convergence of SDN and SDR, CrossFlow works towards providing a target-independent framework for application development in wireless radio networks.

Each vessel in the CSG has a SATCOM link for communication with other vessels and offshore sites and, more importantly, for accessing the services on the GIG. It is important to note that small- and medium-sized ships within the CSG have limited SATCOM bandwidth, typically 256–512 Kbps, which prevents them from accessing large volumes of data. However, they can use the excess bandwidth of the 4–8 Mbps available to the larger ships within the strike group [59]. Figure 7 depicts our proposed SDN-SDR-driven communications between vessels for a representative CSG. Each vessel in the CSG—surface and underwater—is fitted with multiple SDRs and managed by an SDN controller, denoted as SDN-C. Note that the Carrier can have multiple controllers, i.e., SDN-Cs, along with one SDN master controller, denoted as SDN-MC to manage the SDN-Cs. Each vessel in the CSG establishes and maintains an SDN-SDR-driven communications link with the Carrier,

i.e., V2C communication as previously noted. To maintain the V2C link, each vessel's SDN-C communicates with the Carrier's SDN-C using the SDN-SDR unified cross-layer network architecture.

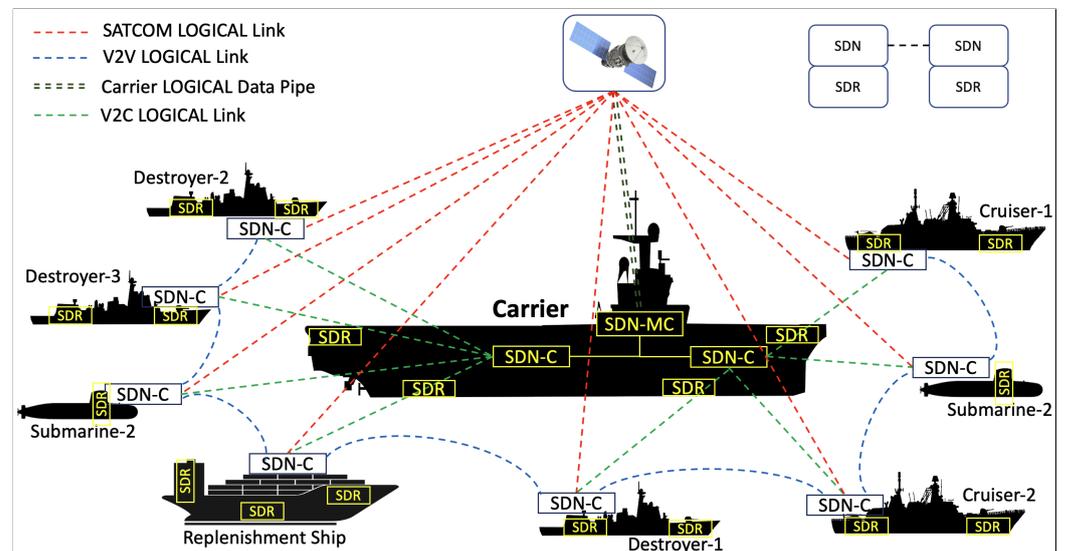


Figure 7. Logical, i.e., network layer (SDN), COMMS with the proposed SDN-SDR cross-layer unified framework.

With multiple SDRs, each vessel has the flexibility to dedicate specific SDRs for specific functions, such as AIS, secure COMMS, etc. While the hardware remains the same, the embedded software is adapted for each application. The Carrier frequency, bandwidth, modulation, and other signal characteristics are specified to meet each communication system's requirements. The use of the same hardware is an advantage in case of an SDR failure. Ready spares can be brought online, i.e., deployed, with the needed software functionality and replaced at sea. In a worst-case scenario, a working SDR for a lower priority system can replace a broken SDR in a critical system. Each Vessel in the CSG has its own SDN-C, which is responsible for managing a specific domain or segment of the network, ensuring optimal performance and handling local network events. However, this teamwork does not stop within one ship, rather it extends to the Carrier itself and reaches out to other vessels in the CSG. The Carrier has its group of SDN-Cs, working together to make sure everything runs smoothly. In order to make sure everyone is in synchronization, the Carrier has a special, global controller called the SDN master controller (SDN-MC). The SDN-MC oversees the entire CSG network infrastructure and acts as a central point of coordination for all vessels in the CSG. The SDN-MC's primary role includes global policy enforcement, network-wide optimization, and traffic engineering. It uses the insights provided by the SDN-C to make strategic decisions that promote efficient resource utilization, load balancing, and overall network resilience. Cooperation between the SDN-C and the SDN-MC is essential for ensuring seamless network operation. The SDN-C continuously provides real-time updates and status reports to the SDN-MC, enabling it to make informed decisions. The SDN-MC, in turn, communicates high-level policies and objectives to the SDN-Cs, ensuring that local decisions align with the global network goals. This collaborative approach allows for dynamic adaptation to changing network conditions, rapid fault detection and recovery, and efficient utilization of network resources.

The SDN-Cs on different vessels within the CSG can talk to each other by vessel-to-vessel (V2V) communication. The Carrier's SDN-Cs stay in touch with the SDN-Cs on the other vessels using vessel-to-carrier (V2C) communication. This connection ensures that everyone is informed and ready to act, no matter where they are. Figure 7 depicts this coordinated effort. This setup boosts the CSG's ability to work as one unit, managing the network, adjusting communications on the fly, and adapting to new challenges in real

time. Therefore, whether it is ship-to-ship or ship-to-carrier, this teamwork of SDN-Cs, guided by the SDN-MC, keeps the CSG connected and responsive, ready to tackle whatever the sea throws their way. In essence, this setup, i.e., the relationship between SDN-Cs and the SDN-MC optimizes network performance by combining the localized expertise of individual controllers with the overarching intelligence and strategic planning of the global controller, i.e., SDN-MC. In addition to the SDN–SDR-driven V2V and V2C, each vessel in the CSG also maintains a SATCOM link for emergencies in the event that the SDN–SDR communication link goes down. Additionally, the Carrier maintains a high bandwidth SATCOM data-pipe to communicate with the GIG and other offshore sites. Having this high-bandwidth data-pipe also enables the Carrier to share its bandwidth with smaller ships in the CSG. In addition to maintaining a communications link with the Carrier, each vessel can also establish and maintain a V2V SDN–SDR communication link with nearby vessels.

5.5. Performance Improvement of SDN–SDR over SATCOM

The exact area occupied by a CSG can vary depending on numerous factors, such as the number and type of ships in the group, the mission of the group, the conditions of the ocean, and the operational orders for spacing, among other things. The US Navy has conducted emergent technology experiments in its annual Trident Warrior exercises [77]. In 2003, the Trident Warrior demonstrated the use of a line-of-sight (LOS) inter-battle-group wireless network to improve both the availability and data rate of the three ships in the experiment compared to SATCOM only [78]. With operations permitting LOS, operating frequencies from ship-to-ship can match the same frequencies used from ship-to-satellite and make use of the same amount of bandwidth, B , as shown in the Shannon–Hartley formula,

$$C = B \cdot \log_2 \left(1 + \frac{S}{N} \right), \quad (1)$$

where C is the data rate in bits per second, S is the received signal power, and N is the received noise power. Among ships in the CSG, the distance will be much less (approximately 20 km) than the distance between the ships and the satellite (approximately 35,000 km), and that is an advantage in the V2V case due to S reducing with the square of distance. In an AIS system, the satellite antenna gain is modeled at 6 dBi, whereas a shipboard dipole antenna may only have a gain of 2 dBi according to the ITU [79]. However, the 4 dBi of advantage to the SATCOM system is erased by distance, d , in the Friis transmission equation,

$$S^{[dB]} = P_t^{[dB]} + G_t^{[dBi]} + G_r^{[dBi]} + 20 \log_{10} \left(\frac{\lambda}{4\pi d} \right), \quad (2)$$

where P_t is the transmitter power, G_t is the transmitter gain, G_r is the receiver gain, and λ is the signal wavelength. The additive noise to the signal, N , is modeled as white Gaussian and is a function of noise temperature and bandwidth.

Based on Equations (1) and (2), the potential data rate with the same carrier frequency is much greater for an LOS V2V system compared to a SATCOM scenario due to the distances involved. However, if ships are operating beyond LOS, lower frequencies, such as in the VHF to HF range, need to be used. Since the maximum operating frequency is lower, the potential bandwidth will be likewise reduced. Additionally, when using an SDN–SDR unified framework, an additional processing delay will be incurred. Processing time in SDN refers to the time required for the SDN controller to manage and make decisions about network traffic and operations. This includes tasks such as analyzing incoming packets, determining routing or forwarding instructions, generating and updating flow rules, enforcing network policies, and responding to changes in network conditions. The processing time in an SDN is closely tied to the control plane activities managed by the controller. Depending on the complexity of the decision-making process and the load on the controller, this can introduce some delay. The control centralization, while beneficial,

can introduce additional delays compared to traditional networks, where devices make decisions independently and in parallel.

There are two types of messages that need to be transmitted between the controller and switches in data planes: Packet-In message (for packets that require controller decision) and FlowMod message (for defining new flow rules). When a packet arrives at a switch or router without a matching flow entry, it triggers a Packet-In message to be sent to the SDN controller. The processing time includes the time the controller takes to make decisions about how to handle the packet. The controller determines and generates flow rules (FlowMod messages) for switches to apply to incoming packets. This includes analyzing network conditions, policies, and the desired behavior.

It should be noted that even in SATCOM, which is the dominant mode of maritime communications, there is still a nodal delay, d_{nodal} . We can model d_{nodal} at the satellite as

$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}, \quad (3)$$

where d_{proc} is processing delay, d_{queue} is queuing delay, d_{trans} is transmission delay, and d_{prop} is propagation delay. When SATCOM is used, we expect d_{prop} to dominate in Equation (3) the other component terms. It should be noted that not every node's nodal delay components in every communication will be computationally significant, but it is important to treat them as non-trivial.

Let us consider the communication needs of Destroyer-1 (see Figure 7), which is a smaller vessel in the CSG with limited bandwidth. With the proposed solution, Destroyer-1 can piggyback on the large bandwidth SATCOM data pipe of the Carrier. When Destroyer-1 needs access to information on the GIG or other on-shore sites, it will contact the Carrier with its request using the proposed SDN-SDR solution (see Figure 7). If the requested information has previously been accessed by the Carrier, then it will be stored locally so that future requests from other vessels in the CSG, such as Destroyer-1, can be satisfied at a fraction of the cost. If, however, Destroyer-1's requested information is not available locally on the Carrier, then the Carrier will request that information using a SATCOM data link, which can support more throughput than the other ships' links due to antenna size and gain advantages, as seen in Equations (1) and (2). This alleviates the burden on Destroyer-1's limited bandwidth SATCOM and potential long delays in accessing critical and time-sensitive information. In [59], the authors note that the typical SATCOM bandwidths found on small ships such as a Destroyer range from 256 to 512 kbps, while large ships such as the Carrier have the capacity for 4–8 Mbps. The cost of the extra-hop of communication from Destroyer-1 to the Carrier is insignificant compared to the cost that will be incurred—directly and indirectly—if Destroyer-1 were to make a direct SATCOM request.

The round trip propagation time when communicating to a 35,000 km altitude geosynchronous satellite with a 25 degree slant angle is approximately 552 ms, i.e., $d_{prop}^{SAT} = 552$ ms. On the other hand, the line of sight communication for ships operating at a range of 25 km (i.e., Destroyer-1 to Carrier physical separation in this example) results in a round-trip propagation time of 0.17 ms, i.e., $d_{prop}^{SDN} = 0.17$ ms. Assuming Destroyer-1 has a SATCOM bandwidth of 512 kbps and the Carrier has a SATCOM bandwidth of 2 Mbps, assuming all the other nodal delay components are the same, the time to process the request for information made directly from Destroyer-1 will be 4x slower compared to a request made via the Carrier. While this would add an additional hop with an added round-trip propagation of 0.17 ms, the overall request would still be processed almost 4x faster. Therefore, with the proposed solution, the additional communication hop between Destroyer-1 and the Carrier is trivial compared to the overall round-trip propagation time. Finally, if the information requested by Destroyer-1 has been saved locally on the Carrier following a previous request, then the entire request can be satisfied without necessitating the use of SATCOM.

6. Conclusions

Maritime industry has a long tradition of continuously adopting and adapting to new technologies. However, the advancements in information and communication technologies have not been adopted as much, primarily due to the restrictions and constraints of the operating environment. In this paper, we have reviewed the current state and different modalities of maritime communications and proposed a novel unified cross-layer SDN–SDR communications framework for the maritime industry. The proposed framework leverages the robust capabilities and baked-in flexibility of SDRs and SDNs. Our proposed framework integrates the existing SATCOM infrastructure for improved and resilient maritime communications in highly dynamic and resource-constrained environments. We have presented the theoretical underpinnings along with a non-trivial example illustrating the expected performance improvement of the proposed framework over purely SATCOM communications in light of a geo-synchronous satellite. Our work, which includes a detailed real-world use-case justifying the motivation for the proposed framework, presents an analytical approach that indicates the feasibility of our overall framework. As an added benefit, with the proposed SDN–SDR framework, the vast amounts of maritime data that are currently going unused can be effectively analyzed and integrated into decision-making processes at all levels of the organization. By creating a more connected, integrated, and efficient maritime industry—from cargo vessels and cruise ships to Navy fleets—digital transformation will have a profound impact on maritime operations.

Our future research will take a two-phase approach. Phase-1 will focus on a simulation-based implementation of the proposed unified SDN–SDR cross-layer communications framework. Among other things, we will take into consideration various environmental factors along with different types of satellites (LEO, MEO, GEO) to empirically validate the robustness of the proposed framework in the highly dynamic and resource-constrained maritime environment. Based on the results and lessons learned, Phase-2 will focus on implementing a working prototype testbed with COTS (commercially off the shelf) SDN and SDR hardware.

Author Contributions: The project’s inception was marked by the collaborative conceptualization efforts of N.N., A.S. and K.S.G. Methodological decisions were collectively shaped by the entire team. N.N., A.S. and K.S.G. were responsible for the articulate writing of the manuscript, ensuring a cohesive presentation of our findings. The critical review and meticulous editing were conducted by N.N. and J.W. J.W. supervision played a pivotal role in guiding the project’s trajectory. Importantly, all authors actively engaged in the review process and collectively endorse the final published version, attesting to our unified dedication to the accuracy and credibility of our research. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported in part by NSF grants CNS 2214940, CPS 2128378, CNS 2107014, CNS 2150152, CNS 1824440, and CNS 1828363.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Alqurashi, F.S.; Trichili, A.; Saeed, N.; Ooi, B.S.; Alouini, M.S. Maritime communications: a survey on enabling technologies, opportunities, and challenges. *IEEE Internet Things J.* **2022**, *10*, 3525–3547. [[CrossRef](#)]
2. Aslam, S.; Michaelides, M.P.; Herodotou, H. Internet of Ships: A Survey on Architectures, Emerging Applications, and Challenges. *IEEE Internet Things J.* **2020**, *7*, 9714–9727. [[CrossRef](#)]
3. Xu, Y. Resource Management of Maritime Edge Nodes for Collected Data Feedback. *IEEE Access* **2020**, *8*, 131511–131521. [[CrossRef](#)]
4. Huo, Y.; Dong, X.; Beatty, S. Cellular communications in ocean waves for maritime Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 9965–9979. [[CrossRef](#)]
5. Wang, J.; Zhou, H.; Li, Y.; Sun, Q.; Wu, Y.; Jin, S.; Quek, T.Q.; Xu, C. Wireless channel models for maritime communications. *IEEE Access* **2018**, *6*, 68070–68088. [[CrossRef](#)]

6. Papa, A.; Kutsevol, P.; Mehmeti, F.; Kellerer, W. Effects of SD-RAN Control Plane Design on User Quality of Service. In Proceedings of the 8th IEEE International Conference on Network Softwarization (NetSoft), Milan, Italy, 27 June 2022–1 July 2022; pp. 312–320. [CrossRef]
7. Bistrovic, M.; Komorčec, D. Methods and Proposals for Solutions in the Applicability of a Software-Defined Radio in Maritime Communication. *J. Mar. Sci. Eng.* **2022**, *10*, 118. [CrossRef]
8. Zhu, C.; Zhang, W.; Chiang, Y.H.; Ye, N.; Du, L.; An, J. Software-Defined Maritime Fog Computing: Architecture, Advantages, and Feasibility. *IEEE Netw.* **2022**, *36*, 26–33. [CrossRef]
9. OECD Work in Support of a Sustainable Ocean. Available online: <https://www.oecd.org/environment/2022-OECD-work-in-support-of-a-sustainable-ocean.pdf> (accessed on 7 July 2023).
10. Ghoshal, S.C.; Hossain, M.M.; Das, B.C.; Roy, P.; Razzaque, M.A. Trade-off Between Latency and Energy for Offloading Tasks in Maritime Internet of Things. In Proceedings of the 4th IEEE International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 17–18 December 2022; pp. 1–6.
11. Wang, J.B.; Zeng, C.; Ding, C.; Zhang, H.; Lin, M.; Wang, J. Unmanned Surface Vessel Assisted Maritime Wireless Communication Toward 6G: Opportunities and Challenges. *IEEE Wirel. Commun.* **2022**, *29*, 72–79. [CrossRef]
12. Difference between Bluetooth and Wi-Fi. Available online: <https://www.geeksforgeeks.org/difference-between-bluetooth-and-wi-fi/> (accessed on 27 June 2023).
13. Alweera, A.; HWMVA, W.; Chandrasiri, R.; De Silva, W.; Gamage, I.; Thilakarathna, T. Location Tracking, Messaging, and Monitoring System for Lightweight Boats Using LoRa Technology ‘Safe Ride’. *Int. J. Eng. Manag. Res.* **2022**, *12*, 62–68.
14. Zhang, X.; Wang, H.; Zhao, H. An SDN framework for UAV backbone network towards knowledge centric networking. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 15–19 April 2018; pp. 456–461.
15. Wu, J. A multi-tiered network with aerial and ground coverage. *Comput. Commun.* **2018**, *131*, 39–42. [CrossRef]
16. Suggala, S.T.; Pothukuchi, S.; Khan, N.A. SDN assisted UAV communication systems: Efficient Deployment Strategies. *arXiv* **2021**, arXiv:2105.10755.
17. Gupta, L.; Jain, R.; Vaszkun, G. Survey of important issues in UAV communication networks. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1123–1152. [CrossRef]
18. Mohsan, S.A.H.; Othman, N.Q.H.; Li, Y.; Alsharif, M.H.; Khan, M.A. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intell. Serv. Robot.* **2023**, *16*, 109–137. [CrossRef] [PubMed]
19. Li, X.; Feng, W.; Wang, J.; Chen, Y.; Ge, N.; Wang, C.X. Enabling 5G on the ocean: A hybrid satellite-UAV-terrestrial network solution. *IEEE Wirel. Commun.* **2020**, *27*, 116–121. [CrossRef]
20. Fang, X.; Feng, W.; Wang, Y.; Chen, Y.; Ge, N.; Ding, Z.; Zhu, H. NOMA-based hybrid satellite-UAV-terrestrial networks for 6G maritime coverage. *IEEE Trans. Wirel. Commun.* **2022**, *22*, 138–152. [CrossRef]
21. Zikou, L.; Papachristos, C.; Tzes, A. The power-over-tether system for powering small UAVs: Tethering-line tension control synthesis. In Proceedings of the 23rd IEEE Mediterranean Conference on Control and Automation (MED), Torremolinos, Spain, 16–19 June 2015; pp. 681–687.
22. Trethowan, J.; Wang, Z.; Wong, K.C. The Viability of a Grid of Autonomous Ground-Tethered UAV Platforms in Agricultural Pest Bird Control. *Machines* **2023**, *11*, 377. [CrossRef]
23. Popov, P.; Mihailov, E.; Dumitrache, L. A new approach to the development of hydrography. In Proceedings of the 9th International Conference EuroGOOS, Brest, France, 3–5 May 2021; pp. 180–185.
24. Alam, M.S.; Hossain, M.F. Reliability and delay in AUV navigation using EM wave based underwater sensor network with shadow fading. In Proceedings of the IEEE International Conference on Telecommunications and Photonics (ICTP), Dhaka, Bangladesh, 26–28 December 2015; pp. 1–5. [CrossRef]
25. Zheng, H.; Wang, N.; Wu, J. Minimizing deep sea data collection delay with autonomous underwater vehicles. *Parallel Distrib. Comput.* **2017**, *104*, 99–113. [CrossRef]
26. Han, G.; Long, X.; Zhu, C.; Guizani, M.; Bi, Y.; Zhang, W. An AUV location prediction-based data collection scheme for underwater wireless sensor networks. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6037–6049. [CrossRef]
27. Liu, Z.; Zhang, Y.; Yu, X.; Yuan, C. Unmanned surface vehicles: An overview of developments and challenges. *Annu. Rev. Control* **2016**, *41*, 71–93. [CrossRef]
28. Zeng, C.; Wang, J.B.; Ding, C.; Lin, M.; Wang, J. MIMO Unmanned Surface Vessels Enabled Maritime Wireless Network Coexisting With Satellite Network: Beamforming and Trajectory Design. *IEEE Trans. Commun.* **2023**, *71*, 83–100. [CrossRef]
29. Plaza-Hernández, M.; Gil-González, A.B.; Rodríguez-González, S.; Prieto-Tejedor, J.; Corchado-Rodríguez, J.M. Integration of IoT technologies in the maritime industry. In Proceedings of the 17th International Conference on Distributed Computing and Artificial Intelligence, Special Sessions, Salamanca, Spain, 6–8 October 2021; Springer: Berlin/Heidelberg, Germany, 2021; pp. 107–115.
30. Jahanbakht, M.; Xiang, W.; Hanzo, L.; Azghadi, M.R. Internet of underwater things and big marine data analytics—a comprehensive survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 904–956. [CrossRef]
31. Wei, T.; Feng, W.; Chen, Y.; Wang, C.X.; Ge, N.; Lu, J. Hybrid satellite-terrestrial communication networks for the maritime Internet of Things: Key technologies, opportunities, and challenges. *IEEE Internet Things J.* **2021**, *8*, 8910–8934. [CrossRef]

32. Chaudhry, S.A.; Irshad, A.; Khan, M.A.; Khan, S.A.; Nosheen, S.; AlZubi, A.A.; Zikria, Y.B. A lightweight authentication scheme for 6G-IoT enabled maritime transport system. *IEEE Trans. Intell. Transp. Syst.* **2021**, *24*, 2401–2410. [[CrossRef](#)]
33. Silverajan, B.; Vistiatio, P. Enabling cybersecurity incident reporting and coordinated handling for maritime sector. In Proceedings of the 14th IEEE Asia Joint Conference on Information Security (AsiaJCIS), Kobe, Japan, 1–2 August 2019; pp. 88–95.
34. Neo, C.M. Soundings Papers: The Rising Threat of Maritime Cyber-Attacks: Level of Maritime Cyber-Security Preparedness along the Straits of Malacca and Singapore | Royal Australian Navy—navy.gov.au. Available online: <https://www.navy.gov.au/media-room/publications/soundings-42> (accessed on 10 May 2023).
35. Balduzzi, M.; Pasta, A.; Wilhoit, K. A security evaluation of AIS automated identification system. In Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, LA, USA, 8–12 December 2014; pp. 436–445.
36. Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. Cybersecurity Challenges in the Maritime Sector. *Network* **2022**, *2*, 123–138. [[CrossRef](#)]
37. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing cyber challenges of maritime navigation. *Mar. Sci. Eng.* **2020**, *8*, 776. [[CrossRef](#)]
38. Global Maritime Security Risks Rise with GNSS Use. *Emerald Expert Briefings*. 2019. Available online: <https://dailybrief.oxan.com/Analysis/DB246110/Global-maritime-security-risks-rise-with-GNSS-use> (accessed on 6 December 2023).
39. Pavur, J.; Moser, D.; Strohmeier, M.; Lenders, V.; Martinovic, I. A tale of sea and sky on the security of maritime VSAT communications. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 18–21 May 2020; pp. 1384–1400.
40. Svilicic, B.; Kamahara, J.; Celic, J.; Bolmsten, J. Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU J. Marit. Aff.* **2019**, *18*, 509–520. [[CrossRef](#)]
41. Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonovic, I.; Bellekens, X. Cyber security in the maritime industry: a systematic survey of recent advances and future trends. *Information* **2022**, *13*, 22. [[CrossRef](#)]
42. Chen, W.; Li, C.; Yu, J.; Zhang, J.; Chang, F. A survey of maritime communications: From the wireless channel measurements and modeling perspective. *Reg. Stud. Mar. Sci.* **2021**, *48*, 102031. [[CrossRef](#)]
43. Status of Conventions. Available online: <https://www.imo.org/en/About/Conventions/Pages/StatusOfConventions.aspx> (accessed on 7 June 2023).
44. Medici, G.M. Modern Maritime Communications. In Proceedings of the 29th World Radiocommunication Seminar, International Telecommunication Union (ITU), Virtual, 30 November–11 December 2020.
45. Krishnan, R.; Babu, R.G.; Kaviya, S.; Kumar, N.P.; Rahul, C.; Raman, S.S. Software defined radio (SDR) foundations, technology tradeoffs: A survey. In Proceedings of the 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 21–22 September 2017; pp. 2677–2682. [[CrossRef](#)]
46. Dillinger, M.; Madani, K.; Alonistioti, N. *Software Defined Radio: Architectures, Systems and Functions*; John Wiley & Sons: Hoboken, NJ, USA, 2005.
47. Gomes, A. 5G and Spectrum: Different Approaches. In Proceedings of the ITU Workshop: 5G and New Technologies, Lomé, Republic of Togo, 9–11 September 2019.
48. International Telecommunication Union. *Recommendation ITU-R (Radio Communication Sector of ITU) M.1371–1374*; Technical Report; International Telecommunication Union (ITU): Geneva, Switzerland, 2010.
49. Oshea, T.J.; Roy, T.; West, N.; Hilburn, B.C. Physical Layer Communications System Design Over-the-Air Using Adversarial Networks. In Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO), Rome, Italy, 3–7 September 2018; pp. 529–532. [[CrossRef](#)]
50. McHale, J. New Communications for Navy Ships Based on Software-Defined Radio. *Military Aerospace*, 1 February 2007.
51. Manaranche, M. Sea Air Space 2021: General Dynamics Introduces New Badger Software-Defined Radio. Available online: <https://www.navalnews.com/event-news/sea-air-space-2021/2021/08/sea-air-space-2021-general-dynamics-introduces-new-badger-software-defined-radio/> (accessed on 7 June 2023).
52. Romero-Godoy, D.; Molina-Padrón, N.; Cabrera, F.; Araña, V.; Jiménez, E. Design and implementation of a prototype with a low-cost SDR platform for the next generation of maritime communications. In Proceedings of the 3rd URSI Atlantic and Asia Pacific Radio Science Meeting (AT-AP-RASC), Gran Canaria, Spain, 30 May–4 June 2022; pp. 1–4. [[CrossRef](#)]
53. Marques, M.M.; Teles, D.C.; Lobo, V.S.; Capela, G. Low-cost AIS Transponder using an SDR device. In Proceedings of the OCEANS 2019 MTS/IEEE SEATTLE, Seattle, WA, USA, 27–31 October 2019; pp. 1–4.
54. Oubbati, O.S.; Atiquzzaman, M.; Ahanger, T.A.; Ibrahim, A. Softwarization of UAV networks: A survey of applications and future trends. *IEEE Access* **2020**, *8*, 98073–98125. [[CrossRef](#)]
55. Yang, T.; Kong, L.; Zhao, N.; Sun, R. Efficient energy and delay tradeoff for vessel communications in SDN based maritime wireless networks. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 3800–3812. [[CrossRef](#)]
56. Biswas, R.; Wu, J. Efficient Switch Migration for Controller Load Balancing in Software Defined Networking. In Proceedings of the 33th IEEE International Teletraffic Congress (ITC-33), Avignon, France, 31 August–3 September 2021; pp. 1–9.
57. Larsen, J.A.; Mortensen, H.P.; Nielsen, J.D. An SDR based AIS receiver for satellites. In Proceedings of the 5th IEEE International Conference on Recent Advances in Space Technologies-RAST2011, Istanbul, Turkey, 9–11 June 2011; pp. 526–531.

58. Shome, P.; Modares, J.; Mastronarde, N.; Sprintson, A. Enabling dynamic reconfigurability of SDRs using SDN principles. In Proceedings of the Ad Hoc Networks: 8th International Conference, ADHOCNETS 2016, Ottawa, ON, Canada, 26–27 September 2016, Revised Selected Papers; Springer: Berlin/Heidelberg, Germany, 2017; pp. 369–381.
59. Deguzman, A.; Ebken, J.; Ho, N.; Lai, R.; Nunez, D.; Raizada, M.; Ross, P.; Tran, N. Network Centric Communications for Expeditionary or Carrier Strike Groups. Ph.D. Thesis, Naval Postgraduate School, Monterey, CA, USA, 2011.
60. Kreutz, D.; Ramos, F.M.V.; Verissimo, P.E.; Rothenberg, C.E.; Azodolmolky, S.; Uhlig, S. Software-Defined Networking: A Comprehensive Survey. *IEEE* **2015**, *103*, 14–76. [[CrossRef](#)]
61. Kushwaha, A.; Bazard, N.; Gumaste, A. IPv6 Flow-Label based Application Aware Routing in SDNs. In Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 10–13 May 2021; pp. 1–6. [[CrossRef](#)]
62. Cui, H.; Zhu, Y.; Yao, Y.; Yufeng, L.; Liu, Y. Design of intelligent capabilities in SDN. In Proceedings of the 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), Aalborg, Denmark, 11–14 May 2014; pp. 1–5. [[CrossRef](#)]
63. Niknami, N.; Wu, J. Enhancing Load Balancing by Intrusion Detection System Chain on SDN Data Plane. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Austin, TX, USA, 3–5 October 2022; pp. 264–272.
64. Du, J.; Song, J.; Ren, Y.; Wang, J. Convergence of broadband and broadcast/multicast in maritime information networks. *Tsinghua Sci. Technol.* **2021**, *26*, 592–607. [[CrossRef](#)]
65. Nazari, S.; Du, P.; Gerla, M.; Hoffmann, C.; Kim, J.H.; Capone, A. Software defined naval network for satellite communications (sdn-sat). In Proceedings of the IEEE Military Communications (MILCOM), Baltimore, MD, USA, 1–3 November 2016; pp. 360–366.
66. Kazmi, S.H.A.; Qamar, F.; Hassan, R.; Nisar, K.; Chowdhry, B.S. Survey on joint paradigm of 5G and SDN emerging mobile technologies: Architecture, security, challenges and research directions. *Wirel. Pers. Commun.* **2023**, *130*, 2753–2800. [[CrossRef](#)]
67. Faujdar, N.; Agrawal, R.; Agarwal, A. Identification of 5G Network Complexity Using SDN. In *Advances in Computational Intelligence and Communication Technology: Proceedings of CICT 2021*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 127–137.
68. Desai, P.R.; Mini, S.; Tosh, D.K. Edge-based Optimal Routing in SDN-enabled Industrial Internet of Things. *IEEE Internet Things J.* **2022**, *9*, 18898–18907. [[CrossRef](#)]
69. Sahay, R.; Meng, W.; Estay, D.S.; Jensen, C.D.; Barfod, M.B. CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships. *Future Gener. Comput. Syst.* **2019**, *100*, 736–750. [[CrossRef](#)]
70. Iridium Satellite Communications. *Satellites 101: LEO vs. GEO*; Iridium Satellite Communications: McLean, VA, USA, 2018.
71. Dascal, V.; Dolea, P.; Cristea, O.; Palade, T. Low-cost SDR-based ground receiving station for LEO satellite operations. In Proceedings of the 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS), Nis, Serbia, 16–19 October 2013; Volume 2, pp. 627–630. [[CrossRef](#)]
72. Lucreti, I.; Di Carlofelice, A.; Tognolatti, P. SDR-based system for satellite ranging measurements. *IEEE Aerosp. Electron. Syst. Mag.* **2016**, *31*, 8–13. [[CrossRef](#)]
73. Maheshwarappa, M.R.; Bowyer, M.D.; Bridges, C.P. A reconfigurable SDR architecture for parallel satellite reception. *IEEE Aerosp. Electron. Syst. Mag.* **2018**, *33*, 40–53. [[CrossRef](#)]
74. Gavrilă, C.; Popescu, V.; Alexandru, M.; Murrioni, M.; Sacchi, C. An SDR-Based Satellite Gateway for Internet of Remote Things (IoRT) Applications. *IEEE Access* **2020**, *8*, 115423–115436. [[CrossRef](#)]
75. Colombo, R.M.; Mahmood, A.; Sisinni, E.; Ferrari, P.; Gidlund, M. Low-cost SDR-based Tool for Evaluating LoRa Satellite Communications. In Proceedings of the IEEE International Symposium on Measurements & Networking (M&N), Padua, Italy, 18–20 July 2022; pp. 1–6. [[CrossRef](#)]
76. Maheshwarappa, M.R.; Bowyer, M.; Bridges, C.P. Software defined radio (SDR) architecture to support multi-satellite communications. In Proceedings of the IEEE Aerospace Conference, Big Sky, MT, USA, 7–14 March 2015; pp. 1–10.
77. CHIPS Articles: NAVWAR Tests New Technologies for Future Fleet at Trident Warrior 2021. Available online: <https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=15323> (accessed on 20 August 2023).
78. Lagana, J.P. FORCEnet: An Analysis of the Trident Warrior 2003 Exercise. Master's Thesis, Naval Postgraduate School, Monterey, CA, USA, 2003.
79. International Telecommunication Union. *Satellite Detection of Automatic Identification System Messages*; International Telecommunication Union Report ITU-R M.2084; International Telecommunication Union (ITU): Geneva, Switzerland, 2006.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.