Journal of *Cybersecurity and Privacy*

MDPI

Communication

Marine Network Protocols and Security Risks

Ky Tran , Sid Keene, Erik Fretheim and Michail Tsikerdekis *

Computer Science Department, Western Washington University, Bellingham, WA 98226, USA; kylemanhtran@gmail.com (K.T.); sid@sidkeene.com (S.K.); frethee@wwu.edu (E.F.)
* Correspondence: Michael.Tsikerdekis@wwu.edu; Tel.: +1-360-650-3968

Abstract: Marine network protocols are domain-specific network protocols that aim to incorporate particular features within the specialized marine context that devices are implemented in. Devices implemented in such vessels involve critical equipment; however, limited research exists for marine network protocol security. In this paper, we provide an analysis of several marine network protocols used in today's vessels and provide a classification of attack risks. Several protocols involve known security limitations, such as Automated Identification System (AIS) and National Marine Electronic Association (NMEA) 0183, while newer protocols, such as OneNet provide more security hardiness. We further identify several challenges and opportunities for future implementations of such protocols.

Keywords: marine; network; security; onenet; nmea2000

Citation: Tran, K.; Keene, S.; Fretheim, E.; Tsikerdekis, M. Marine Network Protocols and Security Risks. *J. Cybersecur. Priv.* **2021**, *1*, 239–251. https://doi.org/10.3390/jcp1020013

Academic Editor: Nour Moustafa

Received: 8 March 2021
Accepted: 9 April 2021
Published: 14 April 2021

1. General Background

Marine network protocols are communication standards that define the rules, syntax, and procedure of synchronization between marine vessels. Seafaring vessel communications have experienced major technological advances within the last century. Early in the twentieth century, radio was implemented to transmit signals in Morse code between vessels. By the 1980s, there were 154 radio operators translating over 20 million words per year [1]. The large demand of manpower and expense for radio communication lead to the increase of satellite broadcasting services by the end of the decade. Companies, such as INMARSAT and COSPAS-SARSAT, have been providing operational communications and safety services for decades with some of the most prominent partners/consumers, such as The U.S. Coast Guard, Boeing, and Comsat [2,3]. Satellite services cover the entire area of communications including voice calling, email and Internet access, navigation and fishing, and tracking vessels. With the variety of services for maritime communication, organizations, such as the National Marine Electronic Association (NMEA), were formed to create a uniform interface standard for digital data exchange between different marine electronic products. NMEA 0183 and NMEA 2000 are the main standards widely accepted by manufacturers and maritime agencies worldwide, and they receive frequent updates, such as NMEA 0183 version 4.11 [4] and NMEA 2000 version 2.000 [5]. However, although much of security research has focused on conventional network protocols (e.g., TCP/IPv6), limited work has been conducted for network marine protocols. Aside from a few security studies [6,7], there is a lack of risk analysis for these types of protocols.

In this communication paper, we highlight the current state of maritime communication and provide an exploratory analysis of security risks. We first highlight the usage and history of marine data transmission. Next, we discuss the requirements for these protocols, such as hardware, software, and manpower. We further identify the mechanisms (built-in or not) used to protect marine network protocols. We introduce our security analysis and identify strengths and weaknesses. The result of this is a classification of security risks associated with each protocol. Finally, we discuss the core challenges and opportunities for marine network protocols.

Marine network protocols are often implemented in software, hardware, or a combination of both. Traditional radio communication utilizes hardware, such as VHF Radios, to

transfer and receive messages. The biggest use of VHF Radio is to send distress signals to coast guards and other vessels within a certain vicinity. In addition, these can be set up as a full-duplex system, which allows both ends to simultaneously communicate with each other. This enables Marine VHF Radios to double up as a telephonic communicator by making calls through a marine operator. In many situations, a radio officer monitors and keeps track of ship communications. With the introduction of modern technology, radio officers have to work not only with radios but also with computers. For example, merchant marines (a civilian fleet of vessels) have radio officers that transmit regular reports about the weather in the oceanic and sea areas where the ship is positioned. When implementing radios, manufacturers must also consider the area of operation of a particular vessel. The Global Maritime Distress and Safety System (GMDSS) divides the world in four sub areas. Depending on where a ship operates, different systems are required to be carried on that ship [8].

In contrast with radio systems, modern day satellite communications generally require both hardware and software. Hardware is used to generate and receive signals relayed by satellites. Many satellite data services also provide internet access, email, and Voice over IP (VoIP) services, which use an interface software, like a secure website that facilitates user interaction. However, similar to radio services, manpower is required to maintain satellite communication. However, an officer is also tasked with maintaining firmware for these technologies.

A single boat can contain multiple devices, such as VHF radio, chart plotter, and depth finder. These may be produced by one or many manufacturers. Information sharing between these tools is guided by standards published by the National Marine Electronics Association. For instance, NMEA 2000 defines the hardware, as well as software, specifications. These include but are not limited to the hardware architecture, data communication between adjacent network nodes, packet routing and shared communication protocols specifications [5].

Figure 1 illustrates a limited number of protocols that may exist on a single marine vessel, as well as how these protocols may interact with other vessels, as well as with coastal services.

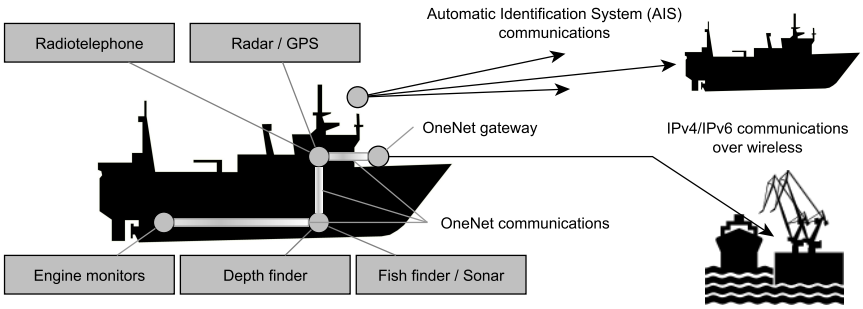

Figure 1. Network protocols utilized by a marine vessel and their interactions with other adjacent vessels or coastal services. National Marine Electronic Association (NMEA) OneNet communications require a gateway that translates packets for IP networks. Automated Identification System (AIS) is broadcasted to other ships via radio frequencies.

2. Security Considerations for Marine Network Protocols

As with other networking protocols, marine network protocols are vulnerable against malicious attacks or unintentional human errors. Manufacturers must consider the extended Confidentiality, Integrity, and Availability (CIA) model that includes also Authentication, Authorization, and Non-repudiation from the creation to implementation and

maintenance of network device firmware. Other studies have conducted similar analyses using this methodology in order to evaluate the efficacy of protocols or products (e.g., Reference [9]). These are also summarized in Table 1.

Table 1. Summary of security considerations.

Security Consideration	Primary Risk
Confidentiality	Access to private data
Integrity	Modification of data
Availability	Inability to access data or resource
Authentication	Inability to confirm identity
Authorization	Improper access to resource or data
Non-repudiation	Inability to confirm an action made by an identity

2.1. Confidentiality

Manufacturers must ensure that only authorized parties are allowed to modify given data. Access control mechanisms and authentication procedures are implemented in the software to control access to resources. Further, encryption protocols are applied to enhance data protection. Additional measures include administrative solutions, such as policies and training, as well as physical controls that prevent people from accessing facilities and equipment. Examples of NMEA training include installation of marine computers, data and ethernet, VHF, physical planning and documentation, and connecting to other data sources, as well as network configuration and troubleshooting [10].

Due to the limitation of bandwidth in many marine network protocols [4,5], encryption mechanisms are not always implemented. As such, the main approach to ensure confidentiality for these systems is primarily through access control.

2.2. Integrity

Ensuring integrity involves protecting information from being modified by unauthorized parties. Similar to confidentiality, access control and validation are common methods that manufacturers utilize to ensure data and communication integrity. Administrative solutions also include policies, separation of duties and training.

In addition, many vessels contain multiple devices that generate communication traffic as mentioned in Section 2. Some of them generate big burst of network traffic which exceeds the bandwidth that a ship can handle. This can lead to disruption and latency as services try to compete for bandwidth. One solution to this challenge was to have a master device and multiple remote devices. When a need for high level of bandwidth is detected, a remote device can be temporarily be assigned to an auxiliary ("spillover") channel to handle the traffic [11].

2.3. Availability

Marine networks must guarantee access of data and services, which under certain conditions they can become critical for the operations and mission of the vessel. The majority of maritime communication protocols support slow transfer speeds [4,5]. As such, protection for availability depends on the hardware specification and configuration to allow data to be transferred at maximum data rate of the protocol. Use of hardware redundancy and backups are necessary for critical systems that require constant accessibility.

For instance, communications between ships and stations are critical, so crew members generally have multiple communication channels, such as Voice over IP (VOIP), marine VHF radios, and satellite services, such as AmosConnect 8 [12].

2.4. Authentication

A further requirement for the firmware is identity verification (i.e., confirm that a receiver or a sender is who they claim to be). While there have been proposals for

authentication mechanisms in the past, very few directly target marine network protocols. However, some of the protocols that ships use support optional authentication mechanisms. These include the Global Navigation Satellite System (GNSS) [13] and systems adopted from vehicular networks [14]. Hence, in theory, these protocols can be adapted to support authentication for marine networks in future revisions.

2.5. Authorization

Many protocols incorporate a form of an ID tag to identify the communication nodes, along with their privileges, as well as access rights, inside a network. However, without a proper method of inspection, a rogue device can generate its own ID with high level of authorization to gain access to sensitive data [15].

2.6. Non-Repudiation

The firmware must verify that the receiver has received a message, and that a receiver is sure about the identity of a sender. Non-repudiation has been increasingly becoming important on other domains of security especially as it relates to forensics and legal challenges [16]. Non-repudiation is bound to become more relevant, even in a high risk environment, such as maritime commercial enterprises. For example, how can a port verify that a vessel operator received a set of instructions in an event where said operator says that no instructions have ever been received?

3. Privacy Considerations for Marine Network Protocols

Even though the focus of this paper is on security considerations, privacy considerations exist for vessels that may prevent some security objectives from being realized. Privacy considerations can vary from identifiability to access to personal data communications [17]. For example, where anonymity is required, anonymous broadcast communications may be necessary even at the expense that these communications can be spoofed or even replayed. Similarly, intrusion detection systems often parse raw and if possible unencrypted data [18]. Access to such systems inevitably leads accessing data that may contain personal communications or otherwise critical communications (e.g., business affairs).

4. Risk Analysis for Current Protocols

There are several marine network protocols in use today that are used in commercial and civilian marine vessels. These include several specialized protocols, as well as generic communication protocols. For the purposes of an examination of the most relevant protocols in use today, we have also obtained the draft of the latest protocol (OneNet) that has been sent by NMEA to manufacturers for the development of the new generation of devices. Additionally, we have included the conventional TCP/IPv6 protocol standard in order to better contrast some of the similarities and differences between conventional and marine network protocols. We itemize a summary of the protocols described below:

- TCP/IPv6: For data transmission via Internet.
- Controller Area Network (CAN) Bus/NMEA 2000: For vehicular and marine data transmission.
- NMEA 0183: For marine data transmission.
- Automated Identification System (AIS): For marine data transmission.
- NMEA OneNet: For marine data transmission.

The list does not include some layer 2 and layer 3 protocols that have been implemented as communication technologies used for automation, such as autonomous navigation, collision avoidance, and early warning. Other protocol examples include 4G, ANT, and Bluetooth. 4G was not originally designed to be used in the maritime industry, but it can be used on boats. It is most commonly paired with a signal booster to make longer range calls. ANT has been used by Garmin in their GNX™ Wireless Wind Pack. Ant is designed and marketed by ANT wireless which is owned by Garmin [19]. Similar to ANT,

Bluetooth is used for low power communication with a short range. Even though Bluetooth is not designed specifically for the maritime industry, it is used on boats (e.g., wireless speakers). Protocols that were not included in the study were omitted for either being too ubiquitous (i.e., they were used in a broader array of settings) or their use was limited.

While these protocols continue to evolve, some are more vulnerable to attacks. We performed a theoretical analysis that contrasts these protocols against common attacks to demonstrate the current security state of these communication protocols. Our goal was to find deficiencies in the protocols that will allow for an attacker to exploit them. For example, protocols that lack authentication could be potentially vulnerability to spoofing attacks. The list of attacks are not meant to be comprehensive but rather representative of the most serious offenses that can be performed in such networks. As such, these attacks formed the basis of our research inquiry. Attacks include:

- Denial of Service (DoS): Targets the availability of data.
- Spoofing: Targets the integrity of data.
- Packet sniffing: Targets the confidentiality of data.
- Replay/Man-in-the-Middle (MITM): Targets both confidentiality and integrity of data.

Table 2 summarizes how each protocols hold up against these attacks. The values within each cell represent our own estimate based on our analysis of these protocols and their corresponding security risks. The relative scale (low, medium, and high) is used in order to highlight the differences between these protocols in a easily readable form and similar to other studies that analyzed similar protocols (e.g., Reference [20]). We further present our security analysis for these protocols and elaborate more on the table in the following subsections.

Table 2. Summary of marine network protocols and their respective security risk level.

	DoS	**Spoofing**	**Packet Sniffing**	**Relay/Man in the Middle**
TCP/IPv6	Medium	Medium	Medium	High
CAN Bus/NMEA 2000	High	High	High	High
NMEA 0183	High	High	High	High
AIS	High	High	High	High
OneNet	Medium	High	Low	Low/High

4.1. TCP/IPv6

TCP/IPv6 is a networking protocol designed for large scale internetworking [21]. It combines the network-layer IPv6 protocol with the transport-layer TCP protocol. IPv6 increases the IP address size from 32 bits to 128 bits. IPv6 further supports extensions for authentication, data integrity, and (optional) data confidentiality. Currently, there is no official implementation of IPv6 on marine vessels. However, application of TCP/IPv6 on marine vessels also provides the advantage that networks can interoperate with existing land networks. On the other hand, this introduces security drawbacks.

4.1.1. Denial of Service

TCP/IPv6, by default, does not have any mechanism to protect against DoS attacks [22]. It is only as vulnerable to DoS attacks as the physical layer that it operates on. Typically, the most vulnerable point on a TCP/IPv6 network to DoS attack is servers and the network infrastructure (e.g., routers, switches).

4.1.2. Spoofing

TCP/IPv6 networks are known to be vulnerable to spoofing at the Data-Link layer (second layer in the 7-layer TCP model) [23,24]. Devices do not typically authenticate the

validity of a claimed Media Access Control (MAC) address, so impersonation of an existing MAC address can be easily implemented by an adversary. Additionally, IPv6 addresses can be spoofed although this may lead to routing and packet-switching errors.

Internet Protocol Security (IPSec) can be implemented to prevent eavesdropping on the communication channel and impersonation [25]. IPsec creates a boundary between unprotected and protected interfaces. Network traffic traversing this boundary is subject to access controls specified by the user or administrator responsible for the IPsec configuration. These controls indicate whether packets cross the boundary unimpeded or are discarded. Typical security services are ensured via an Authentication Header or Encapsulating Security Payload. IPSec ensures transparency for higher network layers (i.e., all software runs unaffected of IPSec). However, an infected computer (e.g., remote or local malware infection) can easily spy on the network's MAC and IPv6 addresses.

4.1.3. Packet Sniffing

Packet sniffing is possible at the physical layer with a passive inline tap [26]. Additionally, data fields are fully vulnerable to sniffing. To avoid packet sniffing, IPSec can be implemented for encryption [25].

4.1.4. Replay/Man-in-the-Middle

The protocol is also vulnerable to replay attacks [27], where an active inline device is used to complete the TCP three-way-handshake with the client and server devices, while intercepting (and potentially modifying) the data in-between.

4.2. NMEA 2000

NMEA 2000 is the marine industry open networking standard on all types of vessels and it is used extensively by manufacturers. This standard is based on the Controller Area Network (CAN) Bus protocol.

CAN Bus protocol is an industrial and automotive networking protocol widely adopted in vehicle electronics systems [28] . The protocol utilizes a message-based architecture and is capable of operating at either 512 Kbps (high-speed variant) or 128 Kbps (fault-tolerant variant) [14,29]. Each device that transmits CAN Bus signals is considered a node. The lower a node's numeric identifier (ID), the higher the priority for its messages. During transmission, a node continuously checks the signal on the bus and compares it with the signal it is transmitting. If a mismatch occurs, an error is raised (except for during arbitration in which case the node will just stop transmitting). Nodes maintain internal error counters to prevent having broken nodes continuously flood the network with invalidated messages. The right of a node to raise errors can be disabled depending on the value of these counters. This guarantees that communication over CAN Bus is reliable, since, even with broken nodes that raise errors, messages will eventually be successfully transmitted.

By default, NMEA 2000 signaling rate is 250 Kbps at the range of 250 m (0.15 miles). Data messages are transmitted as a series of data frames that incorporate robust error checking, confirmed frame delivery and guaranteed latency times [5]. This standard is primarily intended to support relatively brief data messages.

NMEA 2000 does not incorporate any native security features pertaining to confidentiality, authentication, authorization, or non-repudiation. Controls for these attack vectors are left to be implemented by nodes in their own application-specific protocols operating on top of the marine network protocol. We further elaborate more on the potential vulnerabilities of this protocol based on the representative attacks that we have selected.

4.2.1. Denial of Service

We posit that NMEA 2000 is highly vulnerable to Denial of Service attacks due to its low-bandwidth design. A malicious device (or one that was simply misconfigured) could produce a large amount of traffic on the message channel, preventing other devices from

communicating. It has been highlighted as a dated protocol that is still in use by other studies [30].

4.2.2. Spoofing

Our review of the protocol further identified that NMEA 2000 is vulnerable to spoofing attacks [31], where the Parameter Group Number (PGN) used to identify the sending node is copied and used by a malicious device. This imposes an added problem because in NMEA 2000, the PGN is also used to indicate the priority of the message.

4.2.3. Packet Sniffing

NMEA 2000 operates on a single broadcast domain. All nodes on the message channel (similar to a bus on CAN Bus) receive all messages [32,33]. It is the responsibility of the nodes to discern which messages to discard as unneeded. We suggest that this makes passively sniffing messages a trivial task, assuming physical access is possible.

4.2.4. Replay/Man-in-the-Middle

Because NMEA 2000 operates on a broadcast principle, an inline device could be placed between the target node and the rest of the channel (bus). This malicious inline device would be able to pass along messages from either the target node or the rest of the channel in either direction. We have identified a layer of protection in that NMEA 2000 contains a 15-bit Cyclic Redundancy Check (CRC) [5] (inherited from CAN bus). However, this is designed to detect transmission errors, rather than deliberate tampering as CRC is not considered to be cryptographically secure.

4.3. NMEA 0183

NMEA 0183 is an open source standard, with an optional proprietary data transmission process [4]. It facilitates only one-way communications. Put simply, NMEA 0183 devices are either senders or receivers. NMEA 0183 allows a single sender and several receivers on one circuit.

All data is transmitted in the form of sentences, and it has a specific allowable characters set. Sentences can contain printable ASCII characters, carriage return (\r), and line feed (\n). NMEA 0183 does not use any authentication, encryption, or validation. The lack of security measures makes NMEA 0183 susceptible to any attack if attackers are able to identify the network devices that use this standard.

4.3.1. Denial of Service

We identified that both NMEA 0183 version 3.x and 4.10 support a baud rate of 4800 (9600 bits/s). This makes a DoS attack potentially effective against any devices using this protocol depending on the means through which data is transferred to an application [20].

4.3.2. Spoofing/Packet Sniffing

Spoofing and sniffing has been shown to be trivial against the standard [20]. For example, GPS col can be spoofed with GPS simulation software, such as “LabSat 3 GPS Simulator” or “NMEAsoft GPS Simulator” [34,35].

4.3.3. Replay/Man-in-the-Middle

We further highlight a recent 2018 research study that discovered that some NMEA 0183 systems on board a ship were susceptible to a man-in-the-middle attack [36]. The attack implements a malware that intercepts and manipulates GPS coordinates that are received from a sensor integrator via the network. The malware can also cause a software crash to an operator station (a mission critical device).

4.4. Automated Identification System (AIS)

The Automated Identification System is a tracking system that uses transponders on a ship and is used by vessel traffic services. AIS is used to communicate and broadcast metadata (e.g., name, coordinates, etc.) via a VHF transmitter that is built into the transceiver. This data is often picked up by AIS receivers at ports and other vessels. The information is used for better navigation, collision avoidance, and maritime environment protection. The signals are received by AIS transceivers fitted on other ships or on land-based systems. The received information can be displayed on a screen or chart plotter, showing the other vessels' positions in much the same manner as a radar display. Currently, there are no common security measures used to protect AIS protocol [37]. EAIS is a closely related protocol to AIS. The main differences being that it encrypts its traffic and is not as widely used [38].

4.4.1. Denial of Service

Our analysis shows that with a bit rate of 9600 bits/s, AIS is extremely vulnerable against DoS attacks [39]. For example, timing attacks (a form of DoS) can be performed against AIS. The attacker can hinder availability of AIS stations by sending AIS messages that instruct the victim to delay transmission of messages for a certain time and repeat this process continuously.

4.4.2. Spoofing

We further posit that spoofing attacks for AIS can be rather creative. For example, a spoofing against a ship can be performed by creating a fake "ship" with assigned static information, such as vessel's name, identifier, and type of ship [37].

4.4.3. Packet Sniffing

An additional point that we would like to highlight is that most AIS messages are delivered over port 5321 via UDP without any form of encryption. The protocol is extremely vulnerable against packet sniffing allowing for adversaries to track communications between multiple entities that utilize AIS [37].

4.4.4. Replay/Man-in-the-Middle

We further suggest that a man-in-the-middle attack can be performed either through software or radio frequency. An attacker can eavesdrop on a communication between vessels and replace AIS information. Similarly, for radio frequency, an attacker can override a legitimate AIS signal with a fake one. Regardless of the attack method, the recipient only acquires the modified AIS message from the attacker [37].

4.5. OneNet

The NMEA OneNet standard is an evolutionary step from the NMEA 2000 standard. It is an open industry standard that provides a network infrastructure for marine devices and services over IPv6 to allow all OneNet application protocols to co-exist with other protocols and services that operate in parallel on the same network [40].

A OneNet device uses Multicast Domain Name Server (mDNS) to be discovered on the local network. Multicast DNS is used to resolve host names to IP addresses within small networks that do not include a local name server. Each OneNet application has a unique application ID assigned during production or generated when the application is executed. OneNet Application's meta data (product name, NMEA product code, model, etc.) is stored in JSON format with UTF-8 encoding called Application Information Resource (AIR). A OneNet device can request AIR from other OneNet devices via HTTP GET request; this is used to identify which services are accessible by other devices.

OneNet has a Secure Mode supported by OneNet's Pairing Service—a software which allows authorized devices to exchange data in an encrypted tunnel. To create a secure tunnel, a Human Interface Device (HID) application performs an HTTPS connection to

the Pairing Service in order to pair the device to the Secure Network. Anonymous Diffie-Hellman is used as the cipher suite for the connection. Once the HTTPS connection is established, pairing then proceeds.

OneNet devices have a unique verification process to identify which appplications are OneNet certified. This is done by using Application Information Service (AIS), which is the same service used to exchange AIR, to provide the Certification Information Resource (CIR) which contains Cryptographic Message Syntax (CMS) messages for certification verification.

4.5.1. Denial of Service

Operating through Ethernet network, OneNet devices can obtain transfer speeds up to 10 Gbps [40]. As such, we suggest that, because of the high throughput, OneNet devices have a better resistance against DoS attacks, depending on hardware and software configuration.

4.5.2. Spoofing

In a OneNet network, a Human Interface Device is used to provide to newly connected devices information about network configuration . In particular, the HID communicates to the OneNet Application (running on a device) whether it must have Secure Mode enabled to become operational. In addition, the enabling of Secure Mode is initiated and performed by only the HID. However, in our analysis, we have identified a drawback for this system. Due to this exclusive control that HID has, by spoofing an HID, an attacker can trick an OneNet device to communicate with a fake device through Secure Mode and potentially extract information or even take over the target. Further, switching the device to a separate secure channel means that the device would not be able to communicate with devices on the original secure channel [40].

4.5.3. Packet Sniffing

If OneNet devices are already under "Secure mode," their communications are encrypted and the content cannot be seen by any packet analyzer [38]. However, as we posited before, an attacker can spoof a fake HID and potentially capture certificate information. After this step, the attacker can imitate a legitimate OneNet device and further capture traffic from the existing network.

4.5.4. Replay/Man-in-the-Middle

We have further identified that, because the key exchange process in Anonymous Diffie-Hellman does not perform any key authentication [40], the protocol is susceptible to Man-in-the-Middle attacks, especially if a spoofed HID is involved to intercept the connection. This attack can be successfully especially at the initialization of "Secure Mode".

Our investigation has not identified any potential room for replay attacks on the protocol. An unsigned 32-bit integer called Sequence Number (SQN) is used to prevent replay attacks. The SQN number starts at zero when a message using a secure method called Data Security Security Association (SA). SQN then increments with every message. SQN values for a Data Security SA shall not be reused. If an SQN reaches its maximum value, then the Data Security SA is no longer valid, and a new one must be created.

5. Challenges and Opportunities

Based on the above analysis, we have identified a few core challenges and opportunities in relation to security for marine network protocols. The list is not exhaustive, but it is a natural extension of the steps that need to be taken forward to deal with outdated protocols and involve more individuals from different backgrounds in this domain of research. These items include security for legacy protocols, improvements on hardware layer security, and incorporating network security researchers in protocol development, as well as enveloping these systems under a zero-trust paradigm.

5.1. Incorporating Ad-Hoc Security in Legacy Protocols

An upgrade of existing hardware on existing vessels may be prohibitively expensive. As such, manufacturers need to focus on legacy protocols that are currently in use and provide software updates that would enable encryption, as well as authorization/authentication by default. Our analysis has shown that many marine protocols have no such security protections relying instead on the application layer to provide such features. However, additions to protocols have in the past been demonstrated to work. An example of this is the SSL/TLS implementation that did not need to overwrite the existing network stack and its addition has been effective at reducing confidentiality risks in relation to network communication channels. Similarly, AIS can be replaced by newer protocols that run over VHF, such as the VHF Data Exchange System (VDES) [41].

Similarly with software, one protocol that can be incorporated in existing marine network protocols is the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocol [42], which is a variation on traditional asymmetric cryptography. With TESLA, senders distribute a random key (without revealing it) to their receivers. Next, the sender sends a message with an encrypted Message Authentication Code (MAC). After a certain threshold (time interval or number of messages), the key to decrypt the sender's MAC is revealed. Receivers who have received the sender's previous messages can then verify using the key and MAC. If the verifications are correct and out-of-band packet protection is guaranteed by the transfer protocol, then a receiver knows that the packet is authentic. TESLA's advantages include high scalability and minimal overhead. TESLA is advantageous to use in environment where continuous authenticity over radio or satellite is necessary, while packet loss is expected to be high [43]. Marine communications often can fit this profile.

5.2. Adopting Existing Hardware into Current Protocols

We believe that it is possible to elevate protocol security by incorporating techniques that are in use in other conventional, as well as specialized, protocols (e.g., CAN bus). For example, a suggestion for secure communication over CAN bus is a hardware based secure and trusted framework that uses lightweight Physical Unclonable Function (PUF) based on mutual authentication and secure encryption over an insecure communication channel [14]. PUF is a physical layer application used in hardware security protocols; specifically, "strong PUFs" are used for authentication of mobile and embedded devices. The above framework also encrypts every transmitted message, which ensures confidentiality in the network. Further, PUF hardware is designed to have low power-consumption and without sophisticated cryptographic hardware like secure hash algorithm (SHA) or a public/private key encryption algorithm. Therefore, PUF is simple and scalable to implement. A move towards hardware security can assist in making marine devices more tamper-proof in an environment that cannot be adequately by secured using other physical controls.

5.3. Involving Network and Industry Researchers in Protocol Development

Our analysis has identified that even newer marine network protocols may choose to incorporate algorithms and approaches that have been known to be vulnerable. For example, OneNet utilizes Anonymous Diffie-Hellman for the connection between Applications and the Pairing Service. Instead, a viable alternative is Elliptic Curve Cryptography (ECC), which is considered to be faster and harder to crack than many traditional cryptosystems including Diffie-Hellman. Another example where advances in research can result in faster implementation is with the use of machine learning (also deep learning) solutions in order to prevent DoS attacks [44]. As a valuable strategy that is also suggested in literature [45], we recommend that manufacturers and organizations involve network researchers that can further evaluate the security hardiness of these protocols and play an integral role in their secure development. This can also help bridge the gap between technological advances and industry limitations. One such example is shipping vessels and the the low profit margins that they operate in. The fiduciary duties of decision-makers in such organizations

toward cost minimization may influence decisions for enhanced security measures, and, as such, security professionals have to better understand and articulate the associated risks that may come with such decisions.

5.4. Shift towards Zero-Trust Network Protocol Paradigm

With OneNet protocol [40], we can see that marine network protocols are shifting their design toward enhancing throughput and security. In the past, the protocols were constructed just for data transmission. Most marine communications assume that the network is not compromised as demonstrated by our analysis of the various attack vectors. Instead, the presence of multiple devices on vessels requires us to treat the network and, in effect, the network protocols as organizations that need have an established intrusion detection, as well as incident response strategy in place. We recommend that manufacturers change their networking approach from using proprietary or specialized protocols to incorporating flexible, multi-purpose ones. In addition, increasing the bandwidth and transfer speeds for data enables seafaring vessels to implement security measures that work with on-land networking protocols, such as firewalls, intrusion detection systems, and honeypots. For example, a study has used wireless sensors to establish physical intrusion detection on boats [46]. It is only natural that such physical controls can be extended on the technical aspects of marine systems. Finally, recent advances to improve security in Internet of Things devices moves close to a zero-trust paradigm. One such work attempts to document the device types and communication behaviors of Internet of Things devices connected to a network [47].

6. Conclusions

In this paper, we have described the design of marine network protocols and identified their strengths and weaknesses. We have demonstrated that some protocols that are currently used in commercial and civilian marine vessels are lacking in security. We also identified that OneNet as the latest protocol aims to implement better security and throughput for data transfer between vessels and stations, and within the vessels. However, even the latest technology is far from perfect as it implements some weaker design choices due to the unique environmental limitations. For example, in long sea voyages, availability of an inter-connection is not guaranteed, hence having a certificate authority that verifies certificates across ships can be impossible. Given that malicious attacks are becoming more advanced, marine network protocol designs and implementations must further evolve and uniquely address some of these challenges.

Author Contributions: Conceptualization, E.F. and M.T.; Methodology, E.F. and M.T.; Investigation, K.T., S.K., E.F. and M.T.; Writing—Original Draft Preparation, K.T., S.K., E.F. and M.T.; Writing—Review & Editing, K.T., S.K., E.F. and M.T.; Visualization, M.T.; Supervision, E.F. and M.T. All authors have read and agreed to the published version of the manuscript

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Proc, J. The Story of Portishead Radio: Long Range Maritime Radio Communications: 1920–1995. 2001. Available online: http://jproc.ca/radiostor/portis1.html (accessed on 23 February 2021).
2. National Oceanic And Atmospheric Administrator. *History of the Program*; National Oceanic And Atmospheric Administrator: Washington, DC, USA, 2021.
3. Inmarsat Government. *History of the Program*; Inmarsat Government: Reston, VA, USA, 2021.

4. National Marine Electronics Association. *NMEA 0183–Standard for Interfacing Marine Electronic Devices*; National Marine Electronics Association: Reston, VA, USA, 2002.
5. National Marine Electronic Association. *NMEA 2000® Interface Standard Standard for Serial-Data Networking of Marine Electronic Devices*; National Marine Electronic Association: Reston, VA, USA, 2016.
6. Marine and Coastguard Agency. *Radio: Operational Guidance on the Use of VHF Radio and Automatic Identification Systems (AIS) at Sea*; Marine and Coastguard Agency: 2016. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/442648/MGN_324Corr.pdf (accessed on 12 April 2021).
7. Shoab, M.; Jain, K.; Anulhaq, M.; Shashi, M. Development and implementation of NMEA interpreter for real time GPS data logging. In Proceedings of the 2013 3rd IEEE International Advance Computing Conference (IACC), Ghaziabad, India, 22–23 February 2013; pp. 143–146.
8. Federal Communications Commission. *Global Maritime Distress and Safety System (GMDSS)*; Federal Communications Commission: Washington, DC, USA, 2017.
9. Xu, H.; Heijmans, J.; Visser, J. A Practical Model for Rating Software Security. In Proceedings of the 2013 IEEE Seventh International Conference on Software Security and Reliability Companion, Gaithersburg, MD, USA, 18–20 June 2013; pp. 231–232. [CrossRef]
10. National Marine Electronic Association. *Basic NMEA 2000® Installer Training*; National Marine Electronic Association: Severna Park, MD, USA, 2021.
11. Hester, P.; Highsmith, W. Method and Apparatus for Channel Allocation Integrity in a Communication Network. 1994. Available online: https://patentimages.storage.googleapis.com/pdfs/US5349580.pdf (accessed on 12 April 2021).
12. Jo, Y.H.; Cha, Y.K. A Study on Cyber Security Requirements of Ship Using Threat Modeling. *J. Korea Inst. Inf. Secur. Cryptol.* **2019**, *29*, 657–673.
13. Van Herrewege, A.; Singelee, D.; Verbauwhede, I. CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus. In Proceedings of the ECRYPT Workshop on Lightweight Cryptography, Louvain-la-Neuve, Belgium, 28–29 November 2011; p. 20.
14. Siddiqui, A.S.; Gui, Y.; Plusquellic, J.; Saqib, F. Secure communication over CANBus. In Proceedings of the 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA, USA, 6–9 August 2017; pp. 1264–1267. [CrossRef]
15. Samonas, S.; Coss, D. The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *J. Inf. Syst. Secur.* **2014**, *10*, 21–45.
16. Trivedi, K.S.; Kim, D.S.; Roy, A.; Medhi, D. Dependability and security models. In Proceedings of the 2009 7th International Workshop on Design of Reliable Communication Networks, Washington, DC, USA, 25–28 October 2009; pp. 11–20. [CrossRef]
17. Maple, C. Security and privacy in the internet of things. *J. Cyber Policy* **2017**, *2*, 155–184. [CrossRef]
18. Niksefat, S.; Kaghazgaran, P.; Sadeghiyan, B. Privacy issues in intrusion detection systems: A taxonomy, survey and future directions. *Comput. Sci. Rev.* **2017**, *25*, 69–78. [CrossRef]
19. Garmin. Boat Antennas and Sensors. 2021. Available online: https://buy.garmin.com/en-US/US/on-the-water/antennas_sensors/cOnTheWater-c10538-p1.html (accessed on 7 March 2021).
20. Wullems, C.; Pozzobon, O.; Looi, M.; Kubik, K. Enhancing the Trust of Location Acquisition Systems for Critical Applications and Location-Based Security Services. In Proceedings of the 4th Australian Information Warfare & IT Security Conference, Enhancing Trust, Adelaide, Australia, 20–21 November 2003; pp. 391–406.
21. Deering, S.R. Hinden Internet Protocol, Version6 (IPv6) Specification. *RFC2460* **1998**. Available online: https://www.hjp.at/doc/rfc/rfc2460.html (accessed on 12 April 2021).
22. Nikander, P. Denial-of-service, address ownership, and early authentication in the IPv6 world. In *International Workshop on Security Protocols*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 12–21.
23. Garcia-Martinez, A.; Bagnulo, M. An Integrated Approach to Prevent Address Spoofing in IPv6 Links. *IEEE Commun. Lett.* **2012**, *16*, 1900–1902. [CrossRef]
24. Dawood, H. IPv6 security vulnerabilities. *Int. J. Inf. Secur. Sci.* **2012**, *1*, 100–105.
25. Shue, C.A.; Gupta, M.; Myers, S.A. IPSec: Performance Analysis and Enhancements. In Proceedings of 2007 IEEE International Conference on Communications, Glasgow, Scotland, 24–28 June 2007; pp. 1527–1532. [CrossRef]
26. Schulz, M.; Klapper, P.; Hollick, M.; Tews, E.; Katzenbeisser, S. Trust The Wire, They Always Told Me! On Practical Non-Destructive Wire-Tap Attacks Against Ethernet. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, Darmstadt, Germany, 18–20 July 2016; pp. 43–48. [CrossRef]
27. Anbar, M.; Abdullah, R.; Saad, R.M.; Alomari, E.; Alsaleem, S. Review of security vulnerabilities in the IPv6 neighbor discovery protocol. In *Information Science and Applications (ICISA) 2016*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 603–612.
28. Voss, W. *A Comprehensible Guide to Controller Area Network*; Copperhill Media: Greenfield, MA, USA, 2008.
29. Hou, C.; Jiang, H.; Yang, Y.; Rui, W.; Hu, L. Research on Implementing Real Time Ethernet for Ship Power System. In Proceedings of the 2010 2nd International Workshop on Intelligent Systems and Applications, Wuhan, China, 27 May 2010; pp. 1–4. [CrossRef]

30. Furumoto, K.; Kolehmainen, A.; Silverajan, B.; Takahashi, T.; Inoue, D.; Nakao, K. Toward Automated Smart Ships: Designing Effective Cyber Risk Management. In Proceedings of the 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics), Rhodes, Greece, 2–6 November 2020; pp. 100–105. [CrossRef]
31. Caprolu, M.; Pietro, R.D.; Raponi, S.; Sciancalepore, S.; Tedeschi, P. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. *IEEE Commun. Mag.* **2020**, *58*, 90–96. [CrossRef]
32. Taylor, A.; Japkowicz, N.; Leblanc, S. Frequency-based anomaly detection for the automotive CAN bus. In Proceedings of the 2015 World Congress on Industrial Control Systems Security (WCICSS), London, UK, 14–16 December 2015; pp. 45–49. [CrossRef]
33. Kim, J.; Yim, J.; Kang, Y.; Park, Y. Comparison of COTS inertial sensors for getting marine elevator's platform tilt values. In Proceedings of the 2015 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 28–30 October 2015; pp. 989–992. [CrossRef]
34. LabSat. LabSat 3. 2021. Available online: https://www.labsat.co.uk/index.php/en/products/labsat-3 (accessed on 23 February 2021).
35. NMEAsoft. GPS Simulator. 2021. Available online: http://www.nmeasoft.com/product/gpssimulator/ (accessed on 23 February 2021).
36. Lund, M.S.; Hareide, O.S.; Jøsok, O. An Attack on an Integrated Navigation System. *Necesse* **2018**, *3*, 149–163. [CrossRef]
37. 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.
38. Kessler, G. Protected AIS: A demonstration of capability scheme to provide authentication and message integrity. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2020**, *14*, 279–286. [CrossRef]
39. Stewart, A.; Rice, E.; Safonov, P. Digital Authentication Strategies for the Automated Identification System. Available online: http://micsymposium.org/mics2018/proceedings/MICS_2018_paper_64.pdf (accessed on 12 April 2021).
40. National Marine Electronics Association. *OneNet Standard for IP Networking of Marine Electronic Devices*; National Marine Electronics Association: Reston, VA, USA, 2021. Available online: https://www.nmea.org/content/STANDARDS/OneNet (accessed on 23 February 2021).
41. Lázaro, F.; Raulefs, R.; Wang, W.; Clazzer, F.; Plass, S. VHF Data Exchange System (VDES): An enabling technology for maritime communications. *CEAS Space J.* **2019**, *11*, 55–63. [CrossRef]
42. Ruan, N.; Hori, Y. DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things. In Proceedings of the 2012 International Conference on Selected Topics in Mobile and Wireless Networking, Avignon, France, 2–4 July 2012; pp. 60–65.
43. Perrig, A.; Canetti, R.; Tygar, J.D.; Song, D. Efficient authentication and signing of multicast streams over lossy channels. In Proceedings of the 2000 IEEE Symposium on Security and Privacy (S P 2000), Berkeley, CA, USA, 14–17 May 2000; pp. 56–73. [CrossRef]
44. Catak, F.O.; Mustacoglu, A.F. Distributed denial of service attack detection using autoencoder and deep neural networks. *J. Intell. Fuzzy Syst.* **2019**, *37*, 3969–3979. [CrossRef]
45. Zhang, Z.; Li, X.; Wang, X.; Cheng, H. Decentralized Cyber-Physical Systems: A Paradigm for Cloud-Based Smart Factory of Industry 4.0. In *Cybersecurity for Industry 4.0*; Thames, L.S.D., Ed.; Springer: Cham, Switzerland, 2017; pp. 127–171.
46. Luo, H.; Wu, K.; Guo, Z.; Gu, L.; Yang, Z.; Ni, L.M. SID: Ship Intrusion Detection with Wireless Sensor Networks. In Proceedings of the 2011 31st International Conference on Distributed Computing Systems, Minneapolis, MN, USA, 20–24 June 2011; pp. 879–888. [CrossRef]
47. Watrobski, P.; Klosterman, J.; Barker, W.; Souppaya, M. *Methodology for Characterizing Network Behavior of Internet of Things Devices (Draft)*; Technical Report; NIST: Gaithersburg, MD, USA, 2020.