Exposing Vulnerabilities in NMEA Gateways: Insights from Shodan and Honeypot Experiments

Jeroen Pijpker Marten Struijk Fadi Mohsen

Abstract—**As connectivity increases through the Internet of Things (IoT) and Industry 4.0. Previously isolated systems gained remote access capabilities and became more exposed to cyberattacks. For example, in the maritime domain, the Global Maritime Transportation System (GMTS) is considered a high-potential target. Attacking a GMTS system with malware has been shown to influence ships or disrupt onboard operations. Another significant component of the ship network is an NMEA gateway. Prior research has shown evidence of NMEA gateways being exposed to the Internet, and our previous work experimentally demonstrated four practical attack vectors against such gateways: GPS spoofing, AIS injection, autopilot manipulation, and resource exhaustion. However, it remains unclear whether they have been targeted by adversaries or how an attacker could exploit them.**

In this work, an NMEA gateway honeypot is designed, implemented, and deployed. The design of the honeypot is inspired by using Shodan, which is used to identify real and exposed NMEA gateways. Our Shodan results show that Internet-exposed NMEA gateways are widely spread. For instance, the refined $GPRMC-based Shodan query identified 4,305 unique endpoints that transmitted NMEA messages during the observation period, of which 1,542 were analyzed in detail to identify their vulnerabilities and other parameters, such as the attack window. As per the honeypot, although no attacks against the specific NMEA gateway were captured, the honeypot logs captured other types of attacks, such as automated scanning and reconnaissance efforts. These findings indicate that NMEA gateways could become real targets in the near future if not configured or secured properly.

Index Terms—Industrial Cyber-Physical System; Maritime Cybersecurity; NMEA; Honeypot; ICS Security

I. INTRODUCTION

Industrial control systems (ICS) are everywhere in our modern world. These systems play a crucial role in controlling our infrastructure and processes. They are found in many different industries across many different applications and often serve as the connection between the digital and physical world. A couple of examples include the power grid, nuclear reactors, robots in factories, maritime systems, etc. Historically, ICS systems operated in an isolated environment, which offered a degree of protection from remote cyber threats. However, with the rise of the Internet of Things (IoT) and Industry 4.0, this is no longer the case. Often, remote access and data gathering turn out to be very useful features. In turn, this makes these systems prone to being remotely exploited by malicious parties, especially since they are usually not designed to deal with these kinds of threats. Most of the security patches are 'bolt-on' instead of designing new secure systems from the ground up. Generally, bolt-on security is considered a weaker option to secure a system [1].

Manuscript received May 12, 2026; revised May 15, 2026; accepted June 7, 2026. Published June 15, 2026.
Issue category: Regular
Paper category: Regular
DOI: 10.64552/wipiec.v12i1.128

These systems are now everywhere. With the steady increase in the number and importance of these systems, so have attacks on them. Some examples of the most impactful security incidents include Stuxnet [2], but also the 2015 attack on the Ukrainian power network [3]. Lesser known are the attacks on the Global Maritime Transportation System (GMTS). The GMTS is similarly vulnerable to cyberattacks, and documented incidents indicate that this threat is growing and relatively recent [4], [5]. To create a knowledge base, the Maritime Cyber Attack Database (MCAD) was developed [6] showing a steady increase in maritime systems being attacked/targeted. The scale of the GMTS is illustrated by a merchant fleet consisting of 105,500 vessels above 100 gross tons [7], and it continues to grow. The amount (measured in millions of tons) of goods loaded keeps growing too [8]. With the push of Industry 4.0, ships continue to see more digitization. Whereas ships used to be isolated systems, they often feature connections with the outside world these days.

To protect ICS environments within the GTMS, it's crucial to understand how an attacker performs their attack, and ideally, recognize and respond to it as quickly as possible before any harm is done. This is where honeypots and honeynets become very useful. A honeypot is a deceptive tool that mimics authentic operational systems to attract and engage adversaries [9]. This interaction enables them to gather information about the bad actors' tactics, techniques, and procedures (TTPs). A honeynet is a network of honeypots. Some great progress has been made in the research and development of Industrial honeypots. For example, HoneyICS [10], and HoneyPLC [11].

Honeypots and nets have already been proposed in the context of the GMTS. One proposal explores the concept of an actual 'ship' honeynet, in which the attacker believes he is attacking an actual ship. It concludes that gathering real-world data is a worthwhile effort [12]. Another proposal focuses on port security and deploys a honeypot in that network to detect intruders [13]. However, neither of these works deployed a honeypot in the wild, exposed to the Internet.

In our earlier work, we proposed and experimentally evaluated four concrete attack vectors against NMEA gateways in a controlled environment [14]. The work identified four primary attack vectors: GPS spoofing, AIS injection, autopilot manipulation, and resource exhaustion. This journal article extends that work in several ways: (i) performs an Internet-scale reconnaissance of NMEA data exposure using a refined Shodan query, (ii) quantifies the availability of the possible attack window of Internet-facing NMEA gateways, and(iii) presents the design, implementation, and deployment of a NMEA gateway honeypot to study how real adversaries currently interact with these devices.

The main contributions of this work are as follows:

- Evidence through using Shodan OSINT techniques showing that more than 4300 Internet-facing endpoints expose NMEA data over TCP, and that a subset of those gateways remain reachable for hours after Shodan discovery, resulting in a short but actionable attack window for adversaries.
- Design and deployment of a high-interaction NMEA multiplexer/gateway. The NMEA honeypot realistically emulates a commercially available multiplexer/gateway, including AIS messages and an HTTP configuration web interface.
- Empirical analysis of Internet traffic towards the NMEA gateway honeypot to assess the presence (or absence) of protocol-aware attacks.
- Translation of previously demonstrated NMEA-based attacks into cyber-physical attack scenarios for exposed Internet-facing gateways (GPS/AIS spoofing, autopilot manipulation, and NMEA resource exhaustion), and an assessment that multiple of these attacks are feasible within the measured attack window.
- Mapping of known NMEA-based attack vectors to observed exposure and availability patterns of Internet-exposed NMEA gateways, leading to recommendations on hardening configuration, segmentation, and monitoring before attackers deploy specialized tooling.

The remainder of this paper is structured as follows: In Section II, an overview of relevant background topics is given. In Section III, an overview of related works is provided. Section IV presents the methodology, encompassing the identification of NMEA gateways online. Next, in Section V, the results of the experiments are provided, followed by the discussion in Section VI. The paper is concluded in Section VII.

II. Background

In this section, background information about ship networking protocols and equipment is provided, with a focus on the NMEA standards maintained by the National Marine Electronics Association (NMEA)[15].

A. Ship networking protocols and equipment

Modern ships feature fast networks that span the entire ship. An example of such a network can be seen in Figure 1. The figure shows how ship networks should ideally be, but nowadays, there is, in many cases, a lack of network segmentation [16], [17].

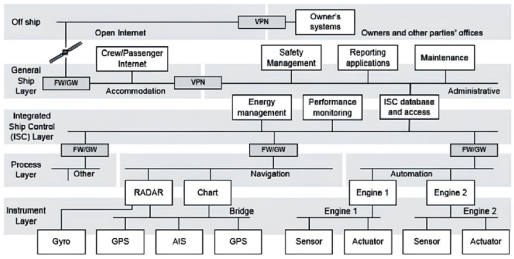

Figure 1 Layered Ship network data network architecture [18].

The different layers found in Figure 1 use different protocols. In the maritime sector, Industrial Control Systems (ICS) are usually used to connect the various technologies onboard. The following protocols and their infrastructure are usually found on ships: Modbus, NMEA 0183, NMEA 2000, and NMEA OneNet. These four technologies are used on most ships to control them and relay information between devices and sensors.

- NMEA 0183 is a serial, one-talker/many-listener standard at a 4,800 baud data bus. The data are in printable ASCII format [19].
- NMEA 2000 is a CAN-based standard for marine electronics, a multi-master bus that supports bidirectional communication and plug-and-play configuration [20].
- NMEA OneNet is an Ethernet and IPv6-based standard that bridges all previous NMEA networks [21].

Each of these protocols has its unique equipment and uses different hardware. A popular choice that is sometimes seen within the Integrated Bridge System (IBS) is to use NMEA over Ethernet [22]. This has the added benefit that no extra cables are required as Ethernet is usually already provided to the systems, but it compromises some of the security separating the layers provides.

Figure 2 Actisense PRO-MUX-2 is a NMEA 0183 Multiplexer designed for marine environments. It enables combining data from up to eight NMEA 0183 talkers and routing them to six listeners, featuring advanced filtering, isolations on all inputs/outputs, and Ethernet configuration capabilities for complex vessel navigation networks. [23]

B. NMEA Gateways

To make communication between the various protocols possible, gateways are introduced. NMEA gateways translate messages between shipboard protocols (such as NMEA 0183 or NMEA 2000) and IP-based networks and are often deployed as multiplexers that bridge multiple serial talkers to TCP or UDP streams. An example of such hardware is shown in Figure 2.

C. NMEA Sentences

The NMEA 0183 sentence starts with either a ’!’ or ’$’. The ’!’ character indicates that the message has a special type of encapsulation. After that, the talker ID follows, and the type of message. The data fields are separated by a ’,’. The number of fields depends on the type of message. After the data fields, an ’*’ follows, which is followed by a checksum based on the previous sentences (excluding the first character). The checksum is computed by XORing all previous bytes. The line ends with ’\r\n’. As an example, the NMEA GPS message that holds the minimal navigational data of the GPS can be seen here:

```
$GPRMC,132233.41,A,5324.6357,N,00611.8764,E,0001.0,26
5.6,280524,0.0,W,A,S*6C
```

An Automatic Identification System (AIS) messages transported via NMEA follow the same high-level grammar but differs in that one of the fields used contains encoded payload data. A typical AIS NMEA sentence is:

```
!AIVDM,1,1,,,1CaL?OhP00PLHAFNSjRh0?v02000,0*25
```

The detailed specification of AIS NMEA encoding is available in the GPSD AIDVM documentation [24].

III. Related Work

In this section, prior research on (maritime) cyber-physical systems is reviewed. The section is structured as follows: cybersecurity of maritime CPS, attacks on ship networks and NMEA-based systems, OSINT-based exposure of maritime OT assets, and honeypots and the maritime context.

A. Cybersecurity of maritime CPS

In the maritime domain, cyber-physical systems refer to the integrated combination of IT (Information Technology) and OT (Operational Technology) systems and the interface with the human operators that collectively enable the monitoring, control, and execution of safety-critical and mission-critical functions of maritime assets [25].

In the work of Tan and Jonos [26], a cyber-physical attack is defined as: A cyber-physical attack can either be a physical attack that adversely affects cyberspace, or an attack that originates in cyberspace and has a physical outcome.

B. Attacks on Ship Networks and NMEA-based Systems

Prior work has demonstrated that exposed NMEA-over-IP gateways provide a technically feasible entry point for compromising maritime CPS. Struijk Pijpker and Mohsen [14] systematically categorized and experimentally validated four attack vectors against an NMEA gateway, namely GPS spoofing, AIS injection, autopilot manipulation, and resource exhaustion through malformed message flooding. These attack scenarios are further organized into three higher-level classes: data spoofing, remote control via data injection, and resource exhaustion. The results of the work provide evidence of protocol-level weaknesses and their potential impact. The experiments are conducted in a controlled environment and do not represent the real world.

Hemminghaus, Bauer, and Padilla created a malware toolkit called Bridge Attack Tool (BRAT). BRAT was designed to compromise systems on board a ship [27]. The tool was able to execute different attacks on ship networks. The attacks primarily affected the availability and integrity of the systems.

The work that is closely related to the NMEA gateway honeypot is HoneyShip [28]. HoneyShip was designed by closely monitoring real-world maritime VSAT systems identified via Shodan, enabling it to emulate an exposed VSAT system on the internet. The honeypot design incorporated detected CVEs, allowing attackers to be closely monitored while interacting with HoneyShip. The dataset collected in this research is publicly available [29]. It includes Shodan and Nmap scans of exposed VSAT systems, and logs from a high-interaction honeypot emulating a Cobham Sea Tel terminal.

C. OSINT-based Exposure of Maritime OT Assets

The work of Amro [30] used Open-Source Intelligence (OSINT) tools to detect maritime components emitting NMEA messages on the internet, identifying 4,942 hosts and 331 possible maritime components. In contrast, our work not only performs an OSINT-based reconnaissance of internet-exposed NMEA gateways but also deploys a NMEA gateway honeypot to observe how Internet-based adversaries currently interact with such a device.

D. Honeypots in the Maritime Context

In the context of maritime systems, multiple papers have been published proposing the use of Honeypots. One of the papers developed a Digital Twin-assisted Honeypot for Cybersecure Smart Seaports. The researchers noted that virtual honeypots must be more realistic to entice attackers, necessitating better high-fidelity. By deploying a digital twin, they created an attractive environment for an attacker. Their solution is called TwinPot, which seems promising for detecting external attacks in smart seaports [13].

In the context of a maritime system exposed to the internet as a honeypot, some work has already been done. McCombie and Pijpker proposed a ship honeynet project that simulates key components of the integrated bridge system to collect data on cyber threats targeting vessels [31]. In another work, Pijpker and McCombie extended this concept with a Ship honeynet explicitly designed to gather structured cyber threat intelligence for vessels.

Brouwer et al. [28] presented HoneyShip, a high-interaction honeypot emulating a maritime VSAT-system to capture attack behavior targeting vessels. The honeypot was deployed on the internet, and the development of HoneyShip was guided by OSINT analysis. The HoneyShip captured thousands of interactions, mainly automated probing and exploitation attempts against known vulnerabilities.

In summary, prior work demonstrated that honeypots and related technologies are effective for studying cyber threats against maritime systems, and that OSINT can reveal exposure of maritime systems on the Internet. Existing studies have focused on VSAT terminals, smart seaports, or conceptual ship honeynets, and NMEA exposure has been analyzed only using OSINT. This work addresses that gap by combining OSINT on NMEA gateways with a NMEA gateway honeypot, enabling empirical observation of how adversaries currently interact with exposed NMEA devices.

IV. Methodology

The study combines active reconnaissance using Shodan for exposed NMEA gateways and the deployment of a custom-

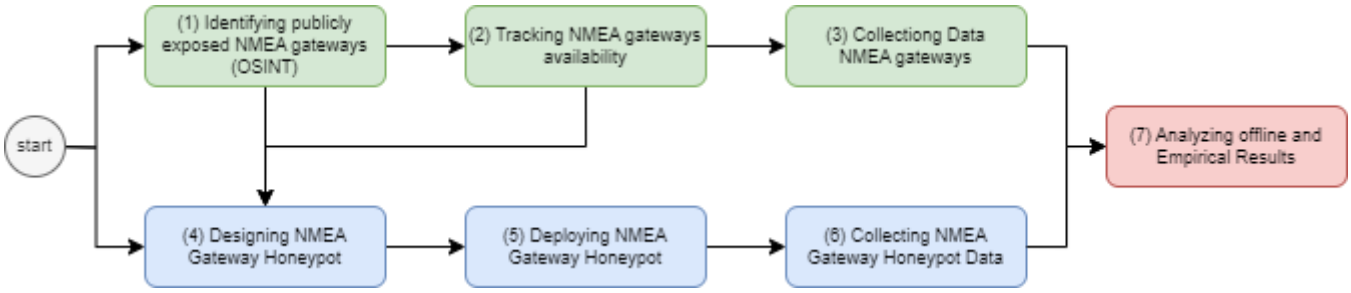

Figure 3 Workflow of the presented study. Publicly exposed NMEA gateways are first identified via OSINT using Shodan, gateway availability is tracked, and data is collected. In parallel, an NMEA gateway honeypot is designed and deployed, and adversary interaction data are collected. The captured datasets are analyzed offline to derive empirical results.

built, high-fidelity NMEA gateway honeypot. The overall workflow, illustrated in Figure 3, consists of two parallel tracks that converge in an offline analysis phase.

Shodan-based Reconnaissance

The green track in Figure 3 identifies, tracks, and collects NMEA gateways that are exposed on the Internet. In previous research, it was shown that many NMEA-exposing connections can be found on Shodan using queries that contain NMEA tags [30]. However, upon manual inspection of the results, many were found to be non-operational, which limits their usefulness to an attacker. To improve the query, this work focuses on a single NMEA sentence starting with $GPRMC, which indicates that a GPS device is emitting minimal navigation data. A Python script issues daily Shodan queries. In total, Shodan was queried 28 times, of which 23 measurements were performed consecutively on a daily basis. To estimate how long these NMEA gateways remain reachable from the Internet, a second Python script performs a daily connectivity check to the reported NMEA gateway ports. By doing this, an estimated attack window before the device goes offline (if it ever does) can be calculated, which in turn tells how useful these devices might be for a potential attacker.

For each endpoint, the date and time of when the queries were done, when Shodan discovered the host for the first time, and every time an attempt to make a connection to the device was made have been recorded. For some of the results, only scans that are on the same day as their update 'timestamp' on Shodan (i.e., new hosts) were taken into account. By doing this we ensure that entries are treated the same regardless of when we performed our query. This allows multiple scans to be done while still being able to build a bigger, overarching dataset as well. The subsequent analysis of the collected data takes temporal factors into account.

A. Honeypot based Experimentation

The blue track in Figure 3 covers the development, deployment, and operation of the NMEA gateway honeypot. The high-fidelity honeypot is designed to emulate an Actisense PRO-MUX-2 multiplexer that bridges multiple serial talkers to IP-based listeners in a realistic shipboard setting. The implementation was built using Java Spring Boot and exposes two services: an HTTP configuration dashboard on port 80 and an NMEA-over-TCP service on port 60001, both services reflecting the look and feel and basic workflow of the real device.

To provide plausible navigation dynamics to an attacker, NMEA traffic is generated from publicly available AIS vessel data sources, converted into GPS and AIS sentences (e.g., $GPRMC, $AIVDM), and replayed at a realistic update interval, with minor disruptions. In Figure 4, the AIS-based message generation is shown.

In our previous work, four practical attack vectors against Internet-exposed NMEA gateways were experimentally evaluated in a controlled environment [14]. These attacks included GPS spoofing, AIS injection, autopilot manipulation, and resource exhaustion. These attacks from our earlier work helped validation of the NMEA gateway honeypot used in this work. Spoofing-based attacks exploit the lack of authentication in the Gateways' NMEA stream by injecting GPS or AIS sentences that override legitimate sensor data, for example, in the ECDIS system. Control-Oriented Attacks target NMEA messages that directly influence actuators, such as autopilot waypoints or heading commands, and inject crafted sentences to steer the vessel. By manipulating these control NMEA messages, an attacker can attempt to alter the course and rudder angle and potentially redirect the ship without the crew's awareness. Resource exhaustion attack targets the communication pipeline. NMEA 0183 over serial connections has limited throughput, and the NMEA gateways have limited buffering capacity. By sending high-frequency or malformed messages over TCP, attackers can flood the system, resulting in dropped messages or delayed transmission of critical data.

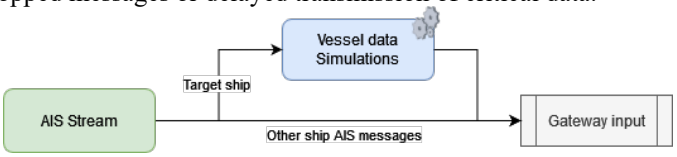

Figure 4 AIS-based message generation. The AIS Stream provides data from the target vessel. For the selected vessel, the AIS data helps to generate believable NMEA messages.

In the implementation of the NMEA Honeypot, several NMEA messages were implemented. This is partly based on the messages in the VDR recording of the work from Calvi and Hakefjord [32].

For validation purposes, the NMEA gateway honeypot was first evaluated in a controlled test environment. The following attacks were executed: brute-forcing the administrator's web interface, passively spying on NMEA traffic, and injecting specially crafted NMEA messages as outlined in the related work section. The honeypot successfully recorded all relevant interaction traces, enabling these attacks to be clearly observed during subsequent analysis. Checkpot [33] was used to verify that the NMEA gateway honeypot was operating as intended. It is a honeypot checker utility developed to help security researchers verify that their honeypots are properly set up to attract high-quality traffic [34].

The NMEA Gateway was deployed on a publicly reachable host with a fixed IP address and is left accessible for a period that overlaps with the Shodan tracking phase. The honeypot is not actively advertised; discovery is left to internet-wide scanning and opportunistic probes. The configuration is hardened to prevent misuse.

All the interactions with the NMEA Gateway Honeypot are collected for offline analysis. The NMEA gateway honeypot collected valid HTTP requests to the HTTP server, along with their payloads. This information is sufficient to determine what an attacker explores on the website and to distinguish between a human and a bot. The NMEA gateway honeypot logged all connections, disconnections, and messages received. The connection details include the source IP and source port. The disconnect event contained the same information, along with the duration of how long the connection was alive. After the Shodan measurement and NMEA gateway honeypot deployment phases, all collected data is analyzed offline to derive empirical results.

Finally, the results from both tracks are interpreted: exposure metrics and attack window estimate from the Shodan analysis provide context for the honeypot interactions, while the honeypot traffic reveals how Internet clients behave towards a realistic NMEA gateway honeypot.

V. Results

This section will describe the empirical results of the research conducted. The results are divided into two different sections. The results of the Shodan analysis can be found in section V-A, and the results of the honeypot deployment in section V-B.

A. Shodan Results

This section presents the empirical results of the OSINT-based identification of tracking-exposed NMEA gateways using Shodan, following the workflow shown in the first track of Figure 3.

Using the refined minimal required navigation data query *$GPRMC*, multiple Internet-facing hosts sending NMEA sentences over TCP were identified during the observation period. In total, the specially formatted *$GPRMC* Shodan query identified 4,305 unique Internet-facing endpoints that transmitted NMEA, confirming that NMEA data streams are widely exposed on the public Internet. Not all of these endpoints are equally suitable for availability and attack window analysis. Due to Shodan's query limitations, it was not feasible to re-scan all 4,305 IP addresses within a single day. Of the gathered IPs, 1,542 were eligible for analysis in the subset.

For each host in the subset of 1,542, an attempt is made to establish a TCP connection, and the received stream is inspected for GPS and potential AIS NMEA sentences. All connected devices have a valid GPS NMEA tag. AIS NMEA messages were only found on one instance. Identifying AIS NMEA messages can help a potential attacker determine whether the target is a real maritime device rather than a decoy.

The Attack window analysis only uses the results that were found within 24 hours of publication on Shodan. This limited the dataset used for this analysis to 1,542 unique hosts. This ensured that all data points are treated equally and have a common starting point. Every 24 hours, a host is re-scanned to see if it is still available. All hosts have an equal amount of times scanned (or more). Availability is at about 40% within the first two hours of Shodan discovery. Figure 5 also shows that the availability drops rapidly below 25% within a couple of days, and the number of hosts that still accept connections has dropped close to 0%.

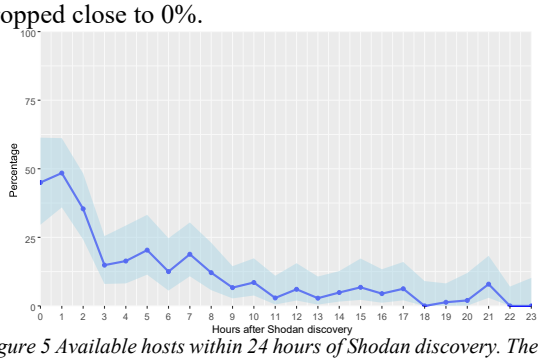

Figure 5 Available hosts within 24 hours of Shodan discovery. The graph shows that the availability of hosts is around 40% within two hours after Shodan has published the result. After two hours there is already a drop to 25% at it declines until almost zero within 24 hours.

B. Honeypot Deployment Results Analysis

Over a period of time, the honeypots were deployed on different platforms. One instance was deployed on a Raspberry Pi and the other instances on a VPS. Combined, the honeypot attracted 2,548 unique IPs to the exposed HTTP dashboard of the NMEA gateway on running on port 80 and 305 unique IPs on the NMEA TCP gateway port 60001. The list of malicious IP addresses that connected to the honeypot is used to compute the abuse confidence score. The abuse confidence

score was calculated based on how many other users observed the IP behaving maliciously. A score of 0 means that the host has not been reported (yet, or at least not frequently). A score of 100 means the host is a well-known malicious IP and has carried out attacks on others as well. In Figure 6 the abuse score result is combined for both honeypots.

The NMEA gateway has seen fewer interactions than the HTTP dashboard from the exposed honeypot. This is to be expected, since most scrapers probably won't target ports 7000 and 51000, as they are not used by many (common) services. Combined for the VPS and RPi, the NMEA gateway has 305 unique IPs connected to it.

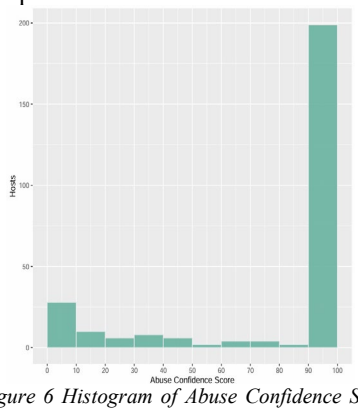

Figure 6 Histogram of Abuse Confidence Score of ALL collected IPs by the honeypots

During the deployment period, no direct, maritime-specific attacks were observed targeting the NMEA protocol. The incoming traffic primarily consisted of automated scanners and reconnaissance attempts. The potential attacks demonstrated in our previous work [14] were not observed during the deployment phase.

In Table 1, the connections are divided into buckets of certain durations for analysis. From this table, it can be observed that some connecting clients to the Gateway had connection durations exceeding 2 hours. This could indicate that a connected client is conducting a manual inspection.

Table 1 Connection duration buckets

Connection duration	Freq
less than 1 second	194
1-5 seconds	145
5-10 seconds	108
10-20 seconds	46
20-60 seconds	52
1-5 minutes	9
5-10 minutes	4
10-20 minutes	3
20-40 minutes	0
40-60 minutes	3
1-2 hours	3
2+ hours	11

Table 2 shows the connections that were manually inspected to check if they performed any activity on the gateway due to a 2h+ connection time. It shows that one IP in particular had quite a few connections open. The origins of the IP are quite diverse.

Table 2 Connections open longer than 2 hours IPs

Source	2h+ conn	Max duration (min)	Country	Abuse Confidence Score
141.98.11.55	1	193.00	LT	100
164.52.25.205	7	787.00	JP	100
206.168.34.35	1	1261.00	US	100
45.156.129.57	1	187.00	BE	100
87.236.176.215	1	148.00	GB	100

VI. Discussion

The Shodan-based analysis phase demonstrated that a significant number of (maritime) devices connected to the Internet expose NMEA streams of different types. This confirms the observation by Amro [30] and extends it by quantifying availability and the attack window.

The use of the Abuse Confidence Score helped our research to filter out 'noise' instead of treating every connection to the honeypot as a possible attack.

The results from Shodan show that the exposure is substantial, but attackers have not yet systematically weaponized NMEA-aware tooling against NMEA gateways. Shodan results should be interpreted cautiously. It has not been confirmed in this work that the Shodan results are real NMEA gateways on actual vessels. Some endpoints may also emulate NMEA gateway behavior, as our honeypot does. Confirming the authenticity of the NMEA gateways was not part of this research.

Most of the incoming traffic consisted of automated scanning and reconnaissance, and there was no clear evidence of NMEA-aware spoofing, control-oriented, or resource exhaustion attacks against the emulated NMEA honeypot gateway that we demonstrated in our previous work [14]. This follows the notion of an early-warning phase: exposure of NMEA gateways is substantial, yet attackers have not systematically weaponized protocol-aware tooling against NMEA gateways. The absence of observed maritime-specific attacks should not be interpreted as proof of safety. Instead, it underscores the need to proactively harden NMEA gateways and their surrounding networks before attackers craft specialized attacks against NMEA gateways.

As Table 3 shows, several impactful attacks from our previous work can be executed within the attack window identified in the Shodan phase. Passive spying on NMEA gateway traffic can take only seconds to establish a TCP connection. Once a TCP connection to an NMEA gateway is established, an NMEA resource exhaustion can also be triggered in seconds to flood the NMEA gateway.

Table 3 NMEA Gateway vulnerabilities related to the previous work [14] translated into feasible attacks

Vulnerability (issue)	Attack type	Short description	Minimal execution time (testbed)	Feasible within observed attack windows
No authentication required NMEA TCP Gateway	Spying (passive)	NMEA Gateway port reachable from the Internet. The NMEA Gateway is bidirectionally configured.	Seconds TCP connect and start logging	Yes, even for short availability
As above	Data fabrication: Spoofing (GPS/AIS/Sensor data)	Sending crafted NMEA sentences to the gateway, the adversary can send spoofed data for various instrumental displays.	Few minutes to craft and inject valid NMEA sentences	Yes, from 10 minutes to an hour
As above	Data fabrication: Controlling the ship (autopilot manipulation)	Autopilot messages are used to instruct the vessel to steer to certain waypoints automatically. By inserting forged *$–APB* and *$–APA* messages into the data stream, the autopilot of ship can be instructed to a certain waypoint [22]	Few minutes to craft and inject valid NMEA sentences	Yes, from 10 minutes to an hour
DoS against NMEA gateway	Resource exhaustion (dropping/delaying NMEA Streams)	The TCP NMEA port can be flooded by sending high rate of messages in short time. So legitimate NMEA messages are being dropped or delayed.	Seconds to start a NMEA stream overload/effect almost immediately	Yes, from 10 minutes to an hour
As above	Spoofing/controlling by degrading legitimate traffic	Like OpenCPN only use for example the last messages received.	Seconds to start a NMEA stream overload/effect almost immediately	Yes, from 10 minutes to an hour
Brute force admin panel	Configuration changes (routing changes, disabling inputs/alarms), firmware upload	Not changing the default credentials on the NMEA gateway or using weak credentials.	Seconds to start	Yes, if the admin panel uses default credentials

The observations in this work may be subject to certain threats to validity, particularly regarding the representativeness of Shodan-identified endpoints and the specificity of our NMEA gateway honeypot implementation.

Shodan-based measurements depend on a third-party scanning service whose coverage, timing, and banner classification we cannot control or fully validate, so some endpoints may not be a real shipboard NMEA gateway.

Additionally, the NMEA gateway honeypot represents a single NMEA gateway with simulated AIS-based traffic rather than a fully IBS, so attacker behavior against a richer or truly operational environment may differ from the observation.

Finally, the duration of deployment was limited, which may restrict how far the traffic patterns can be generalized over time.

VII. Conclusion

This work examined Internet-exposed NMEA gateways that can be classified as critical maritime industrial cyber-physical systems. Prior research showed that NMEA messages are exposed online. In this work, we conducted an OSINT-based reconnaissance study using Shodan and developed and deployed an NMEA gateway honeypot that emulates a commercially available device.

The Shodan study showed that data streams of NMEA gateways remain widely exposed on the Internet and confirmed that many endpoints are reachable over TCP within a short but useful attack window.

Our high-fidelity honeypot showed that it is feasible to emulate a realistic NMEA gateway and attract Internet traffic to both the HTTP dashboard and the NMEA TCP service. Although the honeypot logs did not show any clear evidence of specific attacks identified in our previous work [14] against the NMEA gateway, they did reveal excessive automated scanning and reconnaissance attempts.

This work shows that NMEA Gateways are vulnerable due to a combination of weak or absent authentication, legacy protocol design, and direct internet exposure.

For future work, we aim to deploy a more complex Ship network honeynet, preferably with more realistic maritime traffic sources, and an internet connection relevant to maritime operations, for example, StarLink. Overall, the findings underscore the need to harden NMEA gateways and associated shipboard networks before adversaries begin to exploit these maritime assets.

DATA AND SOURCE CODE AVAILABILITY

The datasets generated and analyzed during the study, along with the source code of the NMEA Gateway honeypot, will be made publicly available upon acceptance of this work.

Acknowledgment

The authors used AI-assisted tools to improve the language and clarity of the publication. In particular, Grammarly and similar grammar-checking tools were used for spelling and grammar corrections, and ChatGPT was used to refine wording, suggest alternative formulations, and tighten abstract,

introduction, and discussion sections. All AI-generated suggestions were manually reviewed and edited by the authors, who take full responsibility for the final content.

REFERENCES

[1] S. Shiva, S. Roy, and D. Dasgupta, "Game theory for cyber security," in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 2010, pp. 1–4.

[2] K. E. Hemsley and Dr. R. E. Fisher, "History of Industrial Control System Cyber Incidents," Idaho National Lab. (INL), Idaho Falls, ID (United States), Dec. 2018. doi: 10.2172/1505628.

[3] D. U. Case, "Analysis of the Cyber Attack on the Ukrainian Power Grid." 2016. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

[4] P. Há. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim, "A Retrospective Analysis of Maritime Cyber Security Incidents," *TransNav*, vol. 15, no. 3, pp. 519–530, 2021, doi: 10.12716/1001.15.03.04.

[5] International Shipping News, "Rising Threat of Maritime Cyberattacks," *International Shipping News*, Oct. 2023, [Online]. Available: https://www.hellenicshippingnews.com/rising-threat-of-maritime-cyberattacks/

[6] "Maritime Cyber Attack Database (MCAD) | NHL Stenden university of applied sciences." Accessed: Dec. 12, 2023. [Online]. Available: https://www.nhlstenden.com/en/maritime-cyber-attack-database

[7] United Nations Conference on Trade and Development (UNCTAD), "World Mercant Fleet." 2026. [Online]. Available: https://unctadstat.unctad.org/insights/theme/243

[8] United Nations Conference on Trade and Development (UNCTAD), "World seaborne trade." [Online]. Available: https://unctadstat.unctad.org/insights/theme/244

[9] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems," Aug. 04, 2021, *arXiv*: arXiv:2108.02287. Accessed: Jan. 31, 2024. [Online]. Available: http://arxiv.org/abs/2108.02287

[10] M. Lucchese, F. Lupia, M. Merro, F. Paci, N. Zannone, and A. Furfaro, "HoneyICS: A High-interaction Physics-aware Honeynet for Industrial Control Systems," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, Benevento Italy: ACM, Aug. 2023, pp. 1–10. doi: 10.1145/3600160.3604984.

[11] "HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems | Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security." Accessed: Dec. 12, 2023. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3372297.3423356

[12] J. Pijpker and S. J. McCombie, "A Ship Honeynet to Gather Cyber Threat Intelligence for the Maritime Sector," in *2023 IEEE 48th Conference on Local Computer Networks (LCN)*, Daytona Beach, FL, USA: IEEE, Oct. 2023, pp. 1–6. doi: 10.1109/LCN58197.2023.10223347.

[13] Y. Yigit, O. K. Kinaci, T. Q. Duong, and B. Canberk, "TwinPot: Digital Twin-assisted Honeypot for Cyber-Secure Smart Seaports," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2023, pp. 740–745. doi: 10.1109/ICCWorkshops57953.2023.10283756.

[14] M. Struijk, J. Pijpker, and F. Mohsen, "Demonstrating Practical Attacks on Maritime Cyber-Physical Systems via Exposed NMEA Gateways," in *2025 14th Mediterranean Conference on Embedded Computing (MECO)*, IEEE, 2025, pp. 1–4.

[15] National Marine Electronics Association (NMEA), "National Marine Electronics Association." 2026. [Online]. Available: https://www.nmea.org/

[16] R. Murthy and R. Ghaffari, "Shipboard Networks and Communications Systems," in *Maritime Transportation Systems*, J. Beckman and others, Eds., Pressbooks, 2025. [Online]. Available: https://pressbooks.pub/maritimesecurity11/chapter/shipboard-networks-and-communications-systems-murthy-ghaffari/

[17] A. Ribeiro, "Maritime cyber incidents jump 103%, as CYTUR warns smart ships under fire; urges secure by design overhaul." [Online]. Available: https://industrialcyber.co/reports/maritime-cyber-incidents-jump-103-as-cytur-warns-smart-ships-under-fire-urges-secure-by-design-overhaul/

[18] S. Krile, D. Kezić, and F. Dimc, "NMEA Communication Standard for Shipboard Data Architecture," *Naše more*.

[19] National Marine Electronics Association, "NMEA 0183 Standard." 2025. [Online]. Available: https://www.nmea.org/nmea-0183.html

[20] National Marine Electronics Association, "NMEA 2000 Standard." 2025. [Online]. Available: https://www.nmea.org/nmea-2000.html

[21] Actisense (Active Research Ltd), *NMEA OneNet and Ethernet Networking Guide*. Poole, United Kingdom: Active Research Limited, 2023. [Online]. Available: https://actisense.com/wp-content/uploads/2023/07/NMEA-OneNet-and-Ethernet-Networking-guide-1.pdf

[22] A. Oruc, V. Gkioulos, and S. Katsikas, "Towards a Cyber-Physical Range for the Integrated Navigation System (INS)," *JMSE*, vol. 10, no. 1, p. 107, Jan. 2022, doi: 10.3390/jmse10010107.

[23] Actisense, "Pro-Mux-2." Accessed: Apr. 20, 2024. [Online]. Available: https://actisense.com/products/pro-mux-2/

[24] E. S. Raymond and the G. project, "AIVDM/AIVDO Protocol Decoding." [Online]. Available: https://gpsd.gitlab.io/gpsd/AIVDM.html

[25] I. Progoulakis, P. Rohmeyer, and N. Nikitakos, "Cyber Physical Systems Security for Maritime Assets," *JMSE*, vol. 9, no. 12, p. 1384, Dec. 2021, doi: 10.3390/jmse9121384.

[26] K. Tam and K. Jones, "MaCRA: a model-based framework for maritime cyber-risk assessment," Jan. 2019, doi: 10.1007/s13437-019-00162-2.

[27] C. Hemminghaus, J. Bauer, and E. Padilla, "BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems," *TransNav*, vol. 15, no. 1, pp. 35–44, 2021, doi: 10.12716/1001.15.01.02.

[28] S. Brouwer, J. Pijpker, and F. Mohsen, "HoneyShip: Unveiling Cyber Threats to Maritime VSAT Systems with a High-Interaction Honeypot," in *2025 IEEE 8th International Conference on Industrial Cyber-Physical Systems (ICPS)*, IEEE, May 2025. doi: 10.1109/icps65515.2025.11087909.

[29] S. Brouwer, J. Pijpker, and F. Mohsen, "HoneyShip: Data from a Maritime VSAT Honeypot and Open Internet Reconnaissance." 2025. doi: 10.34894/7SS2RW.

[30] A. Amro, "Cyber-Physical Tracking of IoT devices: A maritime use case," in *Norsk IKT-konferanse for forskning og utdanning*, 2021.

[31] S. J. McCombie and J. Pijpker, "A Ship Honeynet Project to Collect Data on Cyber Threats to the Maritime Sector," presented at the CYBER 2022, The Seventh International Conference on Cyber-Technologies and Cyber-Systems, Nov. 2022, pp. 81–85.

[32] transmitterdan, "VDRplayer." Accessed: Jul. 07, 2024. [Online]. Available: https://github.com/transmitterdan/VDRplayer

[33] V. Florea, "Checkpot: Honeypot Checker." 2018. [Online]. Available: https://github.com/vladalexgit/checkpot

[34] R. Gabrys, D. Silva, and M. Bilinski, "HoneyGAN Pots: A Deep Learning Approach for Generating Honeypots." 2024. [Online]. Available: https://arxiv.org/abs/2407.07292