ORDU
UNIVERSITY

https://dergipark.org.tr/tr/pub/trjmms

Volume: 10 Special Issue: 1 OCTOBER 2024

TURKISH JOURNAL OF **MARITIME** AND **MARINE** SCIENCES

ORDU
UNIVERSITY

ORDU UNIVERSITY
FATSA FACULTY OF MARINE SCIENCES
2003

Volume: 10 Special Issue: 1 OCTOBER 2024

TURKISH JOURNAL OF **MARITIME** AND **MARINE** SCIENCES

e-ISSN: 2564-7016

TURKISH JOURNAL OF MARITIME AND MARINE SCIENCES

The Turkish Journal of Maritime and Marine Sciences is published by Ordu University
On Behalf of Fatsa Faculty of Marine Sciences

Correspondence Address: Ordu University, Fatsa Faculty of Marine Sciences 52400
Fatsa / Ordu, TURKEY

Web site: http://dergipark.gov.tr/trjmms

Tel: +90 (452) 423 50 53
Fax: +90 (452) 423 99 53
E-mail: trjmms@odu.edu.tr
Sort of Publication: Quarterly
Publication Date and Place: 05/10/2024, ORDU, TURKEY
Publishing Kind: Online

MARINE SCIENCES SECTION EDITORS

EDITORIAL BOARD (MARINE SCIENCES)

EDITORIAL BOARD (MARITIME AND MARINE TECHNOLOGY)

TRJMMS ARTICLE SUBMISSION POLICY

1. Turkish Journal of Maritime and Marine Sciences publication language is either Turkish or English, however publications submitted in Turkish should have an English abstract. This Journal is published twice a year.
2. Submitted work shouldn't have been published before (except as oral and poster presentation), the copyright of the work shouldn't have been transferred to anywhere and the work shouldn't be under review in another journal for publication.
3. The type of the submitted work (original research, brief report, technical notes and review) must be indicated.
4. It will not be published elsewhere in English, in Turkish or in any other language, without the written consent of the copyright-holder.
5. It is important for the submission file to be saved in the valid format of the template of word processor used.
6. References of information must be indicated.
7. To avoid unnecessary errors, you are strongly advised to use the 'spell-check' and 'grammar-check' functions of your word processor.
8. Author(s) is/are fully responsible for his/her/their works published in the Journal.
9. A work submitted to the Journal is forwarded to the publishing committee by the editor and evaluated by two or more referees selected by this committee. A work must be approved by the publishing committee and the referees in terms of both scientific content and writing format in order to be accepted for publication. A work rejected for publication is returned to the author(s). A work for which the referee or the editors requested any revisions is sent back to the author(s) for correction according to the given comments and suggestions. Author(s) has/have to convince the publishing committee and the referee(s) about the comments and the suggestions he/she/they disagree(s) with while giving the necessary explanations. Depending on the revision by the author(s) and/or the referee reports for publication, publishing committee decides whether the work is accepted or rejected.
10. A work accepted for publication is sent to the author(s) for the final control before publishing in order to rewrite it according to writing style and format of the Journal. Finally, author(s) approved version of the work is queued for publishing.
11. A person may have two works, as a first author, at most in the same issue.
12. Articles submitted for a possible publication in the journal have been checked with *iThenticate* program to compose similarity report. This report is sent to the editorial board to be checked. If the program detects more than 25 percentage similarity except that the references, the editorial board requests the revisions from the authors. If the necessary changes does not make in 30 days, the article is declined. If the similarity rate is very high, the article is declined, too.
13. Authors are obliged to comply with the TRJMMS Submission Policy.
14. TRJMMS does not charge any article submission or processing charges.

TRJMMS ETHICAL PRINCIPALS AND PUBLICATION POLICIES

- Turkish Journal of Maritime and Marine Sciences (TRJMMS) is an international, refereed, multidisciplinary scientific and technology journal that has been published at least 2 times a year since 2015. Turkish Journal of Maritime and Marine Sciences (TRJMMS) it is committed to provide a platform where highest standards of publication ethics are the key aspect of the editorial and peer-review processes.
- The editorial process for a manuscript to the Turkish Journal of Maritime and Marine Sciences (TRJMMS) consists of a double-blind review, which means that both the reviewer and author identities are concealed from the reviewers, and vice versa, throughout the review process.
- If the manuscript is accepted in the review stage of the Editorial Process then, the submission goes through the editing stage, which consists of the processes of copyediting, language control, reference control, layout and proofreading. Reviewed articles are treated confidentially in Turkish Journal of Maritime and Marine Sciences (TRJMMS).
- **Papers submitted to Turkish Journal of Maritime and Marine Sciences (TRJMMS) are screened for plagiarism with the iThenticate plagiarism detection tool. In case that the editors become aware of alleged or proven scientific misconduct, they can take the necessary steps. The editors have the right to retract an article whether submitted to Turkish Journal of Maritime and Marine Sciences (TRJMMS) or published in Turkish Journal of Maritime and Marine Sciences (TRJMMS).**
- **Following the completion of the editing stage, the manuscript is then scheduled for publication in an issue of the Turkish Journal of Maritime and Marine Sciences (TRJMMS). The articles which are submitted to Turkish Journal of Maritime and Marine Sciences (TRJMMS) to be published are free of article submission, processing and publication charges. The accepted articles are published free-of-charge as online from the journal website. The articles that are accepted to appear in the journal are made freely available to the public via the journal’s website.**
- Turkish Journal of Maritime and Marine Sciences (TRJMMS) has chief editor, section editors and an editorial board. Turkish Journal of Maritime and Marine Sciences (TRJMMS) has an open access policy which means that all contents are freely available without charge to the user or his/her institution. Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the articles, or use them for any other lawful research purposes.
- **Publication ethics of the Turkish Journal of Maritime and Marine Sciences (TRJMMS) are mainly based on the guidelines and recommendations which are published by the Committee on Publication Ethics (COPE), Council of Science Editors (CSE) and Elsevier’s Publishing Ethics for Editors statements. It must be obeyed research and publication ethics in the article submitted by authors.**

The duties and responsibilities of all parties in the publishing process including editors, authors and others are defined below.

The Responsibilities of the Authors

1. Authors are responsible for the scientific, contextual, and linguistic aspects of the articles which are published in the journal. The views expressed or implied in this publication, unless otherwise noted, should not be interpreted as official positions of the Institution.
2. Authors should follow the "Author Guidelines" in Turkish Journal of Maritime and Marine Sciences (TRJMMS)'s web page on DergiPark.
3. Authors should conduct their researches in an ethical and responsible manner and follow all relevant legislation.
4. Authors should take collective responsibility for their work and for the content of their publications.
5. Authors should check their publications carefully at all stages to ensure that methods and findings are reported accurately.
6. Authors must represent the work of others accurately in citations, quotations and references.
7. Authors should carefully check calculations, data presentations, typescripts/submissions and proofs.
8. Authors should present their conclusions and results honestly and without fabrication, falsification or inappropriate data manipulation. Research images should not be modified in a misleading way.
9. Authors should describe their methods to present their findings clearly and unambiguously.
10. Authors accept that the publisher of Turkish Journal of Maritime and Marine Sciences (TRJMMS) holds and retains the copyright of the published articles.
11. Authors are responsible to obtain permission to include images, figures, etc. to appear in the article.
12. In multi-authored publications - unless otherwise stated - author rankings are made according to their contributions.
13. Authors should alert the editor promptly if they discover an error in any submitted.
14. Authors should follow the TRJMMS Article Submission Policy regarding that the submitted work is original and has not been published elsewhere in any language.
15. Authors should work with the editor or publisher to correct their work promptly if errors are discovered after publication.
16. If the work involves chemicals, procedures or equipment that have any unusual hazards inherent in their use, the authors must clearly identify these in the manuscript.
17. If the work involves the use of animals or human participants, the authors should ensure that all procedures were performed in compliance with relevant laws and institutional guidelines and that the appropriate institutional committee(s) has approved them; the manuscript should contain a statement to this effect.
18. Authors should also include a statement in the manuscript that informed consent was obtained for experimentation with human participants. Because the privacy rights of human participants must always be preserved. It is important that authors have an explicit statement explaining that informed consent has been obtained from human participants and the participants' rights have been observed.
19. Authors have the responsibility of responding to the reviewers' comments promptly and cooperatively, in a point-by-point manner.

The Responsibilities of the Reviewers

1. Peer review process has two fundamental purposes as follow: The first purpose is to decide whether the relevant article can be published in Turkish Journal of Maritime and Marine Sciences (TRJMMS) or not and the second purpose is to contribute to the improvement of the weaknesses of the related article before the publication.
2. The peer review process for an article to the Turkish Journal of Maritime and Marine Sciences (TRJMMS) consists of a double-blind review, which means that both the reviewer and author identities are concealed from the reviewers, and vice versa, throughout the review process. Reviewed articles are treated confidentially in Turkish Journal of Maritime and Marine Sciences (TRJMMS).
3. Reviewers must respect the confidentiality of peer review process.
4. Reviewers must refrain from using the knowledge that they have obtained during the peer review process for their own or others' interests.
5. Reviewers should definitely be in contact with the Turkish Journal of Maritime and Marine Sciences (TRJMMS) if they suspect about the identity of the author(s) during the review process and if they think that this knowledge may raise potential competition or conflict of interest.
6. Reviewers should notify the Turkish Journal of Maritime and Marine Sciences (TRJMMS) in case of any suspicion regarding the potential competition or conflict of interest during the review process.
7. Reviewers should accept to review the studies in which they have the required expertise to conduct an appropriate appraisal, they can comply with the confidentiality of the double-blind review system and that they can keep the details about the peer review process in confidential.
8. Reviewers should be in contact with the Turkish Journal of Maritime and Marine Sciences (TRJMMS) in order to demand some missing documents, following the examination of the article, supplementary files and ancillary materials.
9. Reviewers should act with the awareness that they are the most basic determinants of the academic quality of the articles to be published in the journal and they should review the article with the responsibility to increase academic quality.
10. Reviewers should be in contact with the Turkish Journal of Maritime and Marine Sciences (TRJMMS) editors if they detect any irregularities with respect to the Publication Ethics and Responsibilities.
11. Reviewers should review the articles within the time that has been allowed. If they can not review the article within a reasonable time-frame, then they should notify the journal as soon as possible.
12. Reviewers should report their opinions and suggestions in terms of acceptance / revision / rejection for the manuscript in the peer review process through the Referee Review Form which is provided by DergiPark.
13. In case of rejection, reviewers should demonstrate the deficient and defective issues about the manuscript in a clear and concrete manner in the provided Referee Review Form.
14. Review reports should be prepared and submitted in accordance with the format and content of the Referee Review Form which is provided by Turkish Journal of Maritime and Marine Sciences (TRJMMS).
15. Review reports should be fair, objective, original and prudent manner.
16. Review reports should contain constructive criticism and suggestions about the relevant article.

The Responsibilities of the Editors

1. Editors are responsible of enhancing the quality of the journal and supporting the authors in their effort to produce high quality research. Under no conditions do they allow plagiarism or scientific misconduct.
2. Editors ensure that all submissions go through a double-blind review and other editorial procedures. All submissions are subject to a double-blind peer-review process and an editorial decision based on objective judgment.
3. Each submission is assessed by the editor for suitability in the Turkish Journal of Maritime and Marine Sciences (TRJMMS) and then, sent to the at least two expert reviewers.
4. Editors are responsible for seeking reviewers who do not have conflict of interest with the authors. A double-blind review assists the editor in making editorial decisions.
5. Editors ensure that all the submitted studies have passed initial screening, plagiarism check, review and editing. In case the editors become aware of alleged or proven scientific misconduct, they can take the necessary steps. The editors have the right to retract an article. The editors are willing to publish errata, retractions or apologies when needed.

TRJMMS OPEN ACCESS POLICY

TRJMMS is an open access journal. The term open access gives the right of readers to read, download, distribute, copy, print, search, or link to the full texts of the articles free of charge. This is in accordance with the BOAI definition of open access. According to BOAI (Budapest Open Access Initiative); By "open access" to peer-reviewed research literature, its free availability on the public internet, permitting any users to read, download, copy, distribute, print, search, or link to the full texts of these articles, crawl them for indexing, pass them as data to software, or use them for any other lawful purpose, without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. The author(s) and copyright holder(s) grant(s) to all users a free access to articles.

TRJMMS PLAGIARISM POLICY

Plagiarism can take place in two forms:

1. Author(s) deliberately copy someone else's work and claim it as own work.
2. Author(s) copy their own previously published material either in full or in part without providing appropriate references called as "self-plagiarism" or "duplicate publication"

Every manuscript submitted for publication to TRJMMS is checked for plagiarism after submission and before being sent to reviewer for evaluation. "intihal.net" and "iThenticate" are used to detect instances of overlapping and similar text in submitted manuscript. Depending on this report, the articles can be declined or can be submitted to the editor to be evaluated.

TRJMMS ADVERTISEMENT POLICY

1. All advertisements depend on approval of the Publisher or Editor.
2. Scientific content and decisions made by editorial board have not been affected by advertising.
3. Advertisements are separate from the scientific content.
4. Sales and marketing of the products within the accepted advertising are unfeasible.
5. Editor or publisher of the journal is not responsible for advertisement and its content. This responsibility entirely belongs to owner of advertising.
6. Accepted advertisement can be placed on any page approved by the editor or publisher.
7. Advertising is done according to the contract between advertising company and journal management.
8. Advertising content has not included any distinction of language, religion, race, gender, age, disability and etc.
9. Advertising that contrary to society and publication ethics must not be published.
10. Advertising that produced according to national rules and fulfilling their obligations such as license are accepted for publishing.
11. Advertisements must be prepared in accordance with competition laws and other relevant regulations.
12. Journal management shall not be liable for pecuniary loss due to errors of the advertising content.

CONTENT

Research Article
Turkish Journal of Maritime and Marine Sciences

DOI: 10.52998/trjmms.1519901
Volume: 10 Special Issue: 1 (2024) 1-18

Understanding of the Maritime Future Mentality; Safe E-navigation and Safe Maritime Surface Communication

Denizciliğin Geleceği Mantığının Anlayışı; Emniyetli E-Seyir ve Emniyetli Suüstü İletişimi

Türk Denizcilik ve Deniz Bilimleri Dergisi
Cilt: 10 Özel Sayı: 1 (2024) 1-18

Hasan Bora USLUER[1,*]

[1] *Galatasaray University, Maritime Vocational School, Istanbul*

ABSTRACT

Developing and changing technology affects all sectors globally. Although it primarily affects information systems digitally, it affects all sectors indirectly. Maritime transport, the most important transportation mode in the world, is affected by technological progress as seafarers, ships, and ports. When used for its intended purpose, the technology employs intelligent and rational solutions based on the logic of identifying previous errors and developing predictions accordingly. Maritime transportation is the movement of ships between ports safely and without harming the environment. The sea is a dynamic surface not previously exposed to fixed effects and is affected by meteorological and environmental conditions. As the international maritime authorities keep pace with technological advancements, they have embraced the e-navigation concept, a digital revolution that is set to transform the industry. This shift to Electronic Navigation requires all operations to be digital, making transmission easier and more efficient. It also mandates uninterrupted and high-quality digital communication with ships' land facilities during the entire voyage. ECDIS, one of the advanced automation technology products used for e-navigation, and the vector map ENC it uses are of great importance. ENC maps are produced with specific standards. S-100, which is described as the latest and most advanced standard, provides sailors with good opportunities for safe navigation and communication. The study has been prepared to explain e-navigation types of equipment, their standards, and how they communicate according to cyber security.

Keywords: e-Navigation, Maritime Communication, S-100, ECDIS, ENC, Maritime Management.

Article Info
Received: 21 July 2024
Revised: 30 July 2024
Accepted: 05 August 2024

*(corresponding author)
E-mail: hbusluer@gsu.edu.tr

To cite this article: Usluer, H.B. (2024). Understanding of the Maritime Future Mentality; Safe E-navigation and Safe Maritime Surface Communication, *Turkish Journal of Maritime and Marine Sciences*, 10 (Special Issue: 1): 1-18. doi: 10.52998/trjmms.1519901.

ÖZET

Gelişen ve değişen teknoloji küresel anlamda tüm sektörleri etkilemektedir. Öncelikle bilgi sistemlerini dijital olarak etkilese de dolaylı olarak tüm sektörleri etkilemektedir. Dünyanın en önemli ulaşım şekli olan deniz taşımacılığı, denizciler, gemiler ve limanlar gibi teknolojik gelişmelerden de etkilenmektedir. Teknoloji, amacına uygun kullanıldığında, geçmişteki hataları tespit edip buna göre tahminler geliştirme mantığına dayalı, akıllı ve akılcı çözümler kullanır. Deniz taşımacılığı, gemilerin limanlar arasında güvenli ve çevreye zarar vermeden taşınmasıdır. Deniz, daha önce sabit etkilere maruz kalmayan, meteorolojik ve çevresel koşullardan etkilenen dinamik bir yüzeydir. Uluslararası denizcilik otoriteleri teknolojik gelişmelere ayak uydururken, sektörü dönüştürecek dijital bir devrim olan e-navigasyon konseptini benimsemektedir. Elektronik Seyir'e geçiş, tüm işlemlerin dijital olmasını gerektirirken,iletimi daha kolay ve daha verimli hale getiriyor. Ayrıca tüm seyir boyunca gemilerin kara tesisleriyle kesintisiz ve yüksek kalitede dijital iletişim kurulmasını da zorunlu kılıyor. E-Seyir için kullanılan ileri otomasyon teknolojisi ürünlerinden biri olan ECDIS ve kullandığı vektör haritası ENC büyük önem taşımaktadır. ENC haritaları belirli standartlarda üretilmektedir. En yeni ve en gelişmiş standart olarak nitelendirilen S-100, denizcilere güvenli seyir ve iletişim konusunda önemli ve etkili faydalarda bulunmaktadır. Çalışma, e-navigasyon ekipmanlarının türlerini, standartlarını ve siber güvenliğe göre nasıl iletişim kurduklarını açıklamak amacıyla hazırlanmıştır.

Anahtar Sözcükler: e-Seyir, Deniz Haberleşme, S-100, ECDIS, ESH, Denizcilik Yönetimi.

1. INTRODUCTION

The primary purpose of e-navigation is to explain the real world in full detail, which is important in its logic, and to ensure safe navigation and management on the bridge. The Main issue is to define the nowcasting, which is potentially better than forecasting. But the first question is how to reach the nowcasting about e-nav and maritime communication. Years of work on navigation and maritime communication have led to a wealth of data in the field of marine and marine sciences. (Usluer, 2022)

This data, which includes sea, oceanography, bathymetry, meteorology, land details, communication routes and instruments, effective ranges, and working mechanisms, presents an opportunity for further exploration and potential collaboration (Figure 1; Figure 2; Table 1). As the marine industry continues to decipher and apply this data in the real world, we invite you to join us on this journey of discovery. S-100 international standards, prepared by IHO and understood to be of great use to maritime companies in the future, draw attention to compatibility and interoperability. When creating and implementing e-navigation strategies, it's crucial to remember their pivotal role in preventing ship-borne pollution.

Figure 1. IHO S-100 Digital Communication. (IHO, 2021)

With safety at sea and navigation as our primary goals, it must address the issue of ship-borne pollution. Numerous techniques have been explored and developed to tackle this pressing issue. With electronic navigation being a key aspect of maritime operations, it's clear that marine sciences, such as hydrographic and oceanographic information, are indispensable. (Joseph *et al.*, 2021) The need for their standardization, particularly through the Common Maritime Data Structure (CMDS) working structure and the S-100, has become increasingly apparent in recent years (Lee *et al.*, 2024). Interoperability involves creating consistent services for users when individual components are technically different and managed by various organizations. The essential element of ensuring compatibility and interoperability of the dataset is standardization through consistent semantic data modeling.

Table 1..Literature General Overview

Author/Authors	Publish Date	Article Information
Xiao *et al.*	2015	AIS
DiRenzo *et al.*	2015	Cyber Security
Ming-Cheng	2016	ECDIS
Hareide *et al.*,	2018	Cyber Security
Liangbin *et al*	2018	AIS
Shapiro *et al.*	2018	Maritime Transportation Risks
Rutkowski	2018	ECDIS
Kaleem Awan and Al Ghamdi	2019	e-Navigation
Svilicic *et al.*	2019	ECDIS
Tam and Jones,	2019	Cyber Security
Androjna *et al.*	2020	Cyber Security
Joseph *et al.*	2021	Maritime Safety
Bolat *et al.*	2022	Cyber Security
Usluer	2022	Marine Science
Arıcan *et al.*	2023	ENC-CATZOC
Algani *et al.*	2024	Maritime Communication
Jios *et al.*	2024	ENC
Kayışoğlu *et al.*	2024	Cyber Security
Lee *et al*	2024	S-100
Uflaz *et.al.*	2024	Cyber Security

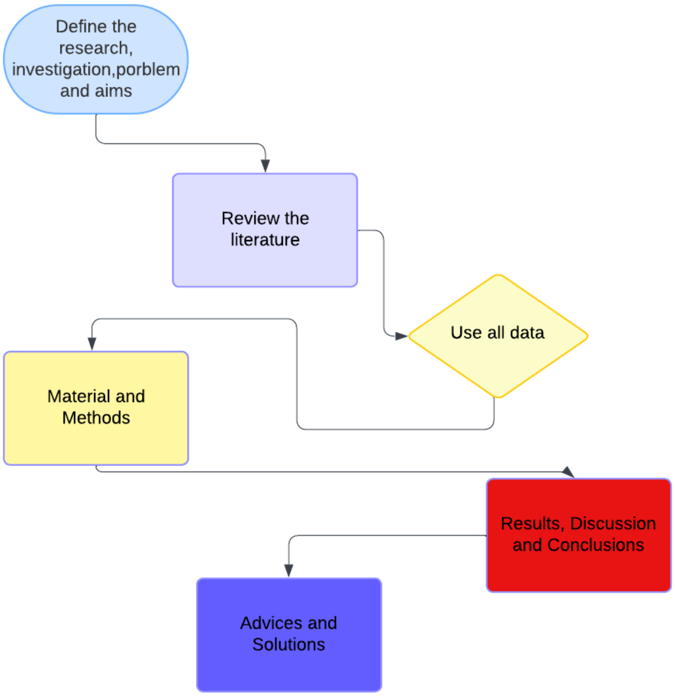

Define the research, investigation,porblem and aims
Review the literature
Use all data
Material and Methods
Results, Discussion and Conclusions
Advices and Solutions

Figure 2. Flowchart of the study

1.1. E-Navigation Overview

The geomatics studies and satellite observations have proven that more than 70% of the world, which does not have a regular shape, is covered with water geography. It is known that more than 80% of the world's population lives near the coastline. It is known that 90% of the transportation activities carried out to meet endless human needs are carried out by maritime transportation. Also, well known that the seas and oceans connect the globe. E-navigation is the safe use of all marine cartographic data sets obtained using the technology resulting from the conversion from analog to digital. It is converting from analog to digital. The first step towards e-navigation was using digital maps for navigational purposes in the early 1990s. At this stage, IHO member countries worked jointly to ensure navigational safety and standards, which are currently ongoing (Figure 3). Due to developing technology, digital maps, and all related systems began to be used on ships with an integrated and compatible automation working method following IMO's founding rules in the early 2000s.

Figure 3. e-nav concept (safety4sea, 2024)

The integrated systems in question are devices such as RADAR, SONAR ECDIS, ENC, AIS; NAVTEX, GYRO, VHF, BNWAS, ECHOSOUNDER, VDR, AUTOPILOT, DPS, and AIS can easily be seen by Figure 4. While e-Navigation was first defined as the technology of tomorrow, it has now become available due to development. Seafarers globally are actively using developing technology devices for safe navigation, which have many strengths.

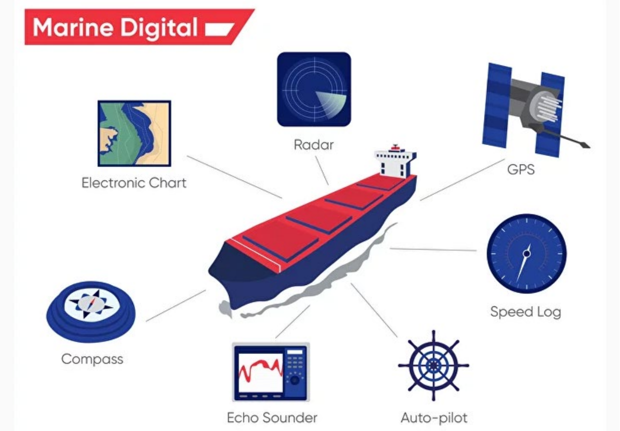


Figure 4. E-Nav systems overview. (Marine-Digital, 2024)

The support of institutions and organizations working for navigational safety, such as IHO and IMO, simplifies the duties of watchkeeping officers during navigation by easily using standardized data, which refers to data that is uniformly formatted and can be easily interpreted by different systems, reducing workloads, increasing safety and environmental performance, and offering real economic advantages to the maritime industry. After a stage, e-navigation has created a fundamental basis for autonomous ships. In this way, connected, digitalized ship systems that operate with high efficiency and safety will be able to operate with constant and standard discipline.

1.2. E-Navigations Equipment's

1.2.1. ECDIS

The universality of device electronic chart display and information system (ECDIS) installations, considered the most important of the e-navigation components, will provide revolutionary solution plans for the era of e-navigation informatics, and intellectualization. (Ming-Cheng, 2016) According to Rutkowski (2018), ECDIS is a useful component that is also a complex, safety system with multiple options for display and integration for working safety navigation (Figure 5). According to the Safety of Life at Sea (SOLAS) convention's regulation V/19, international vessels must carry ECDIS, with some criteria beginning in 2011 (Kayışoğlu *et al.*, 2024).

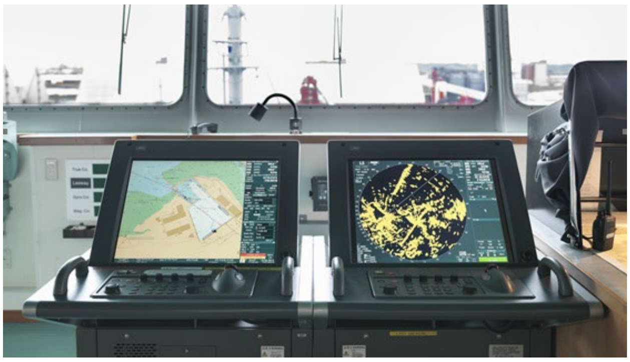


Figure 5. ECDIS system on board. (Safety4sea, 2024)

1.2.2. ENC

Electronic navigation charts, which stand for ENC, are geographic databases compiled in strict accordance with the IHO specifications. ENCs are GIS products that work with ECDIS for safety navigation. (Arıcan *et al*., 2023; Jios *et al.*, 2024)

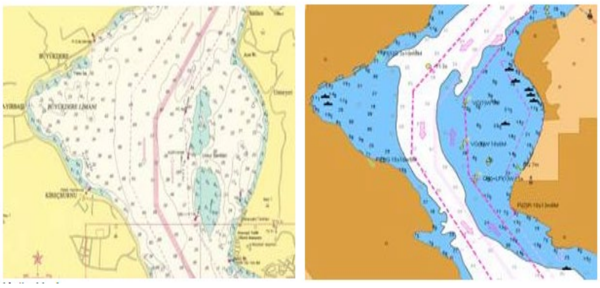


Figure 6. Paper and ENC Charts together. (SHODB, 2024)

Hydrographic organizations produce products that all sailors can understand. This is called standardization. One of the main tasks of IHO is to determine how standard products will be created and to ensure their dissemination. In this context, vector maps were decided to be produced according to certain standards at ENC. According to the vector chart standards S-57, this transition from paper to digital chart marks significant progress and modernization in hydrography (Figure 6). However, it needs to be protected in this state, so the standard called S-63 works to encrypt it. The vector chart produced according to S-57 conditions is encrypted and presented to the user securely (IHO, 2024).

1.2.3. AIS

With navigational safety being the top priority for ships during navigation, the authorities are committed to leveraging devices for this purpose. The Automatic Identification System emerges as a key player in this arena (Figure 7). It provides crucial input parameters in ship traffic simulation models, significantly enhancing risk analysis, especially in the ship's operational area, and thereby preventing potential ship collisions/accidents (Xiao *et al*., 2015; Liangbin *et al*, 2018).

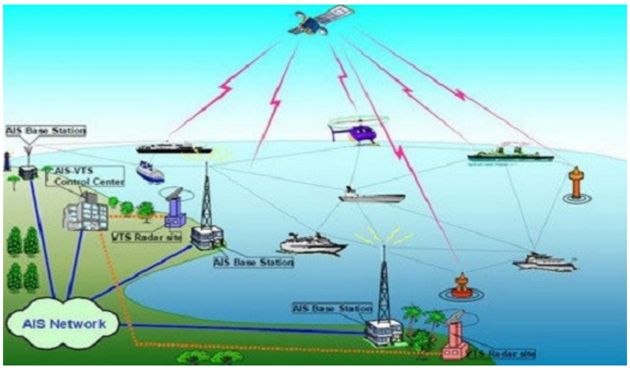
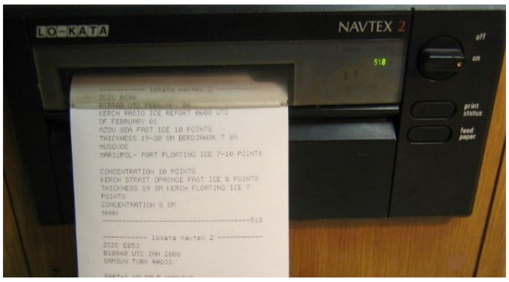


Figure 7.AIS Working cycle. (NATO, 2024)

1.2.4. NAVTEX

At the heart of maritime safety, Navigational Telex is an international communication system that automatically transmits possible danger, safety, and weather reports and warnings to ships on medium frequency. As a crucial part of the International Maritime Organization and the Global Maritime Hazard and Safety System, it works for navigation and seafarer safety, broadcasting free of charge and for the public benefit can easily be seen by Figure 8.



```
----------- lokata navtex 2 -----------
ZCZC BC40
010600 UTC FEBRUARY 06
KERCH RADIO ICE REPORT 0600 UTC
OF FEBRUARY 01
AZOV SEA FAST ICE 10 POINTS
THICKNESS 19-30 SM BERDJANSK 7 SM
MUSOVOE
MARIUPOL- PORT FLOATING ICE 7-10 POINTS

CONCENTRATION 10 POINTS
KERCH STRAIT OPASNOE FAST ICE 8 POINTS
THICKNESS 19 SM KERCH FLOATING ICE 7
POINTS
CONCENTRATION 8 SM
NNNN
-------------------------------------518

----------- lokata navtex 2 -----------
ZCZC EE53
010840 UTC JAN 2006
SAMSUN TURK RADIO
```

Figure 8.NAVTEX is working onboard (Wikipedia, 2024)

1.2.5. RADAR

Another device used for navigational safety is the Radio Detection and Ranging system. The system, known by the abbreviation RADAR, sends radio signals to perform target detection and distance measurement. It is a versatile vessel device that operates with the help of radio signals. It displays the images of the objects within the signal range by reflecting the radio waves broadcast from its antenna off complex objects and returning them to the antenna, leaving a trace on the screen. This versatile device is one of the essential navigational aids on ships, providing the opportunity to detect objects in difficult navigation conditions, such as darkness at night, fog, or rain, show by Figure 9.

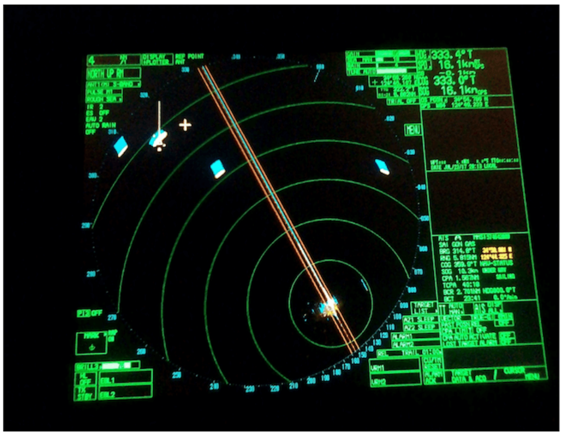


Figure 9. RADAR Screen. (Marineinsight, 2024)

1.2.6. INMARSAT

The International Maritime Satellite Organization and its system provide telephone and data services worldwide, primarily to seafarers and all users who can benefit from this service through terminals established for this purpose (Figure 10). The terminal generally communicates with the satellite and the ground station via the satellite. It provides effective communication services to users who need to communicate over long distances, especially in places without reliable terrestrial networks. Inmarsat also provides free GMDSS services to ships as a public service, demonstrating our commitment to the safety and well-being of the maritime community.

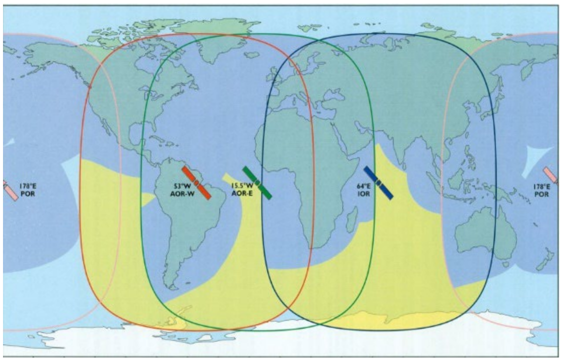


Figure 10. INMARSAT Coverage on Earth (e gmdss, 2024)

1.2.7. VSAT

Marine VSAT (Very Small Aperture Terminal) systems, purposefully designed for maritime use, enhance navigational safety through their adaptable data and voice technology (Figure 11). They facilitate ship tracking over frequencies that determine connection quality and coverage area.

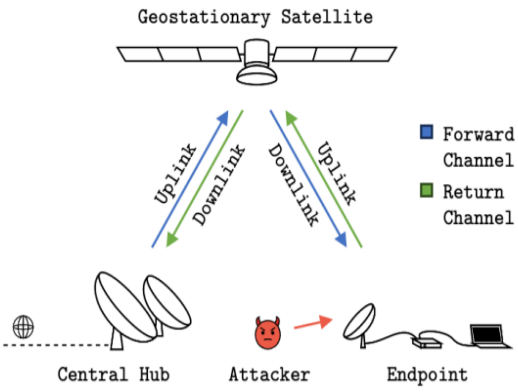


Figure 11. VSAT Communication System working flow (Bisping *et al*., 2024)

Their principle of operation, utilizing C-band, a lower frequency range that requires larger antennas, ensures high-quality satellite Internet communications even in adverse weather conditions, providing reassurance and preparedness for any situation.

1.2.8. GNSS

Global positioning service providers provide latitude-longitude satellite location information that is globally available. To express these correctly, the known and developed positioning systems known as GNSS-Global Navigation Satellite Systems are as follows, GPS-Global Positioning System to the United States, GLONASS – To the Russian Federation, BEIDOU – To China, QZSS – To Japan GALILEO – To the European Union, IRNSS/GAGAN – It is an Indian global positioning system by shown Figure 12.

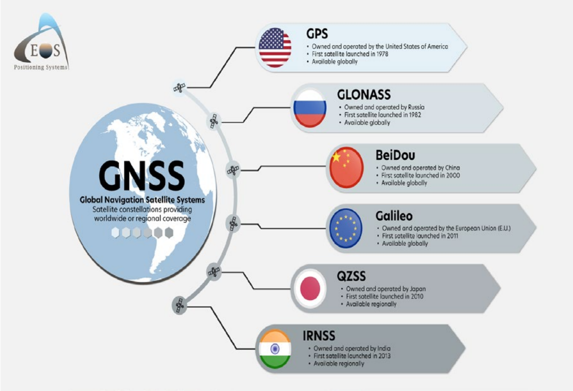

EOS
Positioning Systems
GNSS
Global Navigation Satellite Systems
Satellite constellations providing worldwide or regional coverage
GPS
• Owned and operated by the United States of America
• First satellite launched in 1978
• Available globally
GLONASS
• Owned and operated by Russia
• First satellite launched in 1982
• Available globally
BeiDou
• Owned and operated by China
• First satellite launched in 2000
• Available globally
Galileo
• Owned and operated by the European Union (E.U.)
• First satellite launched in 2011
• Available globally
QZSS
• Owned and operated by Japan
• First satellite launched in 2010
• Available regionally
IRNSS
• Owned and operated by India
• First satellite launched in 2013
• Available regionally

Figure 12. GNSS systems of the world (eos-gnss, 2024)

1.3. S-100 and General Aspects

Institutions and organizations such as the International Maritime Organization work to ensure safe navigation in the world's seas and ensure that all systems and rules are in a clear and understandable structure so that seafarers speaking different languages can understand each other. This understanding is called standardization. S-100, a globally applicable advanced technology product, is a prime example of this understanding. It is a universally understandable data set, designed to provide data from many different data groups in a specific format that all sailors worldwide can understand. Some standards can easily be seen in Table 2 and Figure 13.

This comprehensive framework utilizes data from a wide range of disciplines, including water level information for surface navigation, weather overlay, radio services, aid to navigation information, current information, AIS information, GNSS information, marine traffic management information, underwater keel clearance information, and navigational warnings. It brings together marine protection area information, ensuring that all necessary data is readily available and usable (IHO, 2021).

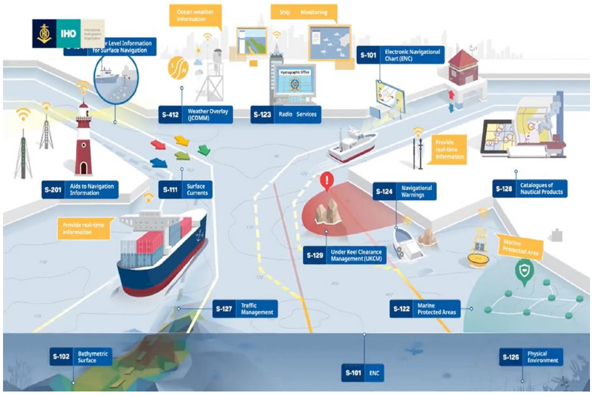

IHO
r Level Information for Surface Navigation
Ocean weather information
Ship Monitoring
Hydrographic Office
S-101 Electronic Navigational Chart (ENC)
S-412 Weather Overlay (JCOMM)
S-123 Radio Services
Provide real-time information
S-201 Aids to Navigation Information
S-111 Surface Currents
S-124 Navigational Warnings
S-128 Catalogues of Nautical Products
Provide real-time information
S-129 Under Keel Clearance Management (UKCM)
Marine Protected Area
S-127 Traffic Management
S-122 Marine Protected Areas
S-102 Bathymetric Surface
S-101 ENC
S-126 Physical Environment

Figure 13. S-100 Data Set and Standards. (IHO,2021)

Thanks to S-100, a relationship, almost a bridge, has been created between bathymetry and oceanography data. It should be understood as a completely digital version of marine ecosystem data that all e-navigation systems can understand the real world with digits. So, all these products are used in e-navigation just because the e-nav systems are becoming more intelligent.

- S-101, Electronic Navigational Charts,
- S-102, Bathymetry Surface,
- S-104 Water Level Information for Surface Navigation,
- S-111 Surface Navigation,
- S-41X Weather Overlays are very important standards for e-navigation and S-100 production can seen in Figure 14.

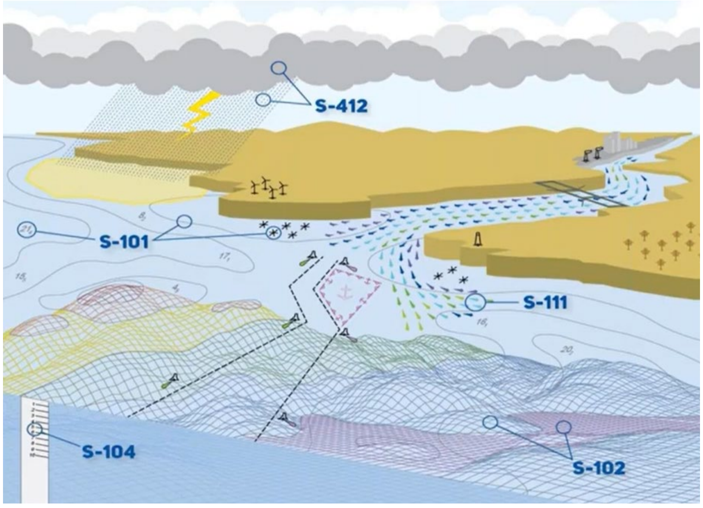


Figure 14. Very important standards for S-100 productions (IHO, 2021)

Table 2. Hydrographic Productions Standards

Standards and numbers	**Descriptions**
S-4	Regulations for International (INT) Charts and Chart Specifications of the IHO
S-5A	Standards of C.ompetence for Category "A" Hydrographic Surveyors
S-5B	Standards of Competence for Category "B" Hydrographic Surveyors
S-8A	Standards of Competence for Category "A" Nautical Cartographers
S-8B	Standards of Competence for Category "B" Nautical Cartographers
S-11	Guidance for the Prep. and Maint. of Int.(INT) Chart and ENC Sch. and Cat. of INT Charts
S-12	Standardization of List of Lights and Fog Signals (June 2004 - Corrections to June 2006)
S-23	Limits of Oceans and Seas (1953). Sheet maps 1, 2 and 3
S-32	Hydrographic Dictionary
S-44	IHO Standards for Hydrographic Surveys
S-49	Standardization of Mariners' Routeing Guides
S-52	Specifications for Chart Content and Display Aspects of ECDIS
S-53	Joint IMO/IHO/WMO Manual on Maritime Safety Information
S-57	IHO Transfer Standard for Digital Hydrographic Data
S-58	ENC Validation Checks
S-60	User´s Handbook on Datum Transformations involving WGS 84
S-61	Product Specification for Raster Navigational Charts (RNC)
S-62	List of IHO Data Producer Codes
S-63	IHO Data Protection Scheme
S-64	IHO Test Data Sets for ECDIS
S-65	ENCs: Production, Maintenance and Distribution Guidance
S-66	Facts about Electronic Charts and Carriage Requirements
S-67	Mariners' Guide to Accuracy of Depth Information in Electronic Navigational Charts (ENC)

Table 2. Hydrographic Productions Standards (continued)

S-97	IHO Guidelines for Creating S-100 Product Specifications
S-99	Operational Procedures for the Org. and Managem of the S-100 Geospatial Inf. Registry
S-100	I HO Universal Hydrographic Data Model - S-100 based Product Specifications
S-101	ENC Product Specification
S-102	Bathymetric Surface Product Specification
S-111	Surface Currents Product Specification
S-121	Maritime Limits and Boundaries Product Specification
S-122	Marine Protected Areas
S-123	Marine Radio Services
S-127	Marine Traffic Management
S-129	Under Keel Clearance Management
S-41X	Weather Overlay

With up-to-date real-world data, all the officers on the vessels can calculate the fastest, safest, and most efficient voyage globally. Also, the maritime industry is affecting many industries (Figure 15). These technological advantages lay the foundations for the future safe navigation of Maritime Autonomous Surface Ships (MASS).

Figure 15. The Maritime Industry works for many reasons. (IHO, 2021)

1.4. MASS Technology

In addition to the benefits that developing technology products provides to humanity, the most important issue to be faced in the future will be the systems and devices that operate unmanned and will be controlled by humans. In maritime trade and transportation, which as a sector has to use more advanced technology compared to other sectors, the issue currently being worked on and causing many discussions about the future is the Maritime Autonomous Surface Ship.

The maritime industry has always been a sector where innovation and advanced technology have found applications. The need for increased efficiency and operational safety has led to the development of various levels of automation both on ships and on land. Recent surveys and expeditions have included situational awareness sensors, such as radar and sonar systems, autonomous navigation systems, off-board communications technologies like satellite communication, and robotics, among others.

Automation, with its potential to reduce the human element and significantly reduce the likelihood of human error, offers a reassuring prospect for the safety of maritime operations. However, it's important to remember that some risks will always be present. Automated systems, while powerful, are not immune to vulnerabilities, from the most straightforward faults like power outages to more threatening faults like cyber/radio frequency/satellite attacks. Risks vary depending on levels of automation and degrees of autonomy; as fully autonomous ships emerge; a set of unique and completely new challenges will need to be addressed. According to IMO studies, a maritime autonomous surface ship can operate independently of human interaction at four degrees. (IMO, 2019)

Degree one: Ship with automated processes and decision support: Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated and, at times, unsupervised, but with seafarers on board, they are ready to take control.

Degree two: Remotely controlled ship with seafarers on board: The ship is controlled and operated from another location. Seafarers are available on board to take control and manage the shipboard systems and functions.

Degree three: Remotely controlled ship without seafarers on board: The ship is controlled and operated from another location. There are no seafarers on board.

Degree four: Fully autonomous ship: The ship's operating system can make decisions and determine actions independently, opening up a world of exciting possibilities.

1.5. Cyber Security

As in almost every sector, the maritime industry also works by keeping up with changing and developing technology. This technological evolution is not just about digitalization, but also about enhancing safety. The global maritime industry is increasingly trying to digitalize, work with operational integration and automation, and reduce human errors. Major mariner nations and maritime trade organizations use the latest technologies and systems that surpass the familiar classical and traditional designs to produce ships and port equipment with advanced remote-controlled communication and connectivity capabilities (DiRenzo *et al.*, 2015; Uflaz *et al.*, 2024). Despite the significant benefits that high-level technology and digital systems bring to their users, they also operate in a vulnerable manner to potential technological threats. Cyber-attacks, in particular, pose a critical and immediate threat to the safety and digital security of ships at sea.

Cyber-attacks can be targeted, aiming at a specific company and its ship, or they can be indiscriminate, striking ships with potential cyber vulnerabilities.

One of the e-navigation elements that may be affected by the attack is the Bridge, where ship navigation and management are carried out. Many elements such as ECDIS, AIS, GNSS, and EPIRB located in Bridge, the ship's brain, can be directly affected. The risk of encountering such attacks increases, mainly thanks to the internet service, which has become an essential human need in today's technology and is primarily requested by the crew (Bolat *et al.*, 2022).

The potential consequences of cyber-attacks are severe, with the possibility of permanent damage to the hull and electronic systems of all ship systems, both commercial and military. In addition to preventing the ship from seeking help, all technical and documentary information and documents belonging to the ship and companies can be seized, leading to significant operational disruptions.

This situation poses a significant threat to the navigational safety of ships, personnel safety, and the reputation of companies. Therefore, it is of utmost importance for ships to proactively prepare against potential cyber-attacks and establish the necessary protective and preventive infrastructures.

1.6. Maritime Communication Information

When humankind first ventured into seafaring, it was a means to secure food and submarine resources for survival. This journey of exploration and discovery continued, evolving with industrialization and the ambition of powerful civilizations to find and utilize resources. Despite the changing priorities of seafarers, the need for maritime communication has always remained constant, marking a fascinating evolution in the history of seafaring (Figure 16).

Particularly in the marine sector, developments and measures have been prepared due to major disasters. The maritime industry has learned a great lesson and standardized the implementation of measures globally.

The Titanic disaster, a tragic event with global repercussions, demonstrated the benefits of remote and wireless communications. Systems that respond especially to emergency calls and Search and Rescue calls have served maritime for more than 100 years, connecting seafarers across the world (IMO-Radio Communications, 2024).

Figure 16. Navigation and communication, search and rescue. (Safety4sea, 2024)

The International Maritime Organization, a key player in maritime safety, considers issues such as navigational safety, survival at sea, and ship-related marine pollution. It has been particularly effective in coordinating and arranging radio communications for search and rescue in case of emergency at sea, providing a reassuring safety net for maritime professionals and policymakers. The first regulation on the subject, a significant milestone in the history of maritime safety, was implemented by the International Telecommunication Union (ITU) in 1906. This was when the SOS signal was first adopted and put into use, a momentous occasion during the International Radio Telegraph Convention accepted in Berlin (Algani *et al*., 2024).

The International Convention for Search and Rescue at Sea (SAR) and the International Convention for the Safety of Life at Sea (SOLAS) have gained importance as amended in 1974. These regulations are not just historical artifacts, but are still being developed and used today, demonstrating the adaptability and ongoing effectiveness of maritime safety regulations.

2. MATERIALS AND METHODS

According to Researchers at NHL Stenden University of Applied Sciences in the Netherlands, from 2001 to 2024, the Maritime Cyber Attack Database was created. Researchers have collected information on over 170 cyber incidents involving the maritime sector, including incidents impacting vessels, ports, and other maritime facilities worldwide.

Due to the development of technology, maritime cyber security affects both ships and relevant units on land. However, it has been understood that one of the most affected electronic navigation aids used for safe navigation is ECDIS. It has been revealed that ships using ECDIS contain many cyber vulnerabilities, such as collisions, grounding, and accidents that may disrupt safe navigation. (Svilicic *et al*., 2019b; 2019c; Tam and Jones, 2019; Androjna *et al*., 2020, Kayışoğlu, *et al*., 2024). When all ship assessment types are applied as per the IMO recommendation, a standard of excellence is upheld. It is understood that the most specific element of cyber security assessment is the execution of cyber security testing based on computational vulnerability scanning and Penetration testing techniques. Penetration testing, on the other hand, is a systematic and comprehensive use of legal and authorized attempts to exploit the target system/asset. Its primary role is to prove the existence of potential cyber risks, making it an essential part of the cyber security assessment process. Electronic Chart Display and Information System has revolutionized the safe navigation of ships. By combining paper maps and other nautical publications, ECDIS has digitized navigation, providing real-time updates, accurate positioning, and enhanced situational awareness. This has significantly improved navigational safety (Brčić *et al*., 2019).

Over the last forty years, studies have created the necessity for the formation and use of ECDIS. Of course, along with the benefits of technology, it also caused various problems that posed a threat to navigational safety, such as safe navigation, which faced cyber threats. (Svilicic *et al*., 2019a, b, c; Kaleem Awan and Al Ghamdi, 2019; Lee *et al*., 2019, Tam and Jones, 2019; Hareide *et al*., 2018; Shapiro *et al*., 2018). The International Maritime Organization (IMO), a specialized agency of the United Nations responsible for regulating shipping, has taken necessary steps to manage cyber risk and prepared guidelines and rules for all the world's seas (IMO, 2017b). It has also regulated performance standards (IMO, 2017a) for better and more efficient operation of ECDIS. In cooperation with the International Electrotechnical Commission (IEC), a new maritime standard for maritime navigation and radiocommunication equipment and systems, IEC 63154, "Cyber Security - General requirements, test methods, and required test results," has started to be studied (IEC, 2019).

Researchers who follow and study digital attacks at sea draw attention to the move to take over the command and control systems of the ships. ECDIS, along with other systems, is significantly impacted by this. When studies on ECDIS between 2010 and 2020 are examined, it is understood that not only one device but also other devices it interacts with are affected. Reports of attacks on more than 20 known e-navigation systems were examined shown by Figure 17.

When cyber-attacks are discussed, it is understood that they attack ship systems using communication systems and communication channels at sea. The investigation revealed that cyber security is aimed at the bridge from which the ship is controlled, especially to take over the cruise control of the ship remotely by affecting the ECDIS device and AIS device. This underscores the urgent need for immediate action to address this critical issue.

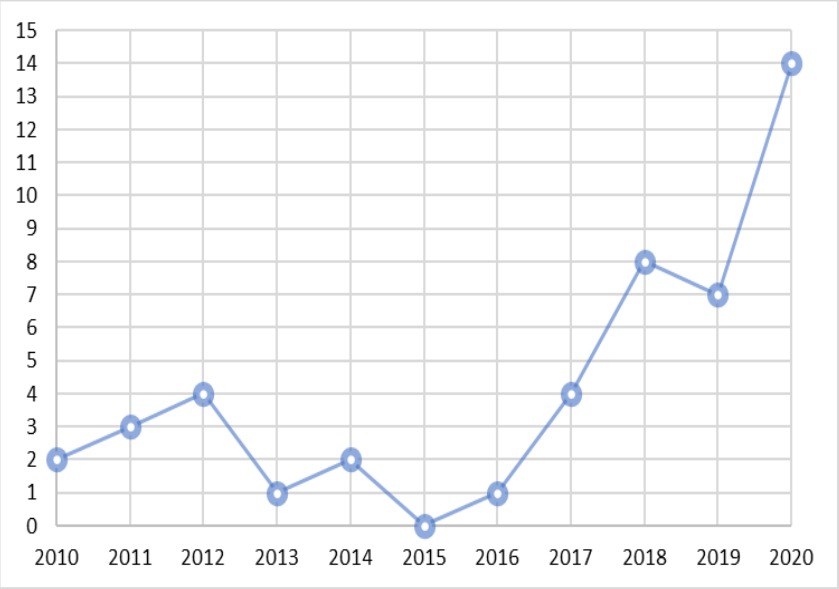


Figure 17. Cyber Incident numbers per year 2010-2020 (Meland *et al*., 2021)

3. RESULTS

The main question is, how can we safely e-navigate the ships?

To ensure safe e-navigation on the ships, the following steps should be taken:

1. **It is crucial to train crew members in effectively utilizing e-navigation systems and how to protect the cyber-attacks. This is a key factor in ensuring their proper use onboard, thereby contributing to the safety and efficiency of the voyage.**
2. Prioritize the use of the most up-to-date electronic navigational charts (ENCs) for route planning. This ensures the ship's route is well-informed and avoids potential hazards and obstacles, thereby enhancing the safety of the voyage.
3. Utilize accurate and reliable data sources: Access accurate and reliable data sources for e-navigation, including meteorological information, water depth, wind speed, and other relevant factors to plan the vessel's course.
4. Identify safety zones and hazard areas: Before commencing navigation, it's crucial to identify potential hazard areas. This vigilance will help you keep clear of these regions during the voyage, ensuring the safety of your vessel and crew.
5. Properly configure automatic pilot systems: It's your responsibility to ensure that automatic pilot systems are accurately configured. This diligence will help maintain the vessel on its intended

course, contributing to the overall safety of the voyage.

6. Verify that radar and other sensors are functioning correctly: Confirm that radar, AIS (Automatic Identification System), and other sensors onboard are in proper working order.
7. Prepare emergency response plans: Develop plans for responding to emergencies such as accidents or fires, train crew members on these procedures, and conduct regular drills to prepare them for any eventuality while using e-navigation systems.
8. **All devices on ships and land must be equipped following cyber security conditions.**

After the eight items explained above, the types of threats that were tried to be explained and the conditions for resisting the threat are mentioned in Table 3. Since all e-navigation systems are integrated and work simultaneously, one cyber-attack element can easily and quickly affect another.

Table 3. Possible Cyber-Attack countermeasure projection.

Affected System	**Affected Devices**	**Possible Precaution against Intimidation and Threats**	**Vulnerabilities effects**
E-Nav Systems (Bridge Navigation System Radiocommunication systems)	Radar ECDIS Conning AIS GPS VDR GMDSS NAVTEX ENC BNWAS Satellite	Ensure the using safe internet and network Internet working security, Ensure using eligible Software, Ensure prepare the Cyber Security applicable procedures, Ensure having available Access controls, Ensure backup of the use of external devices	Make sure that external and internal connections (internet LAN, etc.) are established, Make sure that the software and systems used on all devices are up to date, Ensuring situational awareness, detection, analysis, and intervention during any threat, Ensure all ports to which External Memory can be connected are reliable.
Power systems (generation and distribution)	All the systems (Control, Monitoring, Alarm)	Ensure the possibility to access controls (Physical and logical) Ensure authorized persons' identification checks Ensure Control and audit any time, Ensure it is easy to access by authorized crew member	All-access should be provided to authorized personnel only. All control mechanisms regarding the system must be applicable. All movements must be recorded in the system. The obligation to log out is applied when logging out of the system.

Table 3. Possible Cyber-Attack countermeasure projection (continued).

Affected System	**Affected Devices**	**Possible Precaution against Intimidation and Threats**	**Vulnerabilities effects**
Loading management systems (Dispatch and Administration)	All the systems (Control, Monitoring, Alarm)	Authentication checks must be carried out. (Remote and close) Physical access should only be granted to authorized personnel. National and International Policies and procedures need to be checked periodically. Before using all systems and programs, relevant personnel must be trained.	Authentication using high-level cryptography (Remote) All passwords used should be changed periodically. Situation detection, analysis, and intervention should be carried out when necessary. Every accessible system must be physically and environmentally protected.
Control systems (Access)	All the systems (Control, Monitoring, Alarm)	Ensure that authentication checks are in place. Access permissions should only be provided to authorized personnel. (Physical) All National and International Policies and procedures should be reviewed periodically. Training must be received before using the systems.	Authentication using high-level cryptography (Remote) All passwords used should be changed periodically. Situation detection, analysis, and intervention should be carried out when necessary. Every accessible system must be physically and environmentally protected.
Service and management systems (Crew and Passenger)	All the systems (Control, Monitoring, Alarm)	Ensure the possibility to access controls (Physical and logical) Loading Procedures Ensure authorized persons' identification checks policy Necessary training must be provided to security personnel. Training on security safeguards.	Users must be documented (according to their authority and privileges). Backup systems need to be determined. Sharing of passwords and shared use of accounts is prohibited for all users. The need to recognize and process emergency situations due to situational awareness

Table 3. Possible Cyber-Attack countermeasure projection (continued).

Affected System	Affected Devices	Possible Precaution against Intimidation and Threats	Vulnerabilities effects
Communication systems must use reliable internet.	Connection control equipment must work in harmony with cyber security software.	Protecting confidentiality should be the basic principle. (Especially Network privacy) Updates should be followed. It must be equipped with protection mechanisms against all possible attacks. Latest version protection programs should be used (covering all viruses).	Advanced security measures (such as Routers and firewall) should be used by adopting rules and policies. Continuous notification should be made to the institution and organization where the employee works. Malware infections can be identified.

4. DISCUSSIONS

Maritime transportation carries more than 90% of world trade. Therefore, the maritime industry has a say in all countries with coasts and ports. The sector moves with technology and keeps up with developments quickly. First of all, ships and ports are equipped with advanced technology. The most crucial element, trained human resources, is trained following technological possibilities. However, the development of technology allows malicious use as well as good intentions. Therefore, systemic gaps become cyber threats. Although international institutions and organizations work to ensure safe navigation and prevent marine pollution, cyber security is affected by the rapid development of technology. Ships can be stranded in many threats, from changing their routes to changing their destination port, from opening ship rescue systems to the danger of sinking.

5. CONCLUSIONS

With the rapid evolution of technology, the frequency of cyber-attacks on the maritime sector is on the rise. Shipping Networks and Ships are particularly vulnerable. Notably, even large and crucial companies have fallen victim to these attacks, underscoring the severity of the situation. Despite the professional management of IT staff tasked with defending against these attacks, cyber hackers persist in their activities, employing new methods and effects daily.
Targeted attacks are honing in on the command and control systems of ships, aiming to disrupt both IT and OT technologies. In this context, ECDIS, a key piece of electronic equipment on the bridge, is frequently targeted. While research and tests for precautions are improving daily, the number and severity of threats are also on the rise. It's been found that advanced systems used on ships have previously unrecognized vulnerabilities. Both IMO and electronic device manufacturers advocate and implement preventive measures during production, but the effects of cyber-attacks evolve with technology. Therefore, conducting high-level checks of vulnerabilities and outdated aspects of systems during the production phase can significantly delay and reduce threats.

AUTHORSHIP CONTRIBUTION STATEMENT

Hasan Bora USLUER: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing - Original Draft, Writing-Review and Editing, Data Curation, Software, Visualization, Supervision.

CONFLICT OF INTERESTS

The author declares that for this article they have no actual, potential or perceived conflict of interests.

ETHICS COMMITTEE PERMISSION

No ethics committee permissions is required for this study.

FUNDING

No funding was received from institutions or agencies for the execution of this research.

ORCID IDs

Hasan Bora USLUER:
https://orcid.org/0000-0001-8988-9288

6. REFERENCES

Algarni, A., Acarer, T., Ahmad, Z. (2024). An Edge Computing-Based Preventive Framework With Machine Learning- Integration for Anomaly Detection and Risk Management in Maritime Wireless Communications, *IEEE Access*, 12: 53646-5366. doi: 10.1109/ACCESS.2024.3387529

Androjna, A., Brcko, T., Pavic, I., Gredanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering*, 8 (10): 776. doi: 10.3390/jmse8100776.

Arıcan, O.H., Arslan, O., Unal, A.U. (2023). The Importance of CATZOC in Passage Planning and Prioritization of Strategies for Safe Navigation. *Marine Science and Technology Bulletin*, 12(4): 445-458. https://doi.org/10.33714/masteb.1333432

Bisping, R., Willbond, J., Strohmeier M., Vincent, L. Wireless Signal Injection Attacks on VSAT Satellite Modems, (2024). Accessed Date: 19.07.2024. https://www.usenix.org/system/files/sec24fall-prepub-538-bisping.pdf is retrieved.

Bolat, P., Kayişoğlu, G. (2022). Security Studies: Classic to Post-Modern Approaches, Section 7, Cyber Security,General Perspective on Cyber Security. (Editor: Arda Özkan and Göktürk Tüzsüzoğlu) Lexigton Book, 175-190

Brčić, D., Žuškin, S., Valčić, V., Rudan, I. (2019). ECDIS transitional period completion: analyses, observations and findings. *WMU Journal of Maritime Affairs*, 18: 359–377. doi: 10.1007/s13437-019-00173-z.

DiRenzo, J., Goward, D.A., Roberts, F.S. (2015). The little-known challenge of maritime cybersecurity. In Proceedings of the 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), 1–5, Corfu, Greece

eos-gnss, GNSS systems of the world, (2024). Accessed Date: 20.07.2024 https://eos-gnss.com/knowledge-base/gps-overview-1-what-is-gps-and-gnss-positioning is retrieved.

Hareide, O.S., Jøsok, Ø., Lund, M.S., Ostnes, R., Helkala, K. (2018). Enhancing navigator competence by demonstrating maritime cyber security. *The Journal of Navigation*, 71: 1025–1039. doi: 10.1017/S0373463318000164.

Jiao, C., Wan, X., Li, H., Bian, S. (2024). Dynamic Projection Method of Electronic Navigational Charts for Polar Navigation. *Journal of Marine Science and Engineering*, 12: 577. doi: 10.3390/jmse12040577.

Joseph, A., Dalaklis, D. (2021). The international convention for the safety of life at sea: highlighting interrelations of measures towards effective risk mitigation, *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, 5(1): 1-11. doi: 10.1080/25725084.2021.1880766

IHO, An all embracing data model S-100, (2021). Accessed Date: 19.07.2024. https://www.youtube.com/watch?v=IfKqA7ZkN1w is retrieved.

IHO, Definitions (2024). Accessed Date: 20.07.2024. https://iho.int/en/enc-production is retrieved.

IMO, MSC MASS Degrees, (2019). Accessed Date: 20.07.2024. https://maiif.org/wp-content/uploads/2019/06/MSC-100_20-Annex-20-1.pdf is retrieved.

IMO-Radio Communications, (2024). Accessed Date: 20.07.2024. https://www.imo.org/en/OurWork/Safety/Pages/RadiaCommunicationsSearchRescue-Default.aspx is retrieved.

International Maritime Organization (IMO), (2017a). *ECDIS—Guidance for Good Practice, Resolution* MSC.1/Circ.1503/Rev.1

International Maritime Organization (IMO), (2017b). *Guidelines on Maritime Cyber Risk Management*, MSCFAL.1/Circ.3

International Maritime Organization (IMO), (2017c). *Maritime Cyber Risk Management in Safety Management Systems,* MSC 98/23/Add.1

International Electrotechnical Commission, (2019). *Maritime navigation and radiocommunication equipment and systems-cybersecurity-general requirements, methods of testing and required test results*. IEC 63154 ED1

INMARSAT Coverage on Earth, (2024). Accessed Date: 20.07.2024. https://www.egmdss.com/gmdss-courses/mod/page/view.php?id=2370 is retrieved.

KaleemAwan, M.S., AlGhamdi, M.A. (2019). Understanding the vulnerabilities in digital components of an integrated bridge system (IBS). *Journal of Marine Science and Engineering*, 7: 350–370. doi: 10.3390/jmse7100350.

Kayişoğlu, G., Güneş, B.İ., Bolat, P. (2024). ECDIS Cyber Security Dynamics Analysis based on the Fuzzy-FUCOM Method. *Transactions on Maritime Science,* 13 (1). doi: 10.7225/toms.v13.n01.w09.

Lee, E, Mokashi, A.J., Moon, S.Y., Kim, G. (2019). The maturity of Automatic Identification Systems (AIS) and its implications for innovation. *Journal of Marine Science and Engineering*, 7: 287–304. doi: 10.3390/jmse7090287.

Lee, S., Kim, H. (2024). IHO S-100 Data Model and Relevant Product Specification. *the International Journal on Marine Navigation and Safety of Sea Transportation.* 18(2). doi: 10.12716/1001.18.02.04.

Leite Junior, W.C., de Moraes, C.C., de Albuquerque, C.E.P., Machado, R.C.S., de Sá, A.O.A. (2021). Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems. *Sensors*, 21: 3195. doi: 10.3390/s21093195.

Liangbin, Z., Guoyou, S.İ., Jiaxuan, Y. (2018). Ship Trajectories Pre-processing Based on AIS Data**.** *The Journal of Navigation*, 71(5): 1210-1230. doi: 10.1017/S0373463318000188.

Marine-digital, 21 different types of marine digital equipment's, (2024). Accessed Date: 20.07.2024. https://marine-digital.com/article_21types_of_navigation_equipment is retrieved.

Meland, P.H., Bernsmed, K., Wille, E., Rodseth, O.J., Nesheim, D.A. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents, *International Journal on Maritime and Safety of Sea Tranportation* 15(3): 519-530. doi: 10.12716/1001.15.03.04.

Ming-Cheng, T. (2016), Multi-target collision avoidance route planning under an ECDIS framework, *Ocean Engineering*, 121: 268-278. doi: 10.1016/j.oceaneng.2016.05.040.

NATO Shipping Centre, (2024). Accessed Date: 20.07.2024. https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview is retrieved.

RADAR Screen, (2024). Accessed Date: 20.07.2024. https://www.marineinsight.com/marine-navigation/using-radar-on-ships-15-important-points/ is retrieved.

Rutkowski, G. (2018). ECDIS Limitations, Data Reliability, Alarm Management and Safety Settings Recommended for Passage Planning and Route Monitoring on VLCC *Tankers the International Journal on Marine Navigation and Safety of Sea Transportation*, 12(3). doi: 10.12716/1001.12.03.06.

Shapiro, L.R, Maras, M.H., Velotti, L, Pickman, S., Wei H.L., Till, R. (2018) Trojan horse risks in the maritime transportation systems sector. *Journal of Transportation Security*, 8: 1–19. doi: 10.1007/s12198-018-0191-3.

Safety4sea, e-nav concept, (2024). Accessed Date: 19.07.2024**.** https://safety4sea.com/cm-the-future-of-seafaring-in-an-age-of-safer-smarter-greener-shipping is retrieved.

Safety4sea ECDIS, (2024). Accessed Date: 19.07.2024**.** https://safety4sea.com/cm-ecdis-prons-and-cons-of-paperless-navigation/ is retrieved.

Safety4sea (2024). Navigation and Communication on sea, Accessed Date: 19.07.2024. https://safety4sea.com/imo-navigation-communications-and-search-and-rescue-sub-committee-whats-on-the-agenda/ is retrieved.

SHODB, (2024). Paper and ENC Charts together, Accessed Date: 19.07.2024. https://www.shodb.gov.tr/shodb_esas/index.php/tr/urunler/haritalar/elektronik-seyir-haritalari is retrieved.

Svilicic, B., Kamahara, J., Rooks, M., Yano, Y. (2019a). Maritime cyber risk management: an experimental ship assessment. *The Journal of Navigation*, 72: 1108–1120. doi: 10.1017/S0373463318001157.

Svilicic, B., Kamahara, J., Celic, J., Bolmsten, J. (2019b). Assessing ship cyber risks: a framework and case study of ECDIS security. *WMU Journal of Maritime Affairs*, 18: 509–520. doi: 10.1007/s13437-019-00183-x.

Svilicic, B., Rudan, I., Frančić, V., Doričić, M. (2019c). Shipboard ECDIS cyber security: third-party component threats. *Pomorstvo-Scientific Journal of Maritime Research*, 33 (2): 176–180. doi: 10.31217/p.33.2.7.

Tam, K., Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18: 129–163. doi: 10.1007/s13437-019-00162-2.

Uflaz, E., Sezer, I.E., Tunçel, A.L., Aydin, M., Akyuz, E., Arslan, O. (2024), Quantifying potential cyber-attack risks in maritime transportation under Dempster–Shafer theory FMECA and rule-based Bayesian network modelling, *Reliability Engineering and System Safety*, 243(1). doi: 10.1016/j.ress.2023.109825.

Usluer, H.B. (2022). The effect of the developing and changing Electronic Bridge Equipment and Electronic Navigation Charts on Intelligent Maritime Transportation Systems. *Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi,* 5(1): 116-125. doi: 10.51513/jitsa.1097807.

Xiao, F., Ligteringen, H., Coen van Gulijk, A., Ale, B. (2015). Comparison study on AIS data of ship traffic behavior, *Ocean Engineering*, 95: 84-93. doi: 10.1016/j.oceaneng.2014.11.020.

Wikipedia, NAVTEX, (2024). Accessed Date: 19.07.2024**.** https://tr.wikipedia.org/wiki/NAVTEX#/media/Dosya:Navtex.jpg is retrieved.

Research Article DOI: 10.52998/trjmms.1516839
Turkish Journal of Maritime and Marine Sciences Volume: 10 Special Issue: 1 (2024) 19-30

Performance evaluation of pre-equalized UVLC links over outdated lognormal turbulence channels

Pre-eşitlenmiş UVLC bağlantılarının eski lognormal türbülans kanalları üzerindeki performans değerlendirmesi

Türk Denizcilik ve Deniz Bilimleri Dergisi Cilt: 10 Özel Sayı: 1 (2024) 19-30

Mohammed ELAMASSIE[1,*]

[1]*Department of Electrical and Electronics Engineering, Ozyegin University, Istanbul, Turkey.*

ABSTRACT

Underwater visible light communication (UVLC) is important for various underwater applications, including diver-to-diver information sharing, oil field exploration, port security, underwater surveillance systems, and environmental monitoring. However, it should be remembered that UVLC links are strongly affected by underwater optical turbulence (UOT). This may necessitate frequent adjustments in transmit power based on current channel state information (CSI) to mitigate fading effects. In some applications, such as diver-to-diver links, the quasi-static variations in the channel coefficient between transmission frames—attributable to the semi-fixed positions of the transmitting and/or receiving nodes—lead to practical implementations of the transmit power selection that may rely on outdated CSI. In this paper, we investigate the degradation in error rate performance caused by the use of outdated channel information in setting transmit power. Especially, we derive a closed-form expression for the bit error rate (BER) for a pre-equalized UVLC link over outdated lognormal turbulence channels. We verify the derived expression using Monte Carlo simulations.

Keywords: Underwater visible light communication, optical turbulence, diver-to-diver communication, outdated lognormal turbulence channels.

Article Info
Received: 16 July 2024
Revised: 02 September 2024
Accepted: 08 September 2024

[*](corresponding author)
E-mail: mohammed.elamassie@ozyegin.edu.tr

To cite this article: Elamassie, M. (2024). Performance evaluation of pre-equalized UVLC links over outdated lognormal turbulence channels. *Turkish Journal of Maritime and Marine Sciences*, 10 (Special Issue: 1): 19-30. doi: 10.52998/trjmms.1516839.

ÖZET

Su altı görünür ışık iletişimi (UVLC), dalgıçtan dalgıca bilgi paylaşımı, petrol sahası keşfi, liman güvenliği, su altı gözetim sistemleri ve çevresel izleme gibi çeşitli su altı uygulamaları için önemlidir. Ancak, UVLC bağlantılarının su altı optik türbülansından (UOT) büyük ölçüde etkilendiği unutulmamalıdır. Bu durum, solma etkilerini azaltmak için mevcut kanal durumu bilgisine (CSI) dayalı olarak iletim gücünde sık sık ayarlamalar yapılmasını gerektirebilir. Dalgıçtan dalgıca bağlantılar gibi bazı uygulamalarda, iletim ve/veya alıcı düğümlerin yarı sabit pozisyonlarından kaynaklanan iletim çerçeveleri arasındaki kanal katsayısındaki yarı statik değişiklikler, iletim gücü seçiminin eski kanal verilerine dayanmasına yol açabilir. Bu çalışmada, iletim gücünün ayarlanmasında eski kanal bilgilerinin kullanılmasının hata oranı performansındaki bozulmayı araştırıyoruz. Özellikle, eski lognormal türbülans kanalları üzerinden önceden eşitlenmiş bir UVLC bağlantısı için bit hata oranı (BER) için kapalı formda bir ifade türetiyoruz. Türettiğimiz ifadeyi Monte Carlo simülasyonları kullanarak doğruluyoruz.

Anahtar sözcükler: Sualtı görünür ışık iletişimi, optik türbülans, dalgıçtan dalgıca iletişim, eski lognormal türbülans kanalları.

1. INTRODUCTION

The requirement for underwater communication systems is increasing due to the growing range of human activities underwater, such as underwater scientific data collection, environmental monitoring, oil field exploration, maritime archeology, port security and tactical surveillance (Elamassie *et al.*, 2023; Gussen *et al.*, 2016). Table I summarizes the potential uses, benefits, and limitations of visible light communications (VLC) in various underwater applications. It is important to note that prior to discussing wireless technologies, one should recognize that wire-line systems especially fiber-optic may offer real-time communication solutions underwater and remain a widely accepted and effective solution in some situations. However, wire-line systems are less adaptable and have several shortcomings in their operation, which make them not fully applicable. These limitations necessitate the need for underwater wireless technologies (Elamassie *et. al.*, 2024).

Radio frequency (RF), acoustic, and optical are the three main underwater wireless technologies. The choice of which technology to use underwater depends on the mission requirements and applications. Minimum delay is offered by optical technology due to its high propagation speed. Moreover, optical has high security levels considering it mainly uses line-of-sight (LoS) configurations. These characteristics have made optical technology ideal for real-time, high-data-rate short-distance applications such as underwater imaging and video transmission amongst others. As a result, research into underwater VLC (UVLC) has been intensifying with topics ranging from channel modeling, to controlling propagation channel media, to physical layer and application layer (Gussen *et al.*, 2016; Zeng *et al.*, 2017; Saeed *et al.*, 2019; Ata *et al.*, 2023; Yildiz *et al.*, 2022; Weng *et al.*, 2019; Jiang *et al.*, 2020; Mahmoodi and Uysal, 2022; Wang *et al.*, 2023; Shi *et al.*, 2023; Qian *et al.*, 2023; Zhu *et al.*, 2023; Memon *et al.*, 2023; Hu *et al.*, 2023; Lu *et al.*, 2023; Salam *et al.*, 2023; Wei *et al.*, 2023; Celik *et al.*, 2023; Alqurashi *et al.*, 2023; Tang *et al.*, 2023; Ge and Zhu, 2023; Jiawei *et al.*, 2023; Agarwal and Singh, 2023, Elamassie *et al.*, 2023).

While underwater optical transmission could support high data rates, it is significantly affected by underwater optical turbulence (UOT). Random signal intensity fluctuations caused by fluctuations in refractive index due to salinity and temperature fluctuations within marine environment known as UOT. Bernotas and Nelson, (2015); Oubei *et al.*, (2017); Vali *et al.,* (2018); Jamali *et al.,* (2016), Jamali *et al.,* (2018) have studied the statistical distribution of this underwater fading and it has been found that measurement results generally fit both Lognormal (LN) and Gamma-Gamma (GG) probability density functions which correspond to weak turbulence (WT) and moderate/strong turbulence (MT/ST) conditions respectively. Different viable methods have been presented in the open literature to mitigate the effect of UOT. The widely known one among these is the multiple input multi-output (MIMO) system, which has proved successful in combating fading while exploiting spatial diversity (M. V. Jamali. Nabavi, and J. A. Salehi, 2018). Transmit laser selection (TLS) is another method that effectively eliminates fading with manageable complexity and achieves full diversity gain benefits (Elamassie *et al.*, 2019). In addition, multi-hop serial relaying enhances link distances, energy efficiency improvement as well as cooperative diversity gains (Jamali *et al.*, 2017). It should be however considering that underwater communication possesses unique characteristics, particularly concerning energy availability. Therefore, in good channel conditions, conserving energy by transmitting at low power is needed. Conversely, in poor channel conditions such as weak channel fading coefficient, higher power levels may be used, resulting in more energy consumption in this case. Therefore, one of the possible solutions for mitigating fading coefficient is adaptive power transmission where the transmit power is selected based on the current channel state information (CSI). Most of the literature research works on adaptive optical communication.

Table 1. Potential Applications of UVLC.

Application	**Explanation**	**Limitations**
Oil Field Exploration	Data transmission between underwater exploration equipment.	The water in oil fields can be turbid, which might affect the range and reliability.
Port Security	Enhancing underwater surveillance systems with high-speed data rates.	The turbidity and particulate matter in port waters may limit the effective range.
Environmental Monitoring	Data transmission from sensors monitoring water quality and marine life.	In highly turbid waters, the effectiveness of VLC might be reduced.
Oceanographic Data Collection	Real-time data transmission from various oceanographic instruments.	Depth and water clarity could impact the effectiveness of VLC.
Submarine Communication	Facilitating short-range high-speed communication between submarines.	Limited range and line-of-sight requirements may pose challenges.
Autonomous Underwater Vehicles (AUVs)	Facilitating high-speed data transfer and coordination between AUVs.	Line-of-sight and water clarity issues might limit range and reliability.
Diver Communication Systems	Providing reliable communication for divers, especially in clear waters.	Limited range and the need for line-of-sight may be challenging in some environments.
Underwater Surveillance	Transmitting high-resolution images and video for surveillance.	Effectiveness may be reduced in turbid or particulate-laden waters.
Underwater Robotics	Controlling and receiving data from underwater robots.	Line-of-sight and range limitations may affect usability in complex underwater environments.
Marine Archaeology	Transmitting data and images from underwater archaeological sites.	Water clarity and the need for line-of-sight could pose challenges.
Aquaculture	Monitoring fish behavior and environmental conditions in fish farms.	Limited by water clarity and potential obstructions in fish farming setups.
Recreational Applications	Providing real-time information and enhance underwater tours.	Range and line-of-sight requirements could be a challenge in recreational settings.
Disaster Recovery and Search Operations	Real-time communication and data transmission in search and rescue operations.	Water turbidity and debris may impact the effectiveness of VLC.

systems (Gubergrits *et al.*, 2007; Safi *et al.*, 2019) were built upon the assumption that the CSI is not outdated. In other words, assuming quasi-static (slowly changing) channels, the changes of CSI for a block period of time are neglected. However, an adaptive system requires processing time for estimating CSI, feedback it to the transmitter, and adapting/tuning the transmit parameters. Considering that, in practice, CSI varies continuously (even if the change is slight), the adaptive transmission is based on outdated information. Moreover, the coherence time of the optical channel underwater is generally in the range of 10^{-5} to 10^{-2} sec (S. Tang *et al.*, 2013). Therefore, since the adaptation must be at a rate that is not less than the frequency of channel changes (Elamassie and Uysal, 2021), CSI should be estimated and fed back to the transmitter hundreds, if not thousands, of times per second. Otherwise, CSI is outdated.

When dealing with outdated CSI in certain underwater applications, such as diver-to-diver VLC links or autonomous underwater vehicles (UUV) to sensor nodes, it implies that the parameters for transmission and/or reception may be selected or optimized from channel coefficients that no longer accurately reflect current conditions. This discrepancy arises because these platforms are not perfectly stable. The mismatch between the outdated CSI and the actual CSI can result in suboptimal performance or even communication failure, as the parameters are chosen based on outdated CSI rather than the current one. This issue has previously been addressed in the context of airborne free space optical (FSO) links, where a model for outdated log-normal fading in relay-assisted airborne FSO communication systems was proposed in (Elamassie *et al.*, 2023). Authors have then discussed the utilization of amplification factor based on turbulence strength to ensure signal reception above a targeted threshold even if the channel is outdated.

In this paper, we examine how the selection of transmit power, based on outdated lognormal channel conditions, impacts the BER performance. Specifically, we derive a closed-form expression for the BER of pre-equalized UVLC links operating over outdated lognormal turbulence channels. We validated the derived expression through Monte Carlo simulations. Furthermore, we start the simulation by performing thorough numerical simulations that evaluate the accuracy of outdated lognormal turbulence channel models.

The remainder of the paper is arranged as follows. In Section 2, we present the considered UVLC system model and discuss the outdated lognormal channel. In Section 3, we derive a closed form expression for BER of the considered links over outdated lognormal turbulence channels. Numerical and simulation results are presented in Section 4. We conclude our paper in Section 5.

Notation: Let y be distributed as $\mathcal{LN}\left(\mu,\sigma^2\right)$, indicating y follows a lognormal distribution with mean μ and variance σ^2. Let x be distributed as $\mathcal{N}\left(\mu_n,\sigma_n^2\right)$, indicating x follows a normal distribution with mean μ_n and variance σ_n^2.

2. SYSTEM AND CHANNEL MODELS

As illustrated in Fig. 1, we consider a Diver to Diver UVLC link. The link distance is given by d. Transmit Diver (Denoted by S) is equipped with one laser source with electro-optical conversion factor of η and the receive Diver (Denoted by D) is equipped with one photodetector with opto-electrical conversion factor of r. We assume intensity-modulation direct-detection (IM/DD).

Let x represent the transmitted signal using M-ary unipolar pulse amplitude modulation (M-UPAM). We consider the fading channel coefficient I, which follows a lognormal distribution with variance σ^2 and mean μ, denoted as $I\sim\mathcal{LN}\left(\mu,\sigma^2\right)$. To guarantee that the average power remains unaffected by the channel fading coefficient, it is necessary to normalize the coefficient, implying $\mu=-0.5\sigma^2$. The received signal can be detected with an outdated version of the fading channel coefficient I_{out}. From a mathematical standpoint, the received signal can be expressed as

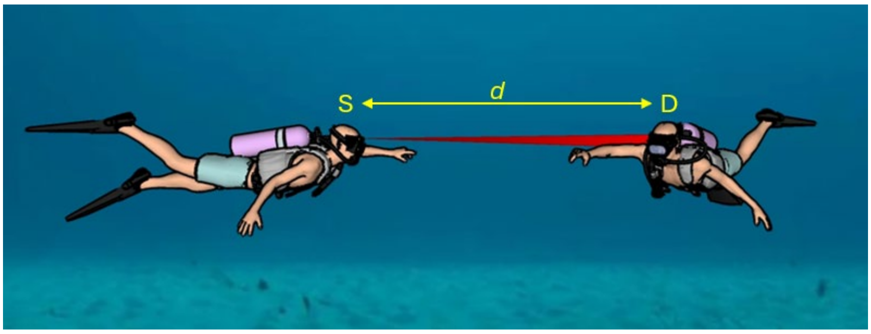


Figure 1. Diver to Diver UVLC Link.

$$y = \sqrt{P_{\mathrm{te}}}\,\eta r h I_{\mathrm{out}} x + w, \tag{1}$$

where h and w denote, respectively, channel deterministic attenuation term and additive white Gaussian noise (AWGN) term with zero mean, i.e., $w \sim \mathcal{N}\left(0, \sigma_n^2\right)$ with σ_n^2 denoting the noise variance. In (1), P_{te} represents the mean electrical transmission power, chosen to ensure that the signal is received with a required power level of P_{req} as

$$P_{\mathrm{te}} = \left(1/\eta^2 r^2 h^2 I^2\right) P_{\mathrm{req}} \cdot \tag{2}$$

By substituting (2) into (1), the received signal can be expressed as

$$y = \sqrt{P_{\mathrm{req}}}\left(\frac{I_{\mathrm{out}}}{I}\right) x + w, \tag{3}$$

indicating that the signal will achieve exactly the necessary power reception only under the condition that the fading channel coefficient remains unchanged (i.e., $I_{\mathrm{out}} = I$).

Feedback from the receiving node to the transmitting node is required for effective implementation of transmit power selection. In diver-to-diver links, UVLC has channel coefficient that may vary from frame to another due to divers being rather non-stationary. As previously denoted, I_{out} represents the outdated version of I and modeled as (Elamassie *et al.*, 2023, eq. (9))

$$I_{\mathrm{out}} = \rho I + (1-\rho) e, \tag{4}$$

where ρ denotes the normalized correlation coefficient and e denotes the channel errors. The fading channel coefficient represents the instantaneous channel condition that varies over time. The 'current' coefficient refers to the present condition, while the 'outdated' one refers to a past coefficient. These coefficients, though from different times, are considered samples from the same underlying probability distribution function, assuming unchanged turbulence strength. This implies that the outdated version of the lognormal fading coefficient (i.e., I_{out}) follows the same lognormal distribution of I, i.e., $I_{\mathrm{out}} \sim \mathcal{LN}\left(\mu, \sigma^2\right)$. To satisfy this, e follows also lognormal distribution with variance $\sigma_e^2 = \sigma^2\left[(1+\rho)/(1-\rho)\right]$ and mean $\mu_e = \mu$, i.e.,

$$e \sim LN\left(\mu, \frac{(1+\rho)}{(1-\rho)}\sigma^2\right), \quad \rho \neq 1 \cdot \tag{5}$$

3. DERIVATION OF BER

It can be noted that the power level of the signal received in equation (3) depends on both the fading coefficient (I) and its outdated version (I_{out}). I_{out} itself is a function of two independent random variables (i.e., I and e). If we define $z = \rho + (1-\rho) e I^{-1}$, we can write the received single as a function of single random variable as

$$y = \sqrt{P_{\mathrm{req}}}\, z x + w, \tag{6}$$

Here, the received instantaneous SNR can simply be defined as $\gamma_{\text{ins}} = \gamma z^2$ with γ denoting the fading free SNR and given as $\gamma = P_{\text{req}} / \sigma_n^2$. As a sanity check, when the channel is not outdated (i.e., $\rho = 1$), the signal will be detected with the required power (i.e., $y = \sqrt{P_{\text{req}}}\, x + w$).

For U-PAM, the conditional BER (i.e., conditioned on z) takes the form of

$$BER_c = F \operatorname{erfc}\left(\sqrt{C\gamma}\, z\right), \tag{7}$$

where $F = (M-1)/\left(M \log_2(M)\right)$ and $C = 3/\left(2(M-1)(2M-1)\right)$. Taking an expectation of (7) with respect to z, we can obtain the average BER as

$$BER = F \int_{-\infty}^{\infty} \operatorname{erfc}\left(\sqrt{C\gamma}\, z\right) f_z(z)\, dz \cdot \tag{8}$$

Performing the integration in (8) requires finding the PDF of $z = \rho + (1-\rho) e I^{-1}$. Recall that $I \sim \mathcal{LN}\left(\mu, \sigma^2\right)$ and $e \sim \mathcal{LN}\left(\mu_e, \sigma_e^2\right)$ are two Independent but Not Identically Distributed (i.n.i.d) lognormal random variables. If we utilize the fact that $\ln\left(x^{-1}\right) = -\ln(x)$, the PDF of I^{-1} can be simply written as

$$I^{-1} \sim LN\left(-\mu, \sigma^2\right) \cdot \tag{9}$$

The PDF of $I^{-1} e$, i.e., the PDF of the product of two i.n.i.d lognormal random variables, follows lognormal and is given by (Drew *et al.*, 2017, Chapter 6) where the overall mean and variance are simply found, respectively, as the summation of means and variances as

$$e I^{-1} \sim LN\left(0, \sigma_e^2 + \sigma^2\right) \cdot \tag{10}$$

The PDF of lognormal random variable multiplied by constant $(1-\rho)$ is obtained by shifting the mean by $\ln(1-\rho)$ (Romeo *et al.*, 2013). Therefore, the PDF of $(1-\rho) e I^{-1}$ is obtained as

$$(1-\rho) e I^{-1} \sim LN\left(\ln(1-\rho), \sigma_e^2 + \sigma^2\right) \cdot \tag{11}$$

The PDF of $z = \rho + (1-\rho) e I^{-1}, z \geq \rho$ can then be obtained by using density transformation (Solomon and Breckon, 2011, Eq. (3.11)) as

$$f_z(z) = \frac{1}{(z-\rho)\sqrt{2\pi\left(\sigma_e^2 + \sigma^2\right)}} \times \exp\left(-\frac{\left(\ln(z-\rho) - \left(\ln(1-\rho)\right)\right)^2}{2\left(\sigma_e^2 + \sigma^2\right)}\right) \cdot \tag{12}$$

If we replace (12) in (8), the average BER can be expressed as

$$BER = \frac{F}{\sqrt{2\pi\left(\sigma_e^2 + \sigma^2\right)}} \int_0^{\infty} \frac{\operatorname{erfc}\left(\sqrt{C\gamma}\, z\right)}{(z-\rho)} \times \exp\left(-\frac{\left(\ln(z-\rho) - \left(\ln(1-\rho)\right)\right)^2}{2\left(\sigma_e^2 + \sigma^2\right)}\right) dz \cdot \tag{13}$$

If the integration variable in (13) is changed of $\xi = \left(\ln(z-\rho) - \left(\ln(1-\rho)\right)\right) \Big/ \sqrt{2\left(\sigma_e^2 + \sigma^2\right)}$, (13) can be written as

$$BER = \frac{F}{\sqrt{\pi}} \int_{-\infty}^{\infty} \exp\left(-\xi^2\right) \times \operatorname{erfc}\left(\sqrt{C\gamma}\left((1-\rho)\exp\left[\sqrt{2\left(\sigma_e^2 + \sigma^2\right)}\,\xi\right] + \rho\right)\right) d\xi \cdot \tag{14}$$

Using the Gauss-Hermite rule, one can express (14) as a truncated sum (Abramowitz and Stegun,1972, Eq. (25.4.46)) as

$$BER \approx \frac{F}{\sqrt{\pi}} \sum_{i=1}^{l} w_{i,l} \times \operatorname{erfc}\left(\sqrt{C\gamma}\left((1-\rho)\exp\left[\sqrt{2\left(\sigma_e^2 + \sigma^2\right)}\, x_{i,l}\right] + \rho\right)\right), \tag{15}$$

where l is the approximation order, $x_{i,l}$, $i = 1, 2, 3, \cdots, l$ is the set of roots defined by

$H_l(x)=0$ with $H_l(x)$ denoting the physicists Hermite polynomial. In (15), $w_{i,l}$, $i=1,2,3,\cdots,l$ are the corresponding weights to $x_{i,l}$.

4. SIMULATION RESULTS

In this section, we first present simulation results validating the expressions for outdated lognormal channel in (4). We then investigate the effect of normalized correlation coefficient on error rate performance and validate our derived closed-form BER expression in (15) via Monte-Carlo simulation results. Unless stated otherwise, we assume modulation order of $M=4$ and fading free SNR in the range of $0\text{ dB}\le\gamma\le 30\text{ dB}$.

In the following, we first confirm that both of the channel fading coefficient (I) and its outdated version (I_{out}) have almost similar distributions for weak turbulence conditions of $\sigma^2<1$. We consider different values of log-amplitude variance of $\sigma^2=1\times10^{-3}$, $\sigma^2=1\times10^{-2}$, and $\sigma^2=1\times10^{-1}$. We further consider normalized correlation coefficients of $\rho=0$, $\rho=0.25$, $\rho=0.50$, $\rho=0.75$, and $\rho=1$.

In Fig. 2, we present the histogram of I_{out} along with the PDF of fading coefficient I. Outdated channel fading coefficients (I_{out}) are calculated through (4). Particularly, channel fading coefficients (I) in (4) are generated using lognormal distribution with mean μ and variance σ^2. Similarly, channel error coefficients (e) in (4) are generated using mean $\mu_e=\mu$ and variance $\sigma_e^2=(1+\rho)/(1-\rho)\sigma^2 \quad \rho\neq1$, (see (5)).

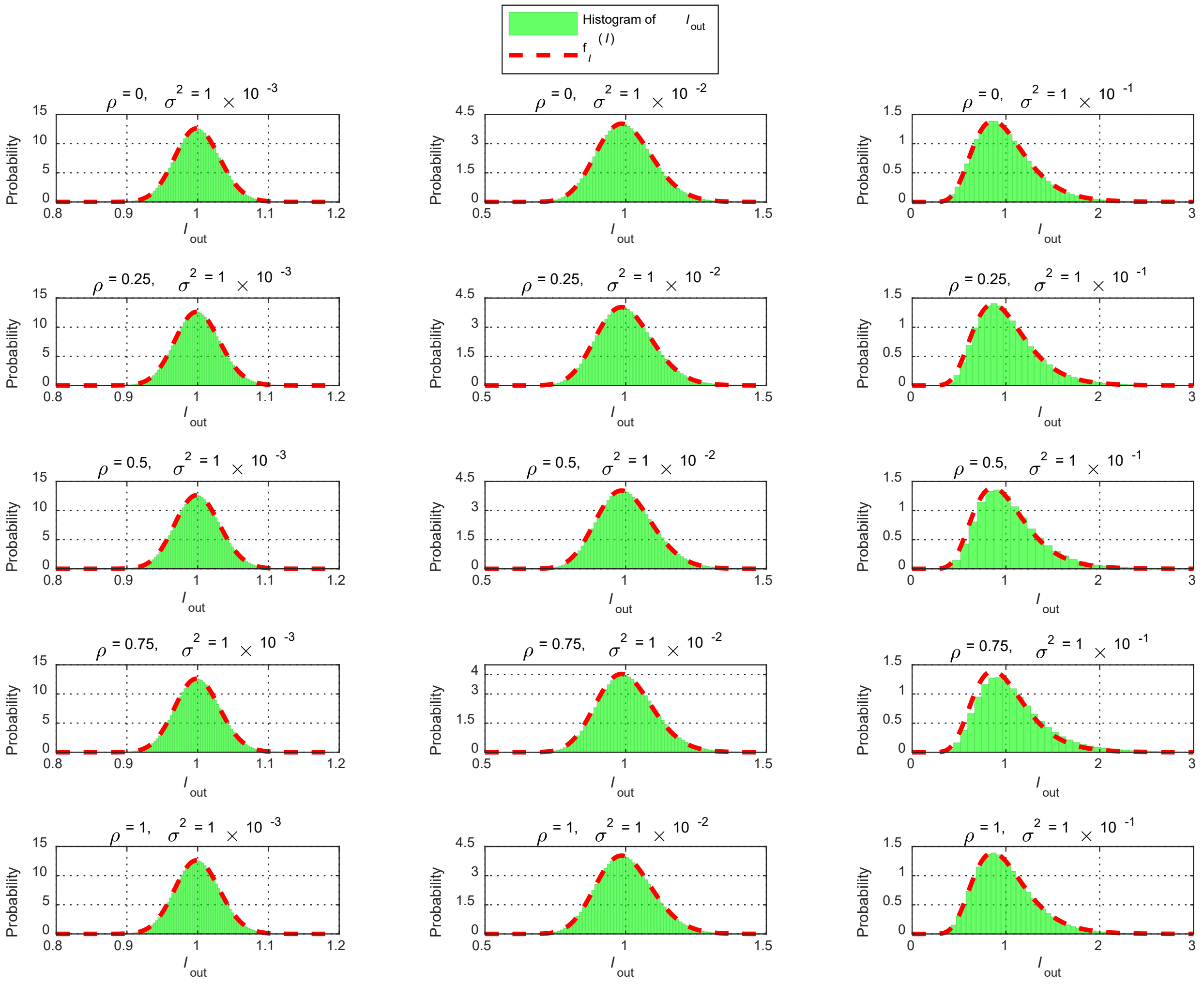


Figure 2. Statistical distribution of I_{out}.

It can be observed for $\sigma^2 < 0.1$ that the histogram of I_{out} coincides with the PDF of I, regardless of the value of normalized correlation coefficient (ρ). As σ^2 become larger, the histogram of I_{out} very slightly deviates from the PDF of I where the deviations depends on the normalized correlation coefficient (ρ).

In the following, we investigate the effect of normalized correlation coefficient on BER values considering log-amplitude variance of $\sigma^2 = 1\times10^{0}$, 1×10^{-1}, 1×10^{-2} and 1×10^{-3} in Figs. 3.a, 3.b, 3.c and 3.d, respectively. For the case of $\rho = 1$, theoretical BER in (7) is used after setting $z = 1$. Our results demonstrated that our derived BER expression in (15) provides a perfect match in all scenarios under consideration confirming the preciseness of our derivations.

On the other hand, while it is known that the outdated channel coefficient (I_{out}) may be larger or smaller than the known channel coefficient at the transmitter side (I), indicating that the instantaneous BER may be larger or smaller than the desired value at a certain SNR, it can be clearly observed from Figs. 3.a, 3.b, 3.c and 3.d that average BER for the case of outdated channel is worse where the smaller the correlation coefficient, the larger the average BER. In other words, higher SNR is needed to achieve the same targeted BER values as long as the normalized correlation coefficient becomes smaller. For example, the required SNR in order to achieve a BER of 10^{-6} assuming

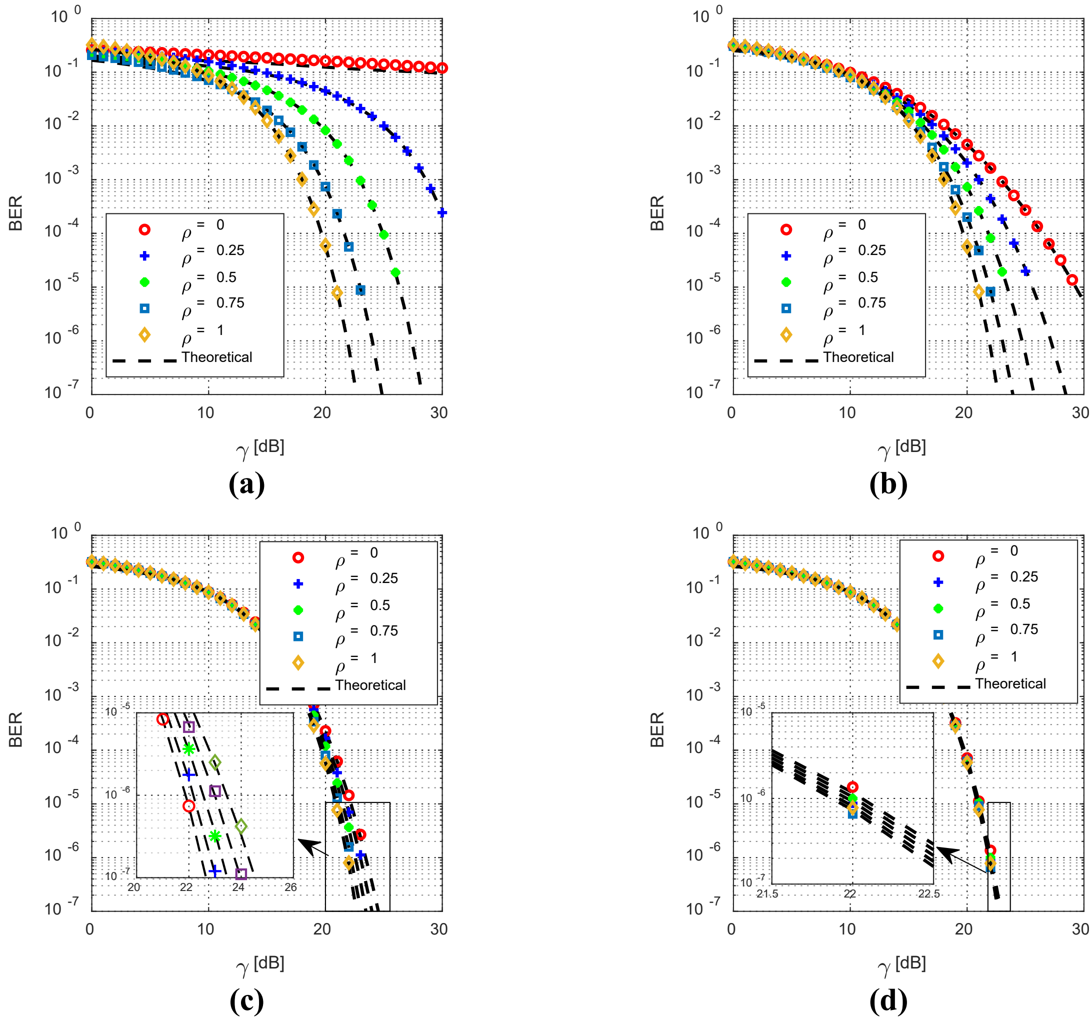


Figure 3. Effect of normalized correlation coefficient on BER: (a) $\sigma^2 = 1\times10^{0}$, (b) $\sigma^2 = 1\times10^{-1}$, (c) $\sigma^2 = 1\times10^{-2}$ and (d) $\sigma^2 = 1\times10^{-3}$.

$\sigma^2 = 1\times10^{-1}$ and normalized correlation coefficient of $\rho = 1$ is $\gamma = 21.88$ dB. This climbs for normalized correlation coefficient of $\rho = 0.75$, 0.5, and 0.25 assuming the same log amplitude variance of $\sigma^2 = 1\times10^{-1}$ to 23.02 dB, 24.67 dB, 27.16 dB. Indicating additional SNR of 1.14 dB, 2.79 dB, and 5.28 dB. It can also be observed that the targeted BER of 10^{-6} cannot be satisfied within the available SNR for zero normalized correlation coefficient, i.e., $\rho = 0.0$. Additionally, the change in average BER is more pronounced for larger turbulence strength (i.e., larger σ^2). For example, the required SNR in order to achieve a BER of 10^{-6} is $\gamma = 21.88$ dB assuming a normalized correlation coefficient of $\rho = 1$. This climbs for $\rho = 0.75$ to 23.75 dB, 23.02 dB, 22.18 dB, and 21.92 assuming, respectively, log-amplitude variance of $\sigma^2 = 1\times10^{-0}$, 1×10^{-1}, 1×10^{-2} and 1×10^{-3}. Indicating additional SNR of 1.87 dB, 1.14 dB, 0.30 dB, 0.04 dB, respectively.

5. CONCLUSIONS

We considered weak UOT that is modeled by lognormal fading and studied how transmit power selection based on outdated lognormal channel affects the BER performance. In particular, we derived a closed-form BER expression for pre-equalized UVLC links over outdated lognormal turbulence channels and validated our findings through Monte Carlo simulations. Our results demonstrated that the average BER deteriorates when channel information is outdated. The level of deterioration depends on the correlation coefficient (ρ) and the turbulence strength (σ^2). Particularly, as the correlation coefficient decreases, the average BER increases, especially for higher turbulence strengths.

CONFLICT OF INTERESTS

The author declares that for this article he has no actual, potential, or perceived conflict of interests.

ETHICS COMMITTEE PERMISSION

No ethics committee permissions are required for this study.

FUNDING

No funding was received from institutions or agencies for the execution of this research.

ORCID IDs:

Mohammed ELAMASSIE:
https://orcid.org/0000-0001-9416-3860

6. REFERENCES

Abramowitz, M., Stegun, I.A. (1972). *Handbook of Mathematical Functions*. US Govt. printing, USA, 10 edition.

Agarwal, A., Singh, K. (2023). Energy-efficient UOWC-RF systems with SLIPT. *Transactions on Emerging Telecommunications Technologies*, e4889.

Alqurashi, F.S., Trichili, A., Saeed, N., Ooi, B.S., Alouini, M.S. (2023). Maritime communications: A survey on enabling technologies, opportunities, and challenges. *IEEE Internet Things Journal*, 10(4): 3525–3547.

Ata, Y., Abumarshoud, H., Bariah, L., Muhaidat, S., Imran, M.A. (2023). Intelligent reflecting surfaces for underwater visible light communications. *IEEE Photonics Journal*, 15(1): 1–10.

Bernotas, M., Nelson, C. (2015). Probability density function analysis for optimization of underwater optical communications systems. In OCEANS 2015 - MTS/IEEE Washington, pp.1–8.

Celik, A., Romdhane, I., Kaddoum, G., Eltawil, A.M. (2023). A top-down survey on optical wireless communications for the internet of things. IEEE *Communication Surveys & Tutorials*, 25(1): 1–45.

Drew, J.H., Evans, D.L., Glen, A.G., Leemis, L.M. (2017). *Computational Probability: Algorithms and Applications in the Mathematical Sciences*. Springer Publishing Company, 2nd edition.

Elamassie, M., Al-Nahhal, M., Kizilirmak, R.C., Uysal, M. (2019). Transmit laser selection for underwater visible light communication systems. In 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 1–6.

Elamassie, M., Al-Shaikhi, A.A., Sait, S.M., Uysal, M. (2023). Multihop airborne FSO systems with relay selection over outdated log-normal turbulence channels. *IEEE Transactions on Vehicular Technology*, 1–13.

Elamassie, M., Geldard, C., Popoola, W. (2024). Underwater Visible Light Communication (UVLC). In: Kawanishi, T. (eds) Handbook of Radio and Optical Networks Convergence. Springer, Singapore. doi: 10.1007/978-981-33-4999-5_62-1

Elamassie, M., Uysal, M. (2021). Feedback-free adaptive modulation selection algorithm for FSO systems. *IEEE Wireless Communication Letters*, 10(9): 1964–1968.

Elamassie, M., Miramirkhani, F., Uysal, M. (2019). Performance Characterization of Underwater Visible Light Communication. *IEEE Transactions on Communications*, 67(1): 543-552.

Ge, X., Zhu, X. (2023). Mathematical modeling of underwater signal anomaly perception based on multi-sensor data fusion. *Journal of Computational Methods in Sciences and Engineering*, 23(1): 23–36.

Gubergrits, M., Goot, R.E., Mahlab, U., Arnon, S. (2007). Adaptive power control for satellite to ground laser communication. *International Journal of Satellite Communications and Networking*, 25(4): 349–362.

Gussen, C.M.G., Diniz, P.S.R., Campos, M.L.R., Martins, W.A., Gois, J.N. (2016). A survey of underwater wireless communication technologies. *Journal of Communication and Information Systems*, 31(1): 242–255.

Hu, Q., Huang, N., Gong, C. (2023). Superposition modulation for physical layer security in water-to-air visible light communication systems. *Journal of Lightwave Technology*, 41(10): 2976–2990.

Jamali, M.V., Chizari, A., Salehi, J.A. (2017). Performance analysis of multi-hop underwater wireless optical communication systems. *IEEE Photonics Technology Letters*, 29(5): 462–465.

Jamali, M.V., Khorramshahi, P., Tashakori, A., Chizari, A., Shahsavari, S., Abdollah Ramezani, S., Fazelian, M., Bahrani, S., Salehi, J.A. (2016). Statistical distribution of intensity fluctuations for underwater wireless optical channels in the presence of air bubbles. In Iran Workshop on Communication and Information Theory (IWCIT), pp. 1–6.

Jamali, M.V., Mirani, A., Parsay, A., Abolhassani, B., Nabavi, P., Chizari, A., Khorramshahi, P., Abdollahramezani, S., Salehi, J.A. (2018). Statistical studies of fading in underwater wireless optical channels in the presence of air bubble, temperature, and salinity random variations. *IEEE Transactions on Communications*, 66(10): 4706–4723.

Jamali, M.V., Nabavi, P., Salehi, J.A. (2018). MIMO underwater visible light communications: Comprehensive channel study, performance analysis, and multiple-symbol detection. *IEEE Transactions on Vehicular Technology*, 67(9): 8223–8237.

Jiang, H., Qiu, H., He, N., Popoola, W., Ahmad, Z., Rajbhandari, S. (2020). Performance of spatial diversity DCO-OFDM in a weak turbulence underwater visible light communication channel. *Journal of Lightwave Technology*, 38(8): 2271–2277.

Jiawei, H., Xiaoqian, L., Xinke, T., Yuhan, D. (2023). Trajectory planning of UUV-assisted UWOC systems based on DQN. *Telecommunications Science* 39(5).

Lu, H.H., Li, C.Y., Tsai, W.S., Chen, Y.X., Fan, W.C., Lin, Y.S., Peng, Y.E., Tang, Y.S. (2023). 5G-based triple-wavelength VLLC-UWLT and laboratory-lighting convergent systems. *Journal of Lightwave Technology*, 41(8): 2351–2360.

Mahmoodi, K.A., Uysal, M. (2022). Energy aware trajectory optimization of solar powered AUVs for optical underwater sensor networks. *IEEE Transactions on Communications*, 70(12): 8258–8269.

Memon, M.H., Yu, H., Jia, H., Fang, S., Wang, D., Zhang, H., Xiao, S., Kang, Y., Ding, Y., Gong, C., Sun, H. (2023). Quantum dots integrated deep ultraviolet micro-LED array toward solar-blind and visible light dual-band optical communication. *IEEE Electron Device Letters*, 44(3): 472–475.

Oubei, H.M., Zedini, E., ElAfandy, R.T., Kammoun, A., Abdallah, M., Ng, T.K., Hamdi, M., Alouini, M. S., Ooi, B.S. (2017). Simple statistical channel model for weak temperature induced turbulence in underwater wireless optical communication systems. *Optics Letters*, 42(13): 2455–2458.

Qian, Y., Chen, C., Du, P., Liu, M. (2023). Hybrid space division multiple access and quasi-orthogonal multiple access for multi-user underwater visible light communication. *IEEE Photonics Journal*, 15(4): 1–7.

Romeo, M., Da Costa, V., Bardou, F. (2003). Broad distribution effects in sums of lognormal random variables. *The European Physical Journal B - Condensed Matter and Complex Systems*, 32(4): 513–525.

Saeed, N., Celik, A., Al-Naffouri, T.Y., Alouini, M.S. (2019). Underwater optical wireless communications, networking, and localization: A survey. *Ad Hoc Networks*, 94: 101935.

Safi, H., Sharifi, A.A., Dabiri, M.T., Ansari, I.S., Cheng, J. (2019). Adaptive channel coding and power control for practical FSO communication systems under channel estimation error. *IEEE Transactions on Vehicular Technology*, 68(8): 7566–7577.

Salam, R., Srivastava, A., Bohara, V.A., Ashok, A. (2023). An optical intelligent reflecting surface-assisted underwater wireless communication system. *IEEE Open Journal of the Communications Society*, 4: 1774–1786.

Shi, J., Niu, W., Li, Z., Shen, C., Zhang, J., Yu, S., Chi, N. (2023). Optimal adaptive waveform design utilizing an end-to-end learning-based pre-equalization neural network in an UVLC system. *Journal of Lightwave Technology*, 41(6): 1626–1636.

Solomon, C., Breckon, T. (2011). *Fundamentals of Digital Image Processing: A practical approach with examples in Matlab*. John Wiley & Sons, New York, NY, USA, 1 edition.

Tang, S., Zhang, X., Dong, Y. (2013). Temporal statistics of irradiance in moving turbulent ocean. In MTS/IEEE OCEANS - Bergen, pp. 1–4.

Tang, Y., Ding, X., Li, Z., Shao, C., Huang, Z., Liang, S. (2023). Crosstalk-free MIMO VLC using two orthogonal polarizations multiplexed large FoV fluorescent antennas. *IEEE Photonics Technology Letters*, 35(23): 1271–1274.

Vali, Z., Gholami, A., Ghassemlooy, Z., Omoomi, M., Michelson, D.G., (2018). Experimental study of the turbulence effect on underwater optical wireless communications. *Applied Optics*, 57(28): 8314–8319.

Wang, K., Song, T., Wang, Y., Fang, C., He, J., Nirmalathas, A., Lim, C., Wong, E., Kandeepan, S. (2023). Evolution of short-range optical wireless communications. *Journal of Lightwave Technology*, 41(4): 1019–1040.

Wei, Z., Wei, Z., Fang, J., Pan, J., Wang, L., Dong, Y. (2023). Impulse response modeling and dynamic analysis for SIMO UOWC systems enhanced by RIS equipped UUV. *IEEE Transactions on Vehicular Technology*, pp. 1–14.

Weng, Y., Guo, Y., Alkhazragi, O., Ng, T.K., Guo, J.H., Ooi, B.S. (2019). Impact of turbulent-flow-induced scintillation on deep-ocean wireless optical communication. *Journal of Lightwave Technology*, 37(19): 5083–5090.

Yildiz, S., Baglica, I., Kebapci, B., Elamassie, M., Uysal, M. (2022). Reflector-aided underwater optical channel modeling. *Optics Letters*, 47(20): 5321–5324.

Zeng, Z., Fu, S., Zhang, H., Dong, Y., Cheng, J. (2017). A survey of underwater optical wireless communications. *IEEE Communication Surveys Tutorials*, 19(1): 204–238.

Zhu, Z., Lei, L., Lin, T., Li, L., Lin, Z., Jiang, H., Li, G., Wang, W. (2023). Embedded electrode micro-LEDs with high modulation bandwidth for visible light communication. *IEEE Transactions on Electron Devices*, 70(2): 588–593.

Research Article DOI: 10.52998/trjmms.1531150
Turkish Journal of Maritime and Marine Sciences Volume: 10 Special Issue: 1 (2024) 31-50

Maritime Cyber Security: Adopting a Checklist Based on IACS UR E26 Standard

IACS UR E26 Standardına Dayalı Gemi Siber Güvenlik Kontrol Listesinin Benimsenmesi

Türk Denizcilik ve Deniz Bilimleri Dergisi Cilt: 10 Özel Sayı: 1 (2024) 31-50

Gizem KAYIŞOĞLU[1,*], Emre DÜZENLİ[1], Pelin BOLAT[1], Fırat BOLAT[1]
[1]*Istanbul Technical University, Maritime Faculty, 34940, İstanbul-Türkiye*

ABSTRACT

The efficient operation of ship systems that control navigation, communications, sensors, and power and machinery is dependent on the increasing digitization of the maritime sector and the intense use of information and operational technologies. The goal of issuing and enforcing global regulations and standards is to lessen the impact of potential dangers that could jeopardize on-board systems, network and data integrity, and operation, functionality and safety. At this point, "Cyber Resilience of Ships" (UR E26) is recently released by the International Association of Classification Societies (IACS) to address the need to improve ships' cyber resilience. This regulation will be applicable to new ships built on and after 1 July 2024. This study aims to create a check list for ship cyber security based on IACS UR E26 standard. A ship cyber security checklist was developed by first analyzing ship operational technologies, identifying potential cyber risks and vulnerabilities, and then creating a checklist in accordance with the IACS UR E26 standard to ensure cyber security on board. With a focus on clean seas and safe ships, the IACS provides technical assistance, verifies compliance, and conducts research and development to enhance maritime safety, security and regulation. This study provides practical tool to ships for ship cyber security management under the safety management system besides IACS standard benefits. Creating a checklist in accordance with the IACS UR E26 standard also allows ship owners and operators to comply with the standards and facilitate inspection processes. This reduces the effort spent to comply with international regulations. It helps to proactively manage cyber risks by providing a systematic approach to ship cyber security management.

Key Words: Maritime cyber security, Ship cyber security check list, Ship cyber resilience, IACS UR E26

Article Info
Received: 10 August 2024
Revised: 05 September 2024
Accepted: 08 September 2024

* (corresponding author)
E-mail: yukselg@itu.edu.tr

To cite this article: Kayışoğlu, G., Düzenli, E., Bolat, P., Bolat, F. (2024). Maritime Cyber Security: Adopting a Checklist Based on IACS UR E26 Standard, *Turkish Journal of Maritime and Marine Sciences*, 10 (Special Issue: 1): 31-50. doi: 10.52998/trjmms.1531150.

ÖZET

Seyir, iletişim, sensörler, güç ve makine kontrol sistemlerinden oluşan gemi sistemlerinin verimli bir şekilde çalışması, denizcilik sektörünün artan dijitalleşmesine ve bilgi ve operasyonel teknolojilerin yoğun kullanımına bağlıdır. Küresel düzenlemeler ve standartların amacı, gemideki sistemlere, ağ ve veri bütünlüğüne, operasyona, işlevselliğe ve güvenliğe zarar verebilecek potansiyel tehlikelerin etkisini azaltmaktır. Bu noktada, Uluslararası Klas Kuruluşları Birliği (IACS) tarafından gemilerin siber dayanıklılığını iyileştirme ihtiyacını ele almak için yakın zamanda "Gemilerin Siber Dayanıklılığı" (UR E26) yayınlandı. Bu düzenleme, 1 Temmuz 2024'ten itibaren inşa edilen yeni gemiler için geçerli olacaktır. Bu çalışma, IACS UR E26 standardına dayalı olarak gemi siber güvenliği için bir kontrol listesi oluşturmayı amaçlamaktadır. Gemi operasyonel teknolojilerinin analiz edilmesi, potansiyel siber risk ve güvenlik açıklarının belirlenmesi ve bu doğrultuda IACS UR E26 standardına uygun bir siber güvenlik kontrol listesi oluşturulması yoluyla bir gemi siber güvenlik kontrol listesi geliştirilmiştir.Temiz denizlere ve güvenli gemilere odaklanan IACS, teknik yardım sağlar, uyumluluğu doğrular ve deniz güvenliğini, emniyetini ve düzenlemesini geliştirmek için araştırma ve geliştirme yürütür. Bu çalışma, IACS standartının faydalarının yanı sıra emniyet yönetim sistemi kapsamında gemi siber güvenlik yönetimi için gemilere pratik bir araç sağlar. IACS UR E26 standardına uygun bir kontrol listesi oluşturmak, gemi sahiplerinin ve operatörlerinin standartlara uymasını ve denetim süreçlerini kolaylaştırmasını da sağlar. Bu, uluslararası düzenlemelere uymak için harcanan çabayı azaltır. Gemi siber güvenlik yönetimine sistematik bir yaklaşım sağlayarak siber riskleri proaktif bir şekilde yönetmeye yardımcı olur.

Anahtar Sözcükler: Denizel alanda siber güvenlik, Gemi siber güvenlik kontrol listesi, Gemi siber dayanıklılığı, IACS UR E26

1. INTRODUCTION

The maritime industry is undergoing a significant transformation driven by the rapid digitization of ship systems and the widespread adoption of information and operational technologies. These advancements have enabled more efficient control of critical systems such as navigation, communications, sensors, and power management, which are essential for the safe and effective operation of modern ships (Kanwal *et al.*, 2024). However, this increased reliance on digital technologies has also introduced new vulnerabilities, particularly in the realm of cyber security.

As ships become more connected, the potential risks associated with cyber threats have escalated, posing significant dangers to on-board systems, network integrity, and overall operational safety (Palbar Misas *et al.*, 2024). Cyber-attacks on ships can lead to severe consequences, including disruptions in communication, navigation failures, data breaches, and even physical damage to ship machinery (Silverajan and Vistiaho, 2019). Recognizing the critical need to address these emerging risks, the International Association of Classification Societies (IACS) has developed the Unified Requirements (UR) on the "Cyber Resilience of Ships" (UR E26) standard, which will come into effect for new ships contracted for construction on or after July 1, 2024 (IACS, 2024). The UR E26 standard represents a proactive approach to enhancing the cyber resilience of ships by providing a comprehensive framework for managing cyber risks throughout the ship's lifecycle. This includes guidelines for the design, construction, and operation of ships with a focus on protecting vital systems against cyber threats.

This study aims to contribute to the ongoing efforts to improve maritime cyber security by developing a practical checklist based on the IACS UR E26 standard. This checklist is designed to assist ship owners and operators in implementing effective cyber security measures as part of their safety management systems. By systematically addressing potential vulnerabilities, the checklist not only facilitates compliance with international regulations but also helps to ensure the continuous and safe operation of ship systems, thereby minimizing the risk of operational disruptions and unexpected failures.

The importance of cyber resilience in the maritime sector cannot be overstated. As digital technologies continue to evolve, the ability to safeguard ship systems against cyber threats will be crucial in maintaining the safety, security, and efficiency of global maritime operations. This paper seeks to provide a practical tool for achieving these goals, reinforcing the essential role of cyber security in the modern maritime landscape.

2. LITERATURE REVIEW

Maritime cyber security has gained increasing attention due to the growing interconnectedness of ships and maritime infrastructure. Research in this field has focused on developing risk assessment techniques and intrusion detection tools (Bolbot *et al*., 2022). The integration of navigational systems on ships, while enhancing safety, also introduces cyber vulnerabilities that require regular maintenance and security testing (Svilicic *et al*., 2019). To address these challenges, academic institutions are developing specialized curricula and research centers dedicated to maritime cyber security (Zăgan *et al*., 2018).

Maritime cyber security guidelines are crucial due to increasing technological dependence and cyber threats in the shipping industry. The International Maritime Organization (IMO) has developed guidelines for cyber risk management, emphasizing the need to address cyber risks in Safety Management Systems by 2021 (IMO, 2022). These guidelines focus on key shipboard Operational Technology systems, including communication, propulsion, navigation, and cargo management (Rajaram *et al*., 2022). They provide risk assessment methods, mitigation measures, and checklists to enhance vessel cyber hygiene (Rajaram *et al*., 2022; Rana, 2019). The guidelines also address the vulnerabilities of Internet of Things (IoT) devices and modern security frameworks used in ships (Ashraf *et al*., 2022). Implementation of these guidelines is crucial for safeguarding against cyber incidents such as GPS interference and malware attacks. National authorities, like the British government, have adopted these guidelines to develop country-specific cyber security practices for ships (Rana, 2019).

In the literature, various studies have demonstrated the cyber vulnerabilities of bridge navigation systems such as GNSS (Santamarta, 2014; Hyra, 2019), VDR (Hyra, 2019; Soner *et al*., 2023a), ECDIS (Hyra, 2019; Jo *et al*., 2022; Kayisoglu *et al*., 2022), and AIS (Hyra, 2019; Tran *et al*., 2021; Soner *et al*., 2023b). Moreover, Kayisoglu *et al*. (2023) examined the CORAS framework to ensure cyber hygiene in shipboard radar systems.

Besides above-mentioned guidelines and researches, iTrust, (2022) lists existing guidelines for maritime cyber security. These are American Bureau of Shipping (ABS) – "The Guide for Cybersecurity Implementation for the Marine and Offshore Industries", Baltic and International Maritime Council (BIMCO) – "Guidelines on Cyber Security Onboard Ships", Det Norske Veritas (DNV) – "Class guideline-Cyber Secure", Det Norske Veritas (DNV) – "Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation", and Institution of Engineering and Technology (IET) – "Code of Practice Cyber Security for Ships". All these guidelines with the IACS UR E26 provide comprehensive framework to implement cyber security onboard ships. However, this study differs from both existing academic research and guidelines in terms of mapping the cyber security measures for the shipboard operational technologies.

3. METHODOLOGY

In this study, it is aimed to create a ship cyber security check list by using IACS UR E26 standard. For this purpose, firstly, ship operational technologies (OT) are examined and their configuration systems in terms of their technological infrastructure, data communication, transferring and processing, and usage function are understood as the context and asset identification by utilizing several maritime cyber security guidelines, ship equipment manufacturer catalog and operational guides, and literature. Then the vulnerabilities of the ship systems and the cyber risks that can occur after the vulnerabilities can be exploited by the malicious people are defined.

The analytical methodologies used in our work include a thorough examination of ship operating technology. First, the current setups and technical infrastructures of ship systems were assessed using a range of marine cyber security standards and literature. The accuracy of the instruments used in this procedure has been verified by comparing them with industry-recognized criteria and standards and verifying them against available literature.

The reliability of the study was guaranteed by using widely utilized protocols in such analyses that have been shown successful in prior research. The verification of the identified cyber hazards and vulnerabilities was conducted by a comparison with documented incidents and guideline papers found in the literature. Furthermore, in order to guarantee the coherence of the results, further studies explored various situations and possibilities throughout the course of the research. Finally, the cyber security checklist for ships is created to ensure cyber mitigation onboard ships by presenting the ships compatibility with IACS UR E26. In this context, the flow diagram for the methodology is as in Figure 1.

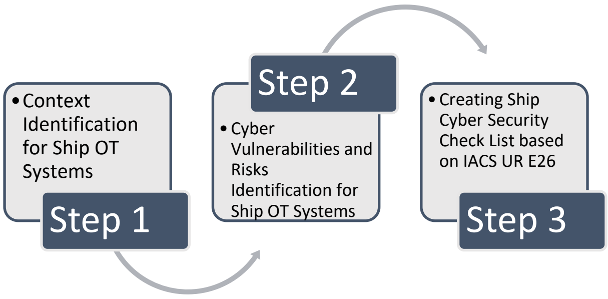

• Context Identification for Ship OT Systems
Step 1
Step 2
• Cyber Vulnerabilities and Risks Identification for Ship OT Systems
• Creating Ship Cyber Security Check List based on IACS UR E26
Step 3

Figure 1. Flow diagram

3.1. IACS UR E26 – Cyber Resilience of Ships

In order to give stakeholders with the technological means to create cyber resilient ships, International Association of Classification Societies (IACS) Unified Requirements (UR) on the “Cyber Resilience of Ships” (UR E26) aims to establish a minimal set of specifications for cyber resilience of ships (IACS UR E26, 2022). The ship as a whole is the focus of IACS UR E26, which aims to provide a foundation for future URs and industry standards that tackle cyber resilience in systems, equipment, and components. It is stated in IACS UR E27 “Cyber Resilience of On-Board Systems and Equipment” that the on-board systems and equipment must meet minimum standards for cyber resilience.

The standard includes mandatory and non-mandatory parts for new ships contracted for construction on or after July 1, 2024. One of these ship types that standard is applicable on as mandatory is cargo ships of 500 gross tonnage (GT) and upwards engaged in international voyages. IACS UR E26 aims to maintain robust cyber security for ships by ensuring secure system design, secure remote connections, and secure manufacturing infrastructure. It is the best practices of ISO 27001 and NIST cyber security framework on the ships.

IACS UR E26 applies to OT systems onboard ships, i.e. those Computer Based Systems (CBSs) using data to control or monitor physical processes that can be vulnerable to cyber incidents and, if compromised, could lead to dangerous situations for human safety, safety of the vessel and/or threat to the environment. In particular, the CBSs used for the operation of the following ship functions and systems are considered communication, navigation, electrical, engine room, cargo control, mooring, ballast systems and any Internet Protocol (IP)-based communication interface from CBSs including crew welfare systems, administrative systems, passenger networks as showed in Figure 2 (Witherby *et al.*, 2023).

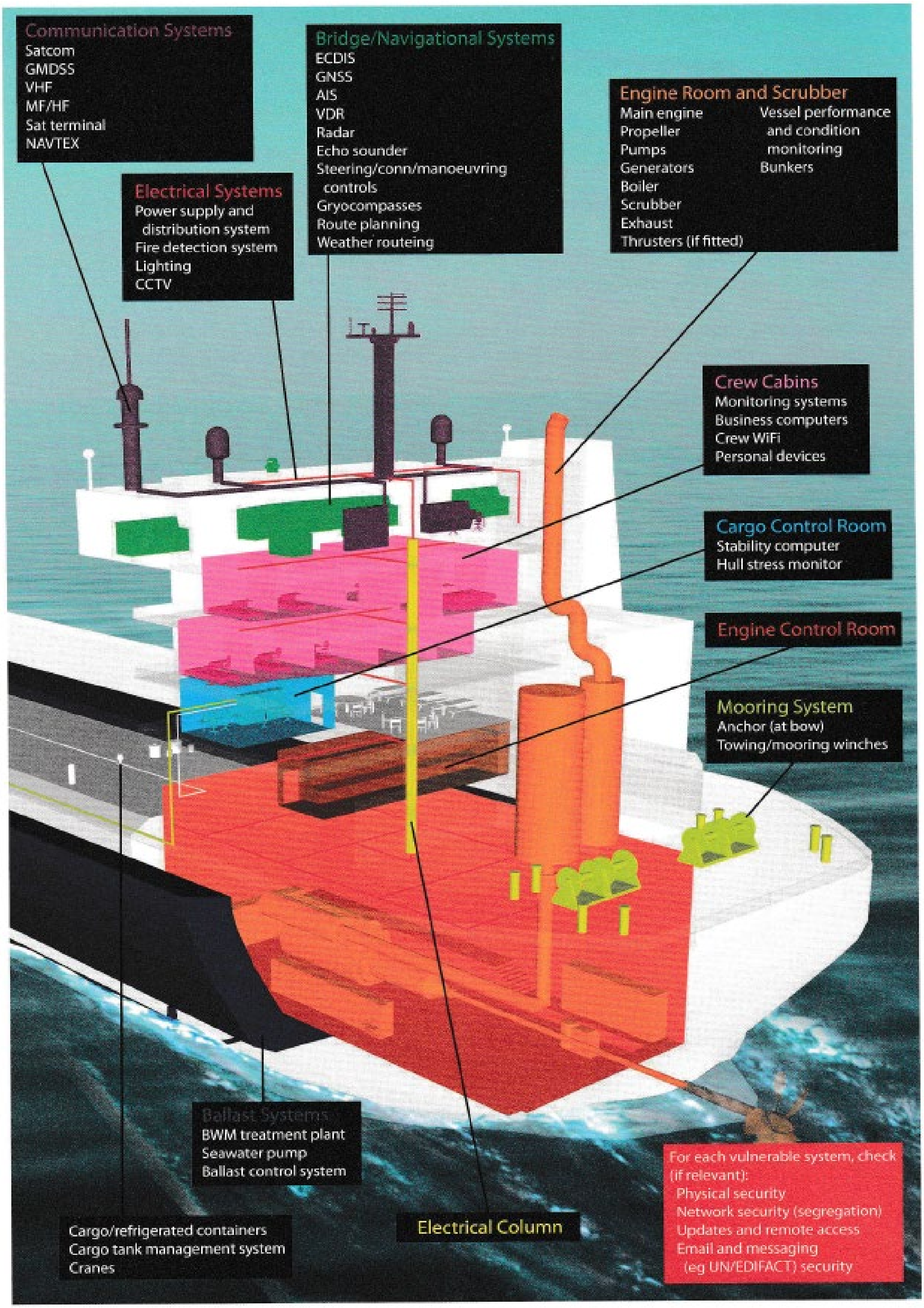


Figure 2. Ship OT systems and their cyber security implications (Witherby *et al*., 2023)

Ship CBSs security capabilities and documentation are designed and set on the ship according to IACS UR E27. System integrators as the stakeholder submit the design documents to the Class society for verification and approval of compliance with requirements in the UR E26. System integrators and shipowner maintain construction, commissioning and operation respectively by keeping the documents updated in accordance with procedure for management of change (MoC). Accordingly, it is concluded that IACS URs integrate each other and the stakeholders including shipyards, system integrator, shipowner, and Class societies work systematically and make cooperation between them according to IACS requirements. This work process and stakeholders' role are shown in Figure 3 (DNV-GL, 2022).

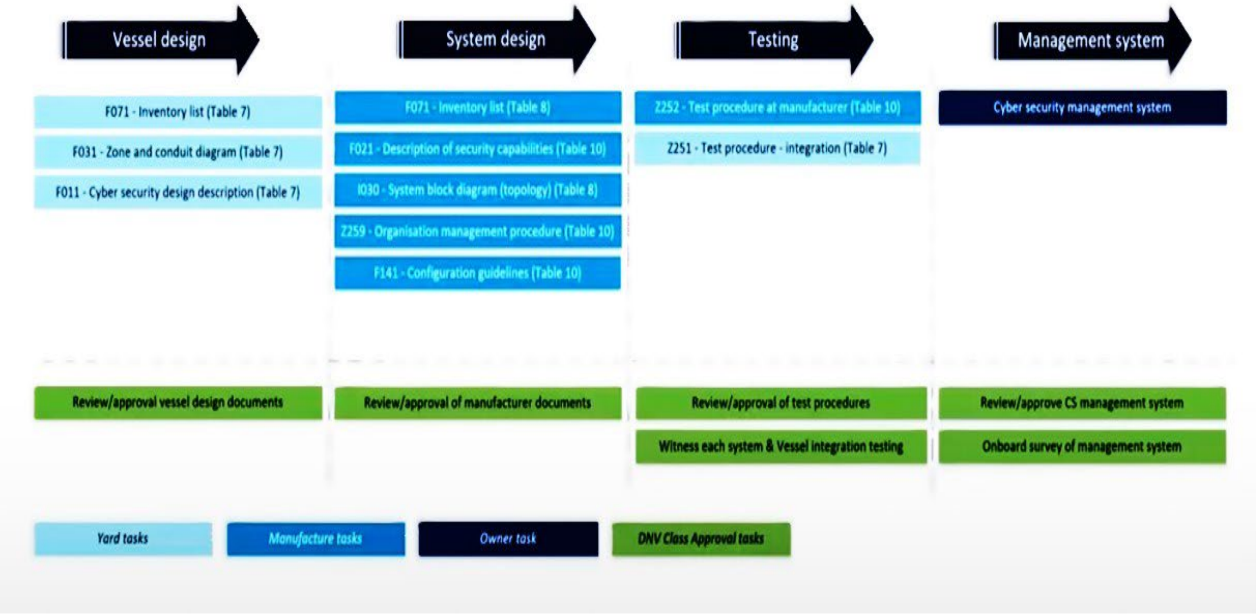
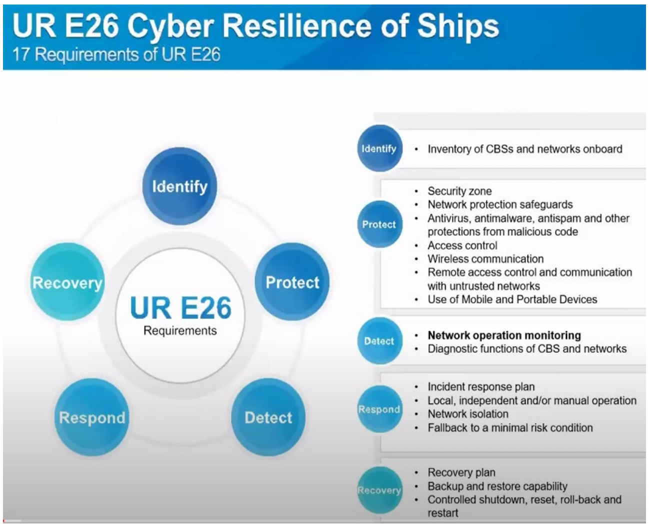

Vessel design
System design
Testing
Management system
F071 - Inventory list (Table 7)
F031 - Zone and conduit diagram (Table 7)
F011 - Cyber security design description (Table 7)
F071 - Inventory list (Table 8)
F021 - Description of security capabilities (Table 10)
I030 - System block diagram (topology) (Table 8)
Z259 - Organisation management procedure (Table 10)
F141 - Configuration guidelines (Table 10)
Z252 - Test procedure at manufacturer (Table 10)
Z251 - Test procedure - integration (Table 7)
Cyber security management system
Review/approval vessel design documents
Review/approval of manufacturer documents
Review/approval of test procedures
Witness each system & Vessel integration testing
Review/approve CS management system
Onboard survey of management system
Yard tasks
Manufacture tasks
Owner task
DNV Class Approval tasks

Figure 3. IACS UR E26 work process

IACS UR E26 involves seventeen requirements under the NIST cyber security framework that includes Identify, Protect, Detect, Respond, and Recovery. The other main part of the standard is demonstration of compliance during design and construction phases, upon ship commissioning, and during the operational life of the ship. Its supplementary part is related to risk assessment for exclusion of CBS from the application of requirements. It also includes security level categorizations from category I to category III, which are suitable with the IACS UR E22 "Computer-based Systems". IACS UR E22 requirements apply to design, construction, commissioning and maintenance of computer-based systems where they depend on software for the proper achievement of their functions. These requirements apply to systems which provide control, alarm, monitoring, safety, or internal vessel communication functions that are subject to classification requirements. Examples of such systems are navigation systems and radio communication system required by SOLAS chapter V and IV, and vessel loading instrument/stability computer (IACS UR E22, 2023). Accordingly, IACS UR E26 integrates with the IACS UR E27 and IACS UR E22.

The requirements of IACS UR E26 are shown in Figure 4 (DNV-GL, 2022). It is firstly required to identify inventory list of CBSs and networks onboard ships. Then, main security measures with protection function are required to be set onboard ships. These requirements cover security zone, network protection safeguards, antivirus, antimalware, and other protections from malicious code, access control, wireless communication, remote access control and communication with untrusted networks and use of mobile and portable devices. The Identify and Protection functions of the standard are almost already implemented onboard ships on service as required International Safety Management (ISM) Code. The International Maritime Organization (IMO) safety code has included a cyber chapter with specific compliance terms including mandatory obligation: MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management. According to the regulation, all vessels are required to implement the necessary cyber security measures no later than 2021 (IMO, 2022) However, the distinctive aspect of IACS UR E26 rather than exist measures under ISM Code starts with the Detect function of the standard. For setting detect function that means cyber-attack detection function on board ships, standard is required network operation monitoring. This is the most significant part for the new constructed ships to ensure cyber security. In Figure 5, an example of network monitoring system is shown (DNV-GL, 2022). The main principle of it is that secure zones for the each OT systems networks of ships are set. Layer 2 switches collect the data packets on each network via network packet collectors. These packets are transferred to Layer3 switch that is called as ship network security device. Internal network data is secured through internal and external firewalls. Ship network security device in the demilitarized zone (DMZ) is equipped with a security management system. By this way, the collected network data is analyzed real time by the cyber security analysts and any anomalies on the systems can be detected by experts and additional security systems such as intrusion detection and prevention systems (IDS/IPS). Additional security functions of the IACS UR E26 are cyber incident response and recovery plans.


UR E26 Cyber Resilience of Ships

17 Requirements of UR E26

Identify
- Inventory of CBSs and networks onboard

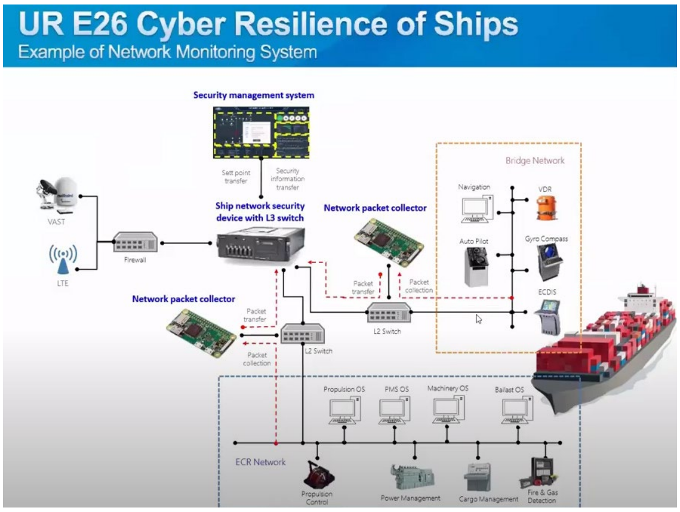
Protect
- Security zone
- Network protection safeguards
- Antivirus, antimalware, antispam and other protections from malicious code
- Access control
- Wireless communication
- Remote access control and communication with untrusted networks
- Use of Mobile and Portable Devices

Detect
- **Network operation monitoring**
- Diagnostic functions of CBS and networks

Respond
- Incident response plan
- Local, independent and/or manual operation
- Network isolation
- Fallback to a minimal risk condition

Recovery
- Recovery plan
- Backup and restore capability
- Controlled shutdown, reset, roll-back and restart

Figure 4. Requirements of IACS UR E26 (DNV-GL, 2022).


UR E26 Cyber Resilience of Ships

Example of Network Monitoring System

Figure 5. Example for network monitoring system

Cyber security requirements for ships according to IACS UR E26 are as in Table 1

Table 1. IACS UR E26 requirements (IACS UR E26, 2022)

Requirement Code	Requirement Name	Section in the Standard	Requirement Definition
R1	Vessel Asset Inventory	4.1.1	An inventory of hardware and software (including application programs, operating systems, if any, firmware and other software components) of the CBSs in the scope of applicability of this UR and of the networks connecting such systems to each other and to other CBSs onboard or ashore shall be provided and kept up to date during the entire life of the ship.
R2	Security Zones and Network Segmentation	4.2.1	All CBSs in the scope of applicability of this UR shall be grouped into security zones with well-defined security policies and security capabilities. Security zones shall either be isolated (i.e. air gapped) or connected to other security zones or networks by means providing control of data communicated between the zones (e.g. firewalls/routers, simplex serial links, TCP/IP diodes, dry contacts, etc.). Only explicitly allowed traffic shall traverse a security zone boundary
R3	Network protection safeguards	4.2.2	Security zones shall be protected by firewalls or equivalent means as specified in section 4.2.1. The networks shall also be protected against the occurrence of excessive data flow rate and other events which could impair the quality of service of network resources. The CBSs in scope of this UR shall be implemented in accordance with the principle of Least Functionality, i.e. configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, where unnecessary functions, ports, protocols and services are disabled or otherwise prohibited.
R4	Antivirus, antimalware, antispam and other protections from malicious code	4.2.3	CBSs in the scope of applicability of this UR shall be protected against malicious code such as viruses, worms, trojan horses, spyware, etc.
R5	Access control	4.2.4	CBSs and networks in the scope of applicability of this UR shall provide physical and/or logical/digital measures to selectively limit the ability and means to communicate with or otherwise interact with the system itself, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions. Such measures shall be such as not to hamper the ability of authorized personnel to access CBS for their level of access according to the least privilege principle.
R5.1	Physical access control	4.2.4.3.1	CBSs of Cat.II and Cat.III shall generally be located in rooms that can normally be locked or in controlled space to prevent unauthorized access, or shall be installed in lockable cabinets or consoles. Such locations or lockable cabinets/consoles shall be however easy to access to the crew and various stakeholders who need to access to CBSs for installation, integration, operation, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship.
R5.2	Physical access control for visitors	4.2.4.3.2	Visitors such as authorities, technicians, agents, port and terminal officials, and shipowner representatives shall be restricted regarding access to CBSs onboard whilst on board, e.g. by allowing access under supervision.
R5.3	Physical access control of network access points	4.2.4.3.3	Access points to onboard networks connecting Cat.II and/or Cat.III CBSs shall be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance. Independent computers isolated from all onboard networks, or other networks, such as dedicated guest access networks, or networks dedicated to passenger recreational activities, shall be used in case of occasional connection requested by a visitor (e.g. for printing documents).

Table 1 (continued). IACS UR E26 requirements (IACS UR E26, 2022)

Requirement Code	Requirement Name	Section in the Standard	Requirement Definition
R5.4	Removable media controls	4.2.4.3.4	A policy for the use of removable media devices shall be established, with procedures to check removable media for malware and/or validate legitimate software by digital signatures and watermarks and scan prior to permitting the uploading of files onto a ship's system or downloading data from the ship's system.
R5.5	Management of credentials	4.2.4.3.5	CBSs and relevant information shall be protected with file system, network, application, or database specific Access Control Lists (ACL). Accounts for onboard and onshore personnel shall be left active only for a limited period according to the role and responsibility of the account holder and shall be removed when no longer needed. is not necessary to "uniquely" identify and authenticate all human users. CBSs which require strong access control may need to be secured using a strong encryption key or multi-factor authentication. Administrator privileges shall be managed in accordance with the policy for access control, allowing only authorized and appropriately trained personnel full access to the CBS, who as part of their role in the company or onboard need to log on to systems using these privileges
R5.6	Least privilege principle	4.2.4.3.6	Any human user allowed to access CBS and networks in the scope of applicability of this UR shall have only the bare minimum privileges necessary to perform its function. The default configuration for all new account privileges shall be set as low as possible. Wherever possible, raised privileges shall be restricted only to moments when they are needed, e.g. using only expiring privileges and one-time-use credentials. Accumulation of privileges over time shall be avoided, e.g. by regular auditing of user accounts.
R.6	Wireless communication	4.2.5	Wireless communication networks in the scope of this UR shall be designed, implemented and maintained to ensure that: - Cyber incidents will not propagate to other control systems - Only authorised human users will gain access to the wireless network - Only authorised processes and devices will be allowed to communicate on the wireless network - Information in transit on the wireless network cannot be manipulated or disclosed
R7	Remote access control and communication with untrusted networks	4.2.6	User's manual shall be delivered for control of remote access to onboard IT and OT systems. Clear guidelines shall identify roles and permissions with functions. For CBSs in the scope of applicability of this UR, no IP address shall be exposed to untrusted networks. Communication with or via untrusted networks requires secure connections (e.g. tunnels) with endpoint authentication, protection of integrity and authentication and encryption at network or transport layer. Confidentiality shall be ensured for information that is subject to read authorization.
R8	Use of Mobile and Portable Devices	4.2.7	The use of mobile and portable devices in CBSs in the scope of applicability of this UR shall be limited to only necessary activities and be controlled in accordance with UR E27 section 4.1 item 10. For any CBS that cannot fully meet these requirements, the interface ports shall be physically blocked. Mobile and portable devices shall only be used by authorised personnel. Only authorised devices may be connected to the CBSs. All use of such devices shall be in accordance with the shipowner's policy for use of mobile and portable devices, taking into account the risk of introducing malware in the CBS.

Table 1 (continued). IACS UR E26 requirements (IACS UR E26, 2022)

Requirement Code	Requirement Name	Section in the Standard	Requirement Definition
R9	Network operation monitoring	4.3.1	Networks in scope of this UR shall be continuously monitored, and alarms shall be generated if malfunctions or reduced/degraded capacity occurs. Measures to monitor networks in the scope of applicability of this UR shall have the following capabilities: (i) Monitoring and protection against excessive traffic, (ii) Monitoring of network connections, (iii) Monitoring and recording of device management activities, (iv) Protection against connection of unauthorized devices, (v) Generate alarm if utilization of the network's bandwidth exceeds a threshold specified as abnormal by the supplier. See UR E22 section 7.2.1. Intrusion detection systems (IDS) may be implemented, subject to the following: (i) The IDS shall be qualified by the supplier of the respective CBS, (ii) The IDS shall be passive and not activate protection functions that may affect the performance of the CBS, (iii) Relevant personnel should be trained and qualified for using the IDS
R10	Verification and diagnostic functions of CBS and networks	4.3.2	CBSs and networks in the scope of applicability of this UR shall be capable to check performance and functionality of security functions required by this UR. Diagnostic functions shall provide adequate information on CBSs integrity and status for the use of the intended user and means for maintaining their functionality for a safe operation of the ship.
R11	Incident response plan	4.4.1	An incident response plan shall be developed by the shipowner covering relevant contingencies and specifying how to react to cyber security incidents. The Incident response plan shall contain documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against CBSs in the scope of applicability of this UR. The Incident response plan shall provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin. The incident response plan shall, as a minimum, include the following information: (i) Breakpoints for the isolation of compromised systems, (ii) A description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events, (iii) A description of expected major consequences related to cyber incidents, (iv) Response options, prioritizing those which do not rely on either shut down or transfer to independent or local control, if any, (v) Independent and local control information for operating independently from the system that failed due to the cyber incident, as applicable. The Incident response plan shall be kept in hard copy in the event of complete loss of electronic devices enabling access to it.
R12	Local, independent and/or manual operation	4.4.2	Any CBS needed for local backup control as required by SOLAS II-1 Regulation 31 shall be independent of the primary control system. This includes also necessary Human Machine Interface (HMI) for effective local operation. The CBS for local control and monitoring shall be self-contained and not depend on communication with other CBS for its intended operation. If communication to the remote control system or other CBS's is arranged by networks, segmentation and protection safeguards as described in 4.2.1 and 4.2.2 shall be implemented. This implies that the local control and monitoring system shall be considered a separate security zone.

Table 1 (continued). IACS UR E26 requirements (IACS UR E26, 2022)

Requirement Code	Requirement Name	Section in the Standard	Requirement Definition
R13	Network isolation	4.4.3	It shall be possible to terminate network-based communication to or from a security zone. Where the Incident Response Plan indicates network isolation as an action to be done, it shall be possible to isolate security zones according to the indicated procedure, e.g. by operating a physical ON/OFF switch on the network device or similar actions such as disconnecting a cable to the router/firewall. There shall be available instructions and clear marking on the device that allows the personnel to isolate the network in an efficient manner. Individual system's data dependencies that may affect function and correct operation, including safety, shall be identified, clearly showing where systems must have compensations for data or functional inputs if isolated during a contingency.
R14	Fallback to a minimal risk condition	4.4.4	As soon as a cyber incident affecting the CBS or network is detected, compromising the system's ability to provide the intended service as required, the system shall fall back to a condition in which a reasonably safe state can be achieved. Fall-back actions may include: (i) bringing the system to a complete stop or other safe state; (ii) disengaging the system; (iii) transferring control to another system or human operator; (iv) other compensating actions. Fall-back to minimum risk conditions shall occur in a time frame adequate to keep the ship in a safe condition. The ability of a system to fall back to a minimal risk condition shall be considered from the design phase by the supplier and the systems integrato
R15	Recovery plan	4.5.1	A recovery plan shall be made by the shipowner to support restoring CBSs under the scope of applicability of this UR to an operational state after a disruption or failure caused by a cyber incident. Details of where assistance is available and by whom shall be part of the recovery plan.
R16	Backup and restore capability	4.5.2	CBSs and networks in the scope of applicability of this UR shall have the capability to support back-up and restore in a timely, complete and safe manner. Backups shall be regularly maintained and tested.

Note: Pink: Identify Function in the NIST; Blue: Protection Function in the NIST; Yellow: Detect Function in the NIST; Grey: Response Function in the NIST; Green: Recovery Function in the NIST

3.2. Ship OT Systems and Cyber Risks

Ship OT systems are shown in Figure 2. The cyber risks are examined for each ship OT systems as in Table 2 by utilizing "Guidelines for Cyber Risk Management in Shipboard Operational Technology Systems" published by iTrust, (2022). The Table 2 highlights the broad spectrum of cyber risks that can impact the various OT systems on ships, ranging from communication and navigation to propulsion and cargo management. The potential impact of these risks includes disruption of operations, unauthorized access to sensitive information, and even physical safety hazards. Therefore, addressing these risks through robust cyber security measures is essential to maintaining the integrity and safety of maritime operations. Accordingly, phishing emails involve deceptive emails designed to trick users into revealing sensitive information or downloading malicious software. In the context of SATCOM and ICS, phishing attacks could compromise the security of communication channels, potentially leading to unauthorized access to critical information (Kesseler, 2019). Vulnerabilities in outdated software can be exploited by attackers to gain control over communication systems, leading to disruptions or unauthorized access (DNV-GL, 2016). Eavesdropping refers to unauthorized interception of communications. For SATCOM, ICS, and VOIP it could lead to the exposure of sensitive information, endangering the vessel's operations (Kavallieratos *et al*., 2019). Unauthorized access of vessel network involves an attacker gaining unauthorized entry into the vessel's network, potentially leading to a full-scale compromise of the ship's communication infrastructure (Tucci, 2017). a DoS attack, which aims at overwhelming the system to disrupt normal operations, incapacitate the WLAN, disrupting network services on the ship, and hampering operational efficiency (Reilly and Jorgensen, 2016). Man-in-the-middle (MITM) attack involves intercepting and potentially altering communications between two systems. In the context of these critical systems, a MITM attack could lead to severe operational disruptions or safety hazards (Kayisoglu *et al*., 2023). Malicious software could be used to disrupt, damage, or gain unauthorized access to these systems, potentially leading to catastrophic failures in propulsion or power management. Malware attack, DoS attack, and Spoofing could severely disrupt navigation by either corrupting data, overwhelming the system, or providing false navigational information, potentially leading to navigational errors (Martínez *et al*., 2024). Ransomware and malware attack could result in the encryption of critical data or disruption of the cargo management processes, leading to operational delays or financial losses (Tam and Jones, 2019).

Table 2. Ship OT systems and cyber risks (iTrust, 2022)

Ship OT Systems	Ship OT Sub-Systems	Cyber Risks
Communication Systems	Satellite Communication System (SATCOM) and Integrated Communication System (ICS)	o Phishing emails o Outdated VSAT software o Eavesdropping o Cross-site scripting attack o Unauthorized access of vessel network
	Voice Over Internet Protocol (VOIP)	o Denial of Service (DoS) attack o Eavesdropping o Vishing
	Wireless Local Area Network (WLAN)	o DoS attack o Access point tampering o Eavesdropping
Propulsion, Machinery and Power Control Systems	Engine System	o Man-in-the-middle (MITM) attack o Malware attack
	Fuel Oil System	o MITM attack o Malware attack
	Alarm Monitoring and Control System	o MITM attack o Malware attack
	Power Management System (PMS)	o MITM attack o Malware attack
Navigation Systems	Electronic Chart Display and Information System (ECDIS)	o Malware attack o DoS attack o Spoofing
	Radio Detection and Ranging (RADAR)	o Malware intrusion o MITM attack
	Automatic Identification System (AIS)	o Spoofing o Replay attack o Frequency hopping attack
	Global Positioning System (GPS)	o GPS spoofing o GPS jamming
	Global Maritime Distress Safety System (GMDSS)	o Spoofing o Eavesdropping o DoS attack
	Voyage Data Recorder (VDR)	o Malware attack o Remote code execution
	Integrated Navigation System (INS)	o MITM attack o Remote code execution
Cargo Management Systems	Cargo Control Room (CCR)	o Ransomware o Malware attack
	Ballast Water System (BWS)	o Malware attack o Phishing emails

3.3. Ship Cyber Security Check List

Based on IACS UR E26, this study aims to create a checklist for ship cyber security. For this purpose, ship OT systems and their cyber risks are examined as Table 2. Then, the attack method for each cyber risks and their mitigations are investigated. Accordingly, IACS requirements are transformed to security control items and matched with applicable ship OT system as in Table 3.

Table 3. Ship cyber security checklist

Requirement Code	Requirement Name	SATCOM and ICS	VOIP	WLAN	Engine System	Fuel Oil System	Alarm Monitoring and Control System	Power Management System (PMS)	ECDIS	RADAR	AIS	GPS	GMDSS	VDR	INS	CCR	BWS
R1	Vessel Asset Inventory	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R2	Security Zones and Network Segmentation		✓				✓					✓					✓
R3	Network protection safeguards		✓				✓					✓					✓
R4	Antivirus, antimalware, antispam and other protections from malicious code	✓				✓	✓	✓	✓						✓	✓	
R5	Access control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R5.1	Physical access control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R5.2	Physical access control for visitors	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R5.3	Physical access control of network access points	✓			✓	✓	✓	✓				✓					✓
R5.4	Removable media controls	✓				✓	✓		✓	✓	✓			✓	✓	✓	
R5.5	Management of credentials	✓			✓	✓	✓										
R5.6	Least privilege principle	✓			✓	✓	✓										
R.6	Wireless communication			✓													

Table 3 (continued). Ship cyber security checklist

Requirement Code	Requirement Name	SATCOM and ICS	VOIP	WLAN	Engine System	Fuel Oil System	Alarm Monitoring and Control System	Power Management System (PMS)	ECDIS	RADAR	AIS	GPS	GMDSS	VDR	INS	CCR	BWS
R7	Remote access control and communication with untrusted networks	✓			✓	✓	✓		✓					✓		✓	✓
R8	Use of Mobile and Portable Devices	✓				✓	✓		✓	✓	✓			✓	✓	✓	
R9	Network operation monitoring		✓				✓					✓					✓
R10	Verification and diagnostic functions of CBS and networks		✓				✓					✓					✓
R11	Incident response plan	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R12	Local, independent and/or manual operation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
R13	Network isolation		✓				✓					✓					✓
R14	Fallback to a minimal risk condition	✓			✓	✓				✓	✓	✓					
R15	Recovery plan				✓	✓				✓	✓	✓					
R16	Backup and restore capability						✓	✓						✓			

4. FINDINGS AND DISCUSSION

This study provides a practical tool for ship cyber security. The obtained checklist can be used as a map for application of the IACS UR E26 onboard ships. According to the Table 3, Vessel Inventory List should be implemented for the whole computer based shipboard operational systems. The vessel asset inventory includes information about the system in the ship's network (system category, security zone where the system is installed), the location and connections of the systems, and the systems' hardware and software. For network devices (switches, firewalls, routers, etc.) and security devices (IDS, Security Information and Event Management (SIEM), etc.) IACS UR E26 is required to be additionally installed by the systems integrator and the inventory information should be filled by them. Security Zones and network segmentation illustrate how systems are grouped when constructing the network on the ship, and how communication between different groups is controlled, providing both physical and logical information. For instance, In the Table 3, SATCOM and ICS, VOIP, and WLAN can be grouped in one network segregation and called as Communication Systems in the security zone. Network protection covers a multitude of technologies, rules and configurations designed to protect the integrity, confidentiality and availability of networks. The threat environment is always changing, and attackers are always trying to find and exploit vulnerabilities. There are many layers to consider when addressing network protection. Attacks can happen at any layer in the network layers model, so network hardware, software and policies must be designed to address each area. While physical and technical security controls are designed to prevent unauthorized personnel from gaining physical access to network components and protect data stored on or in transit across the network, procedural security controls consist of security policies and processes that control user behaviour. The design of network shall include means to meet the intended data flow through the network and minimize the risk of denial of service (DoS) and network storm/high rate of traffic. Estimation of data flow rate shall at least consider the capacity of network, data speed requirement for intended application and data format. Therefore, network safeguard protection should be applied on the systems in each network segregation. In this context, firewall is configured to allow only whitelisted sources or IP addresses within a subnet. Virtual Private Network is used while accessing the Internet. IP address is private, and it is not available on any public domain such as in Shodan. Malware protection should be implemented on CBSs onboard ships. On CBSs having an operating system for which industrial-standard anti-virus and anti-malware software is available and maintained up-to-date, anti-virus and/or anti-malware software should be installed, maintained and regularly updated, unless the installation of such software impairs the ability of CBS to provide the functionality and level of service required. On CBSs where anti-virus and anti-malware software cannot be installed, malware protection shall be implemented in the form of operational procedures and physical safeguards. As the CBSs, antivirus software should be installed in the engine and fuel monitoring system, alarm monitoring & control system and power management system. Besides, OS, antivirus, firewall and other applications used in the business computer (The computer used for accessing emails, and VSAT modem's web interface) is updated/patched regularly. Access to CBSs and networks onboard ships and all information stored on such systems should only be allowed to authorized personnel, based on their need to access the information as a part of their responsibilities or their intended functionality. CBSs of Cat.II and Cat.III shall generally be located in rooms that can normally be locked or in controlled space to prevent unauthorized access or shall be installed in lockable cabinets or consoles. Such locations or lockable cabinets/consoles shall be however easy to access to the crew and various stakeholders who need to access to CBSs for installation, integration, operation, maintenance, repair, replacement, disposal etc. so as not to hamper effective and efficient operation of the ship. Visitors such as authorities, technicians, agents, port and terminal officials, and shipowner representatives shall be restricted regarding access to CBSs onboard whilst on board, e.g. by allowing access under supervision. Access points to onboard networks connecting Cat.II and/or Cat.III CBSs should be physically and/or logically blocked except when connection occurs under supervision or according to documented procedures, e.g. for maintenance. Accordingly, for all systems onboard ships access control requirements should be considered. A policy for the use of removable media devices should be established, with procedures to check removable media for malware and/or validate legitimate software by digital signatures and watermarks and scan prior to permitting the uploading of files onto a ship's system or downloading data from the ship's system. In this context, these requirements should be implemented on the systems having ports for the portable devices such as Alarm Monitoring and Control System, Power Management System, ECDIS, VDR, and cargo control systems. Multi-factor authentication (MFA) should set up for accessing the business computer and VSAT web interface. The admin login credentials in engine and fuel monitoring system, alarm monitoring and control system and power management systems should have strong password. On the GMDSS, messages exchanged between ships and port authorities should be authenticated (e.g., PKI schema). Any human user allowed to access CBS and networks in the scope of applicability of this UR shall have only the bare minimum privileges necessary to perform its function. This is called as zero-trust system. A secure encryption standard should be used in wireless networks. USB port blockers should be used to block unused ports in the engine and fuel monitoring system, alarm monitoring and control system and power management system, as well as other systems including ports. USB cleaning station (a separate PC with antivirus software to scan the USB drives before use) should be setup onboard ships. Finally, the incident response plan should provide procedures to respond to detected cyber incidents on networks by notifying the proper authority, reporting needed evidence of the incidents and taking timely corrective actions, to limit the cyber incident impact to the network segment of origin. The incident response plan shall, as a minimum, include the information about (i) breakpoints for the isolation of compromised systems, (ii) a description of alarms and indicators signalling detected ongoing cyber events or abnormal symptoms caused by cyber events, (iii) a description of expected major consequences related to cyber incidents. The incident response plan should be kept in hard copy in the event of complete loss of electronic devices enabling access to it. Incident response plan should be prepared for all systems onboard ships, but recovery plan should be firstly considered for recover operational life of the ship. Therefore, it should be considered system recovery, which are the specified methods and procedures to recover communication capabilities in terms of Recovery Time Objective (RTO), and data recovery, which are the specified methods and procedures to recover data necessary to restore safe state of OT systems and safe ship operation in terms of Recovery Point Objective (RPO). Consequently, the check list is created by considering stages on the design of the ship, setting systems on the ships, and operating ship systems. Hence, the stakeholders, such as shipyards, system integrators, ship owners, and class societies cooperate each other for ensuring cyber security onboard ships. The IACS UR E26 provides not only design of the systems and integration of them into the ship but also maintaining them onboard ships and auditing them in the first and annual surveys of ships.

5. CONCLUSIONS

In an era where the maritime industry is increasingly reliant on digital technologies, ensuring the cyber resilience of ships has become paramount. This study has developed a practical checklist for ship cyber security based on the IACS UR E26 standard. The checklist serves as a comprehensive tool for ship owners and operators, aiding in the systematic management of cyber risks and ensuring compliance with international regulations.

The implementation of this checklist not only facilitates adherence to the IACS UR E26 standard but also enhances the overall safety and security of maritime operations by addressing potential vulnerabilities in ship systems. By adopting a proactive approach to cyber security, the maritime sector can mitigate the risks associated with cyber threats, thereby safeguarding critical systems and ensuring the uninterrupted operation of ships.

As the maritime industry continues to evolve, the importance of robust cyber security measures will only grow. Future research could focus on the continuous improvement of these measures, ensuring they remain effective against emerging threats. Additionally, the integration of this checklist into broader safety management systems could further streamline operations and improve the resilience of maritime infrastructure.

AUTHORSHIP CONTRIBUTION STATEMENT

Gizem KAYİSOGLU: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing, Review and Editing, Visualization, Supervision.
Emre DÜZENLİ: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing.
Pelin BOLAT: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing, Review and Editing, Visualization, Supervision.
Fırat BOLAT: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing.

CONFLICT OF INTERESTS

The authors decelerate that they have no conflict of interest.

ETHICS COMMITTEE PERMISSION

No ethics committee permissions are required for this study.

FUNDING

This work was funded by Istanbul Technical University, Scientific Research Projects, General Research Project, which is titled as “Protection of Ship Bridge Systems Against Cyber Threats: Security Mechanisms and Implementation Strategies” with 45514 project code.

ORCID IDs

Gizem KAYİSOGLU
https://orcid.org/0000-0003-2730-9780
Emre DÜZENLİ
https://orcid.org/0009-0009-5179-1627
Pelin BOLAT
https://orcid.org/0000-0003-4262-3612
Fırat BOLAT
https://orcid.org/0000-0001-9807-7089

6. REFERENCES

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. Bin, Nosheen, S. (2022). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, 1–14. doi:10.1109/TITS.2022.3164678.

Bolbot, V., Kulkarni, K., Brunou, P., Banda, O.V., Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, 39: 100571. doi: 10.1016/j.ijcip.2022.100571

DNV-GL, (2016). Cyber security resilience management for ships and mobile offshore units in operation. *DNV-GL Corporate Report*, *DNVGL-RP-0* (September), 1–86.

DNV-GL, Cyber Secure Class Notation, (2022). Accessed Date: 03/07/2024, https://www.dnv.com/services/cyber-secure-class-notation-124600/ is retrieved.

Hyra, B. (2019). Analyzing the Attack Surface of Ships. DTU Compute Department of Applied Mathematics and Computer Science Technical University of Denmark. Accessed Date: 08/07/2024, https://backend.orbit.dtu.dk/ws/portalfiles/portal/218483747/190401_Analyzing_the_Attack_Surface_of_Ships.pdf is retrieved.

IACS, IACS UR E26 and E27 Press Release, (2024). Accessed Date: 05/08/2024, https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release is retrieved.

IACS UR E22, Computer-based Systems, (2023). Accessed Date: 05/08/2024 https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2023/08/10161629/ur-e22rev3.pdf is retrieved.

IACS UR E26, Cyber Resilience of Ships, (2022). Accessed Date: 05/08/2024, https://www.classnk.or.jp/hp/pdf/info_service/iacs_ur_and_ui/ur_e26_rev.1_nov_2023_cr.pdf is retrieved.

IMO, Guidelines on Maritime Cyber Risk Management, (2022). Accessed Date: 16/06/2024, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf is retireved.

iTrust, Guidelines for Cyber Risk Manegement in Shipboard Operational Technology Systems, (2022). Accessed Date: 16/06/2024, https://itrust.sutd.edu.sg/research/projects/maritime-cyber/ is retrieved.

Jo, Y., Choi, O., You, J., Cha, Y., Lee, D.H. (2022). Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework. *Sensors*, 22(5): 1860. doi: 10.3390/s22051860.

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., Chang, C.H. (2024). Maritime cybersecurity: are onboard systems ready? *Maritime Policy and Management*, 51(3): 484–502. doi: 10.1080/03088839.2022.2124464.

Kavallieratos, G., Katsikas, S., Gkioulos, V. (2019). Cyber-Attacks Against the Autonomous Ship. In S. K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, A. Antón, S. Gritzalis, J. Mylopoulos, & C. Kalloniatis (Eds.), Computer Security, Springer International Publishing, 11387, pp. 20–36. doi: 10.1007/978-3-030-12786-2.

Kayisoglu, G., Bolat, P., Tam, K. (2022). Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime. *The Journal of Navigation* 75: 364–1388. doi: 10.1017/S0373463322000534.

Kayisoglu, G., Bolat, P., Tam, K., (2023). A novel application of the CORAS framework for ensuring cyber hygiene on shipboard RADAR. *Journal of Marine Engineering & Technology*, 1–15. doi: 10.1080/20464177.2023.2292782.

Kesseler, G.C. (2019). Cybersecurity in the Maritime Domain. *USCG Proceedings of the Marine Safety & Security Council*, 76(1): 11–13.

Martínez, F., Sànchez, L.E., Santos-Olmo, A., Rosado, D.G., Fernàndez-Medina, E. (2024). Maritime cybersecurity: protecting digital seas. *International Journal of Information Security*, 23(2): 1429–1457. doi: 10.1007/s10207-023-00800-0.

Palbar Misas, J. D., Hopcraft, R., Tam, K., Jones, K. (2024). Future of maritime autonomy: cybersecurity, trust and mariner's situational awareness. *Journal of Marine Engineering and Technology*, 23(3): 224–235. doi: 10.1080/20464177.2024.2330176.

Rajaram, P., Goh, M., Zhou, J. (2022). Guidelines for cyber risk management in shipboard operational technology systems. *Journal of Physics: Conference Series*, 2311(1): 012002. doi: 10.1088/1742-6596/2311/1/012002.

Rana, A. (2019). Commercial Maritime and Cyber Risk Management. *Safety & Defense*, 5(1): 46–48. doi: 10.37105/sd.42.

Reilly, G., Jorgensen, J. (2016). Classification considerations for cyber safety and security in the smart ship era. RINA, Royal Institution of Naval Architects - Smart Ship Technology 2016, Papers, January, pp. 33–39.

Santamarta, R. (2014). SATCOM Terminals: Hacking by Air, Sea, and Land. IOActive. Accessed Date: 23/05/2024, https://www.ioactive.com is retrieved.

Silverajan, B., Vistiaho, P. (2019). Enabling Cybersecurity Incident Reporting and Coordinated Handling for Maritime Sector. 2019 14th Asia Joint Conference on Information Security (AsiaJCIS), 88–95. doi: 10.1109/AsiaJCIS.2019.000-1.

Soner, O., Kayisoglu, G., Bolat, P., Tam, K. (2023a). Cybersecurity risk assessment of VDR. *The Journal of Navigation*, 76(1): 20–37. doi: 10.1017/S0373463322000595.

Soner, O., Kayisoglu, G., Bolat, P., Tam, K. (2023b). Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. *Applied Ocean Research*, 142: 103855. doi: 10.1016/j.apor.2023.103855.

Svilicic, B., Rudan, I., Jugović, A., Zec, D. (2019). A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. *Journal of Marine Science and Engineering*, 7(10): 364. doi: 10.3390/jmse7100364.

Tam, K., Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1): 129–163. doi: 10.1007/s13437-019-00162-2.

Tran, K., Keene, S., Fretheim, E., Tsikerdekis, M. (2021). Marine Network Protocols and Security Risks. *Journal of Cybersecurity and Privacy Communication*, 239–251. doi: 10.3390/jcp1020013.

Tucci, A.E. (2017). Cyber Risks in the Marine Transportation System. In: Cyber-Physical Security Protecting Critical Infrastructure at the State and Local Level, R. M. Clark & S. Hakim (Eds.), Springer International Publishing, Switzerland, pp. 113–131. doi: 10.1007/978-3-319-32824-9_6.

Witherby, BIMCO, ICS, (2023). *Cyber Security Workbook for On Board Ship Use*.

Zăgan, R., Raicu, G., Hanzu-Pazara, R., Enache, S. (2018). Realities in Maritime Domain Regarding Cyber Security Concept. *Advanced Engineering Forum*, 27: 221–228. doi: 10.4028/www.scientific.net/AEF.27.221.

Research Article
Turkish Journal of Maritime and Marine Sciences

DOI: 10.52998/trjmms.1531187
Volume: 10 Special Issue: 1 (2024) 51-61

A Comprehensive Analysis of Maritime Cyber Security Incidents: Trends, Impacts, and Countermeasures

Denizcilik Sektöründe Siber Güvenlik Olaylarının Kapsamlı Analizi: Trendler, Etkiler ve Karşı Önlemler

Türk Denizcilik ve Deniz Bilimleri Dergisi

Cilt: 10 Özel Sayı: 1 (2024) 51-61

Emre DÜZENLİ[1], Gizem KAYİŞOĞLU[1,*] Tayfun ACARER[2], Pelin BOLAT[1], Ayşe NAK[1]

[1]*Istanbul Technical University, Maritime Faculty, 3940, Istanbul, Turkiye*
[2]*Piri Reis University, Maritime Faculty, 34940, Istanbul, Turkiye*

ABSTRACT

The maritime industry is currently experiencing a process of digital transformation, which involves a significant level of automation and enhanced communication with external networks. As a result, various facilities in the maritime sector such as commercial and navy vessels, shipping companies, ports, and shipbuilders, are becoming more susceptible to cyber threats. In addition to the potential economic and reputational harm to shipping companies, a cyber-attack on maritime systems could result in significant incidents such as the release of hazardous substances, collisions, grounding, and fires. This poses significant risks to both ship crew, ship, cargo, and environment. This study examines cyber security events in the maritime sector. The main objective is to cultivate a thorough comprehension of cyber-attacks that specifically target systems in maritime facilities, by analyzing insights derived from incidents in the Maritime Cyber-Attack Database. The work involves the construction and examination of a number of cyber security incidents. An inquiry is carried out to determine the time patterns, geographical spread, sector-specific consequences, and attributes of these cyber-attacks, including the identity of the perpetrator, intention (whether deliberate or unintentional), and the affected systems inside the maritime domain. The paper examines particular instances to identify the main stages of a cyber-attack on maritime facilities' systems, the fundamental strategies employed by attackers, and proposes standard cyber security solutions to reduce these risks. The study's contribution entails the methodical delineation of the cyber security terrain that is unique to the maritime industry.

Keywords: Maritime cyber security incident, Maritime cyber security, Cyber incident analysis

Article Info
Received: 10 August 2024
Revised: 05 September 2024
Accepted: 08 September 2024

*(corresponding author)
E-mail: yukselg@itu.edu.tr

To cite this article: Düzenli, E., Kayisoglu, G., Acarer, T., Bolat, P., Nak, A. (2024). A Comprehensive Analysis of Maritime Cyber Security Incidents: Trends, Impacts, and Countermeasures, *Turkish Journal of Maritime and Marine Sciences*, 10 (Special Issue: 1): 51-61. doi: 10.52998/trjmms.1531187.

ÖZET

Denizcilik endüstrisi, kapsamlı otomasyon ve harici ağlarla artan bağlantı ile karakterize edilen dijital bir dönüşümden geçmektedir. Bu durum, deniz tesislerini siber tehditlere karşı savunmasız hale getirmektedir. Nakliye şirketleri için potansiyel ekonomik ve itibar zararının ötesinde, deniz sistemlerine yönelik bir siber saldırı, tehlikeli maddelerin boşaltılması, çarpışmalar, karaya oturma, yangınlar gibi ciddi olaylara yol açabilir ve dolayısıyla hem deniz personeli hem de çevre için önemli tehlikeler yaratabilir. Bu çalışma, denizcilik endüstrisindeki siber güvenlik olaylarını araştırmaktadır. Birincil amaç, geçmiş olaylardan içgörüler çıkararak deniz tesislerindeki sistemleri hedef alan siber saldırılar hakkında kapsamlı bir anlayış geliştirmektir. Çalışma, NHL Stenden Uygulamalı Bilimler Üniversitesi'ne ait Deniz Siber Saldırı Veritabanı'ndan (MCAD) toplanan 146 siber güvenlik olayını analiz etmektedir. Saldırganın kimliği, niyet (kasıtlı veya kazara) ve denizcilik alanı kapsamında etkilenen sistemler dahil olmak üzere bu siber saldırıların zamansal kalıplarını, mekansal dağılımını, sektörel etkilerini ve özelliklerini ayırt etmek için bir araştırma yürütülmüştür. Belirli olayları inceleyerek, çalışma deniz tesislerindeki sistemlere yönelik bir siber saldırının temel aşamalarını, saldırganlar tarafından kullanılan birincil taktikleri belirler ve bu tür tehditleri azaltmak için tipik siber güvenlik önlemlerini önerir. Çalışmanın katkısı, denizcilik sektörüne özgü siber güvenlik manzarasının sistematik haritalanmasını sağlar.

Anahtar Kelimeler: Denizel alanda siber güvenlik olayları, Denizel alanda siber güvenlik, Siber güvenlik olay analizi

1. INTRODUCTION

The maritime industry has seen a significant digital revolution in recent years, characterized by the incorporation of enhanced automation and increased communication with external networks (Kyriakides, 2021). The use of digitization has completely transformed the methods used in maritime operations, resulting in significant improvements in productivity and the ability to gather valuable operational knowledge. Nevertheless, amidst these progressions, a significant obstacle arises - the increasing menace of cyber-attacks aimed at maritime facilities (Bolat *et al*., 2016).

As the maritime industry adopts digital technologies to make procedures more efficient and improve communication, it unintentionally becomes vulnerable to a wide range of cyber threats. The merging of operational technology (OT) and information technology (IT) in maritime systems results in a complicated cyber environment, with numerous vulnerabilities and a significant risk of malicious exploitation. Every element within the maritime network, including cargo ships and port infrastructure, can be targeted by cyber attackers with the intention of disrupting operations, causing financial harm, or posing a risk to human life (Farah *et al*., 2022).

The ramifications of a successful cyber-attack on maritime systems go much beyond simply monetary losses or harm to the reputation of shipping corporations (Tam and Jones, 2019). Undoubtedly, these catastrophes have the capacity to trigger disastrous events with significant consequences for both human existence and the environment. Compromised maritime systems can pose serious threats such as the release of hazardous substances, collisions, grounding, and fires (Bernsmed *et al*., 2017). Given these potential dangers, ensuring the cyber security of maritime facilities is of utmost significance, as it not only safeguards assets and infrastructure, but also preserves human safety and environmental integrity.

In light of this context, this study aims to thoroughly investigate cyber security occurrences in the maritime industry. The study aims to gain a detailed understanding of the changing cyber threat landscape in the maritime sector by evaluating a complete dataset of 146 cyber security incidents and extracting insights from prior occurrences. The focus of this effort is to analyze the timing patterns, geographical spread, effects on different sectors, and methods used in cyber-attacks on maritime systems. The study is centered around the Marine Cyber-Attack Database (MCAD), which is a collection of data on cyber security occurrences in the marine industry. The database is managed by NHL Stenden University of Applied Sciences and provides valuable empirical information (NHL STENDEN University of Applied Science, 2001). Using this dataset, the study seeks to uncover the complexities of cyber-attacks on maritime facilities, providing insight into the identities of the attackers, their motives (whether deliberate or unintentional), and the specific systems that are most targeted within the maritime ecosystem.

The study aims to analyze individual occurrences and uncover similarities among different cyber-attacks in order to outline the main stages of an assault on maritime systems, identify the principal strategies used by attackers, and propose effective cyber security measures to reduce these dangers. This study aims to provide stakeholders in the maritime industry with the necessary knowledge and insights to strengthen their ability to withstand cyber-attacks and enhance their defenses against constantly changing cyber threats. The study seeks to provide industry stakeholders, policymakers, and cyber security professionals with practical insights to protect the integrity, security, and sustainability of maritime operations in an increasingly digitalized world by explaining the complex nature of cyber risks faced by maritime facilities.

2. LITERATURE REVIEW

A comprehensive analysis of cyber incidents in the maritime sector reveals a significant number of unreported attacks, emphasizing the need for improved threat information sharing. These incidents, often with low frequency but high impact, are difficult to predict and prepare for, and are carried out by a variety of attackers using different techniques (Meland *et al*., 2021). The maritime industry's cyber security policy, cyber-attacks, and vulnerability assessment are key components in addressing these threats (Mednikarov *et al*., 2020). A holistic approach to maritime cyber security management is recommended, with a focus on the increasing complexity, digitalization, and automation of systems (Mraković and Vojinović, 2019).

Silverajan and Vistiaho (2019) stated in their study that a prevalent security vulnerability currently identified in maritime vessels and operation systems is the simplicity of infiltration of malicious code and payloads, including but not limited to malware, ransomware, spyware, and viruses, into the critical systems of a ship. Injections of this nature manifest via malicious firmware updates, the introduction of a compromised device or sensor into the ship's network, or the utilization of infected removable media.

It has been discovered that certain onboard Voyage Data Recorders (VDR) are vulnerable to buffer overflows, common injection flaws, and faulty firmware update mechanisms (Söner *et al*., 2023). VDRs are supposed to be tamper-proof, but incidents have already occurred showing VDRs have been tampered with, in order to eliminate incriminating evidence of ship activity. Ships are facing a growing number of cyber security risks associated with the compromise of their positioning and navigational systems, specifically through the manipulation or forgery of the Global Positioning System (GPS) signal. The act of spoofing a GPS signal entail manipulating the positioning systems installed on an unmanned vessel to perceive a forged signal, with the intention of causing inadvertent course corrections. GPS signal jamming is executed in a manner analogous to GPS signal deception, whereby the GPS receiver is obstructed from receiving any GPS signals or is duped into obtaining inaccurate location coordinates. At present, there is evidence suggesting that state-sponsored operations engage in deceptive GPS spoofing (Androjna and Perkovič, 2021).

Cyber security incidents in the maritime domain extend beyond the confines of ship-based systems. Recent reports have surfaced from various parts of the globe regarding ransomware and malware infections that specifically target ship navigational and control systems and ports (Meland *et al*., 2021). The NotPetya cyber-attack, which targeted the global systems of a shipping conglomerate, had far-reaching and consequential consequences that affected not only the organization but also the entire industry. Furthermore, it caused significant devastation to numerous interconnected enterprises operating in the manufacturing, logistics, and cargo handling sectors (Capano, 2021).

Karas (2023) stated that installing software, exchanging data, logging into systems, online banking operations, using data carriers these are just a few examples of activities during which a cyber-attack is possible. Accordingly, the most common types of cyber-attacks in maritime are phishing attacks, watering hole attacks, physical infiltrations, cyberpiracy, ransomware, integrated bridge system tampering, Automatic Identification System (AIS) spoofing, VDR tampering, GPS jamming.

In the literature, the studies directly related to maritime cyber incident analysis are limited. These are (Meland *et al*., 2021) and a preprint study Schwarz *et al*. (2021) However, rather than maritime industry, there are some studies related to cyber incident analysis in other sectors. For instance, Iaiani *et al*. (2021) aimed to provide a comprehensive overview of cyber-attacks on automated control systems in process facilities and share lessons learned from previous occurrences. Davis *et al*. (2009) examined the potential effects of cyber security incidents on firms that primarily operate online. It is tested for structural changes caused by widely reported cyber security incidents using web traffic time series for a representative collection of online firms. The findings consistently show that cyber security incidents have negligible effect on the structure of web traffic for the sample of online firms examined. Patterson *et al*. (2023) offer a fresh look at how organizations learn from incidents by methodically examining academic research on organizational learning from cyber security incidents and recommending additional research needs in this area. Kaneko *et al*. (2021) looked into an information security incident case called "AIST (National Institute of Advanced Industrial Science and Technology) report on unauthorized access to information systems," and attempted accident analysis with Causal Analysis using System Theory (CAST). They studied whether CAST, which is generally used for safety analysis, might be used to conduct cyber security analysis.

To the best of authors' knowledge, there is a gap for cyber incident analysis towards maritime industry in the literature. In this study, similar to Iaiani *et al*. (2021), a significant number of cyber-attacks infected the Operational Technologies (OT) systems and Information Technologies (IT) in maritime sector are analyzed by focusing on time trend, geographical distribution, impacts of the incidents, and nature of the cyber-attacks (attacker, intentional/accidental type, system infected). The analysis of a sub-set of more detailed incidents allowed the identification of the general steps of a cyber-attack on maritime systems, the main hacking techniques used by the attackers and the more common cyber security countermeasures applicable to the prevention of a cyber-attack.

3. METHODOLOGY

Data from the Marine Cyber-Attack Database (MCAD), the website containing cyber-attack data on the maritime industry created by NHL Stenden University of Applied Sciences, were analyzed. A total of 146 cyber-attacks took place between 2001 and 2023. These attacks were examined by dividing them into categories such as year, month, number of incidents, incident country, victim country, victim type, attack type. These categories are associated with each other and the number of incidents by years, the number of incidents by months, the comparison of incidents by months and years, the number of incidents by victim type, the number of incidents by countries, the number of cyber-attack attack types, the types of cyber-attacks on ships and ports are visualized and the findings are presented.

4. FINDINGS

The internet-based data shared by NHL Stenden University of Applied Sciences was analyzed in different categories. When cyber-attacks against the maritime sector from 2001 to 2023 are examined, it can be said that there is a generally rising trend until 2020 with the increase in technological developments (Figure 1). When the data is examined with the impact of the COVID epidemic on the world in 2020 and 2021, it is observed that there is an increase in cyber-attacks against the maritime sector. In the following years, it has been observed that there has been a decrease in these attacks with the increasing awareness in the sector, rules, published guidebooks and the measures taken by companies to protect their information systems. However, it should not be forgotten that with technological innovations, the number of successful cyber-attacks will increase due to the diversity of cyber-attacks and the lack of understanding of the cyber vulnerabilities of new systems.

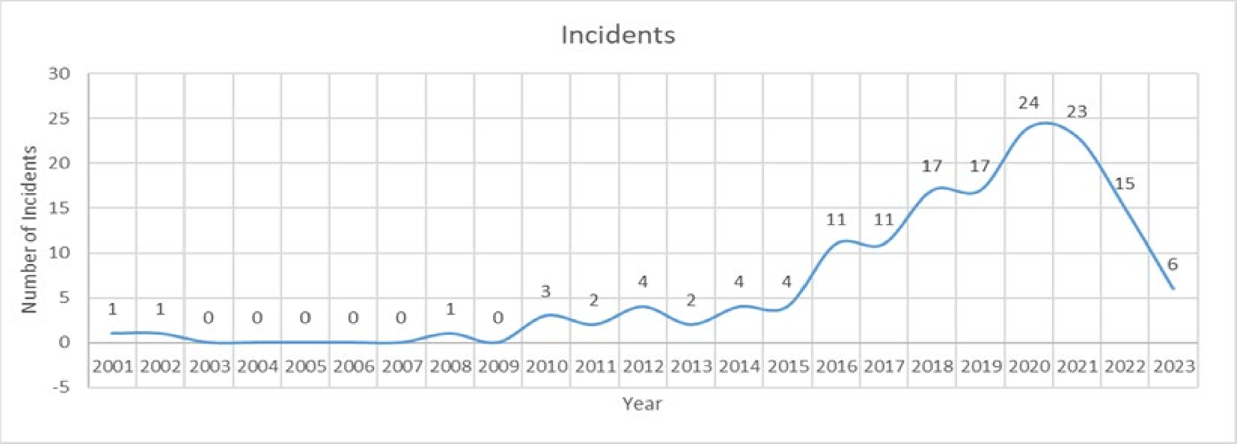


Figure 1. Cyber-attack incidents analysis to maritime sector between 2001 and 2023

When the cyber-attacks are analyzed by months, it can be said that the density of cyber-attacks is between 8 and 13 bands in Figure 2. However, cyber-attacks are more common in June, the beginning of summer, and September, the beginning of autumn, compared to other months. After June, especially in the months when people's holiday plans were more intense, cyber-attacks against the maritime sector showed a downward trend compared to other months, and with the beginning of September, this decrease ended and cyber-attacks increased.

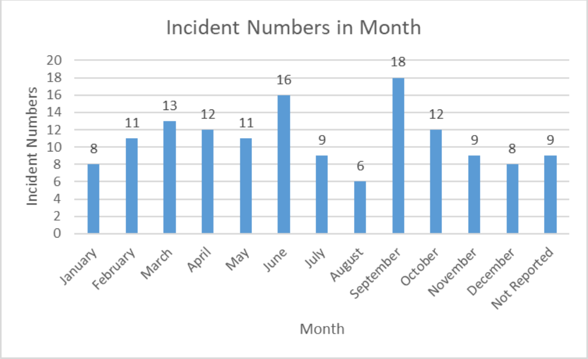


Figure 2. Number of cyber incidents by month from 2001 to 2023

When examined by year and month, as shown in Figure 3, the highest number of cyber-attacks against the maritime sector occurred in September 2020, 9 in total. One of these attacks took place against the CMA CGM company. The attackers notified the company that was exposed to the Ragnar Locker ransomware cyber-attack by sending an e-mail on September 27, 2020.

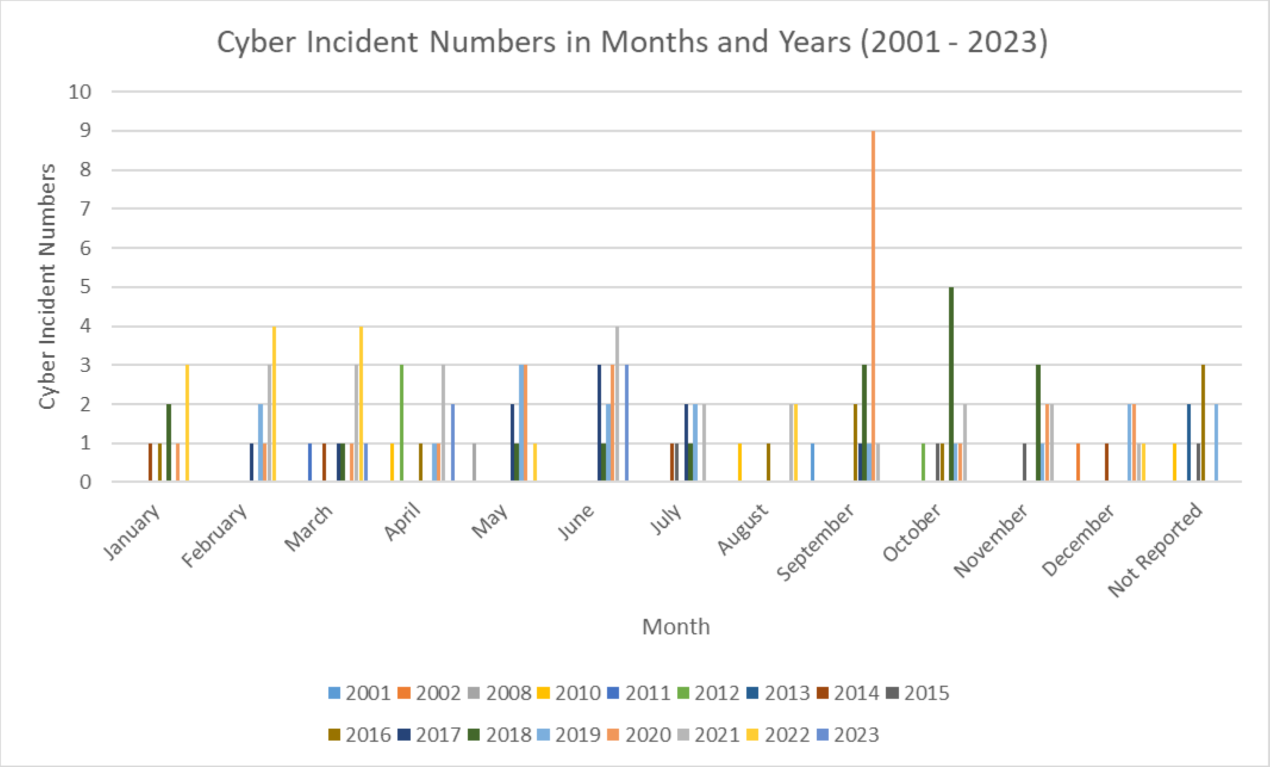


Figure 3. Maritime cyber incidents in months and years (2001-2023)

Cyber-attacks have affected many different stakeholders in the maritime industry. When the data is examined, it can be said that there is a more intense land-based attack on the maritime sector. However, we should not neglect the connection of ships with the land. In other words, it should not be forgotten that when a cyber-attack occurs against the maritime companies responsible for the ships in service, the ships they operate may also be affected by these attacks. At the same time, cyber-attacks on third parties working in cooperation with ships and shipping companies can affect both shipping companies and the ships they operate.

Maritime stakeholders exposed to cyber-attacks are shown in Figure 4. If we list the ones most affected by the attacks, vessels, shipping companies, ports, navy vessels, and shipbuilders are the parties most affected by cyber-attacks. Different actors of the maritime sector such as marine insurance, broker, salvage, offshore, coastguard, port authority are also affected by these attacks. These actors in the maritime sector are in close relationship with and influence each other. Therefore, it is one of the important cyber situational awareness that should not be forgotten that cyber-attacks on one of these actors may also affect other stakeholders.

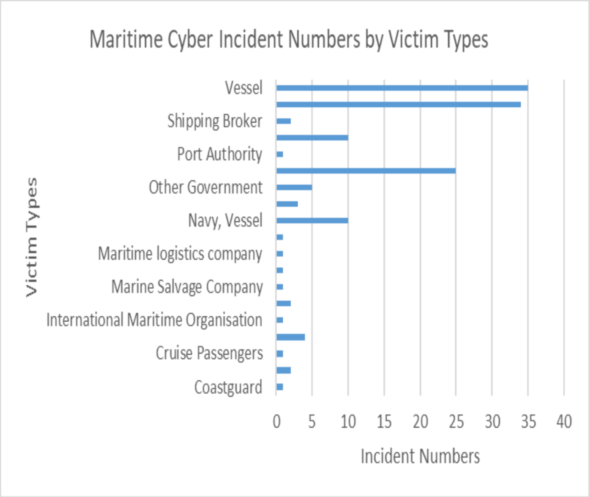


Figure 4. Maritime cyber incident numbers by victim types

In Figure 5, the analysis results of the maritime sector actors most affected by cyber-attacks are given according to their countries. In total, 43 countries were affected by maritime cyber-attacks. But the country most affected by these attacks is the USA. South Korea and the United Kingdom follow next. When the list is examined, it can be explained that actors in the world such as Russia-Ukraine, South Korea-North Korea, USA-Iran-China, who experience attacks and conflicts among themselves, are more affected by cyber-attacks than other countries.

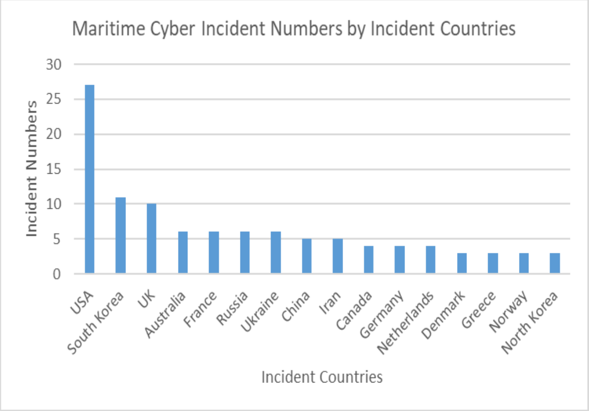


Figure 5. Maritime cyber incident numbers by countries where the incident took place

When we look at the types of cyber-attacks on the maritime industry, it is recorded that ransomware attacks occur the most (Figure 6). The maritime industry is one of the sectors where costs are intense, and planning and timing are important. The closure of the Suez Canal caused by the Ever given ship caused global shipping worth $10 billion to stop. It is obvious that the maritime industry will attract attackers because it is a sector that involves such high costs. Therefore, performing cyber-attacks on the information and operational systems of maritime industry stakeholders and demanding ransom for the systems to work again is a more popular type of cyber-attack among cyber attacker actors.

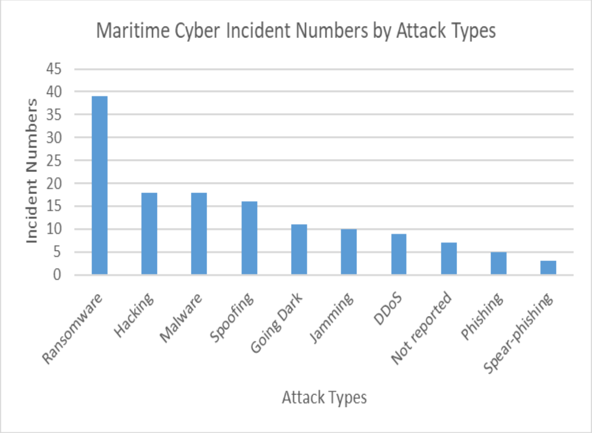


Figure 6. Maritime cyber incident numbers by cyber-attack types

When cyber-attacks against ships are analyzed, Spoofing, Jamming and Going Dark cyber-attacks lead the way. Spoofing attacks are carried out to manipulate AIS and GPS, including location and identities (Figure 7). The U.S. Maritime Administration sent a fairly ordinary safety advisory about GPS disruption in the Black Sea, nevertheless, the consequences were extensive. Commercial boats had substantial GPS errors, with several vessels displaying their location many miles onshore instead of being offshore. Several boats had similar problems, since their AIS systems displayed inaccurate vessel positions. The analysis indicates intentional manipulation of GPS signals, most likely achieved via the use of illegal jammers that are easily accessible on the internet. This occurrence highlights the susceptibility of GPS systems to manipulation, which raises issues over the safety of marine navigation and the availability of disruptive technologies.

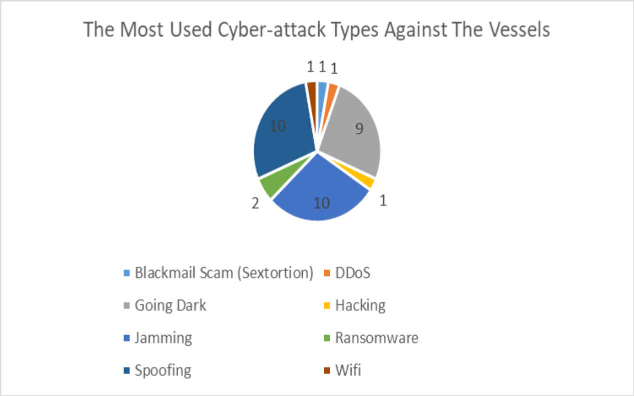


Figure 7. The most used cyber-attack types against the vessels

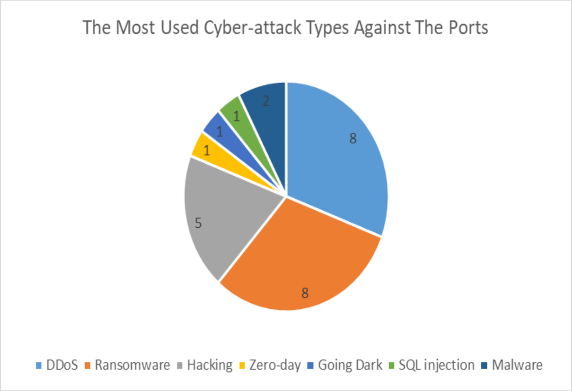


Figure 8. The most used cyber-attack types against the ports

In Figure 8, there are a total of 25 attacks against ports (One attack is both DDoS and malware). Ransomware, DDoS and Hacking cyber-attacks are the leading types of these attacks. Ports are one of the maritime infrastructures that play a critical role in carrying out the operations of ships. Therefore, attacks against them disrupt the operations of ships, disrupt global shipping, and endanger the maritime security of countries. In 2021, Transnet, the port operator in South Africa, invoked force majeure due to a ransomware assault that caused a complete shutdown of its IT systems and impacted container operations at many ports, including Durban, Cape Town, and Port Elizabeth in February 2022, a ransomware assault occurred at ports located in Germany, Belgium, and the Netherlands, resulting in the disruption of oil terminal operations and the incapacitation of port systems.

5. DISCUSSION

The analysis applied in the methodology section is reliable enough to make such specific conclusion because of several reasons - i.e. reliability and relevance of data source, transparency in comprehensiveness with which data has been analyzed, categorization & visualization techniques used, and its contribution for literature. MCAD an data source that is reliable and of utmost importance as this was created by NHL Stenden University of Applied Sciences in order to collect all information about the cyber-attacks in maritime domain. MCAD provides a detailed documentation of maritime cyber incidents between the years 2001 and up to 2023, therefore offering ample information on changes in cyber threats over time within the maritime sector. Database for maritime cyber-attacks is a major gap in the current academic literature, and it makes use of such a specialized and pertinent dataset render this study even more credible. Additionally, it being multi-dimensional approach i.e., to check not only type of incident but also the crime victim and country regional spread. These multi-dimensional categories enable the capture of both breadth and depth when considering cyber threats to shipping. This means that this paper does not simply reveal the top line or lay only superficial, toplining bare bones open for comparisons and contrasts about cyber-attack vulnerabilities in the critical infrastructure sector. By identifying and visualizing the data based on area like year, month, country-wise distribution of cyber-attack tells how these two different maritime sectors face potential attacks in their nature. Moreover, the categorization and breakdown of these threats over time offer a new understanding to maritime cyber risks that improves academic discourse as well as operations. This assists in the recognition of which actors are predominantly at higher risk by comparing incidents across various months, years and classifying it based on attack / victim type providing a good idea of its threat landscape. Decision-makers can use these visualizations to identify deep-rooted trends and advice their maritime cyber security policy.

This study on maritime cyber security incidents sheds lights upon some significant trends that reveal present day vulnerabilities and threats. Although improving operational efficiency, the growing digitalization of maritime systems has also given rise to more frequent and advanced cyber-attacks in this domain. The results confirm the gradual increase in cyber incidents seen over time, with a peak during COVID-19 and signs that an increased awareness of the threats including improved security measures has led to some decrease as well but also shows how maritime is challenged because of new form factors or cyber risk.

The research also contributes to such literature by adding the finer-grained geographical distribution of cyber-attacks and specific impact on various actors in the maritime industry, such as vessels, shipping companies, and ports. Indeed, attacks in countries such as the USA, South Korea, and the United Kingdom confirm scholarship done by scholars like Capano (2021), which shows the increase of geopolitical tension manifested in the cyber domain with state-sponsored cyber operations against critical maritime infrastructure.

These findings have important implications for stakeholders in the maritime industry. The study outlines the urgent need for closer international cooperation in the sharing of threat intelligence and actual development of uniform cyber security standards. Since the maritime systems are becoming increasingly interconnected, fragmented or isolated security methods will just not work. The patterns of the study will be important to inform future cyber defense strategies and policies, taking into consideration the seasonal peaks that cyber-attacks usually take place and the type of actors most targeted. The ability to learn from incidents in the past, coupled with adapting to the shifting threat landscape, determines the capacity to predict and prevent cyber-attacks.

6. CONCLUSION

The maritime sector, like all other sectors, is affected by digital transformations. As systems shift towards automation and their connections with each other over the network are increasing, the presence of cyber-attack actors in the maritime sector is mentioned. The source of finance, especially in the maritime sector, attracts cyber attackers. On the other hand, those who are attacked meet the demands of cyber attackers in order to avoid disruptions in their planning and loss of reputation in the sector.

In this study, cyber-attack data on the maritime sector between 2001 and 2023 from the Maritime Cyber-Attack Database (MCAD) provided by NHL Stenden University of Applied Sciences were examined in order to analyze cyber-attacks on the maritime sector. According to these investigations, cyber-attacks that started in 2001 reached their peak especially during the COVID19 pandemic. It shows a decreasing trend due to increasing awareness in the sector, regulations, guidebooks, and guidance from international organizations. When looked at by month, most attacks occur in September and June. September 2020 was the period when these attacks were most intense. When the victim groups are examined, ships, maritime companies and ports are the maritime sector actors that were most exposed to cyber-attacks. When examined in the victim countries category, the USA was most exposed to cyber-attacks. In the category of cyber-attack types, ransomware is at the top. While cyber-attacks against ships are spoofing and jamming, these attacks are observed as DDoS and ransomware in ports.

To sum up, many aspects have examined in order to understand the incentives behind cyber attackers and to guide stakeholders in the maritime sector towards implementing effective cyber security strategies and practices to prevent such cyber-attacks.

For further studies, it can be proposed correlation analyses between attack types and victim types, as well as time series analyses to further explore the trends in cyber-attacks over time. These enhancements would build on the existing methodology without undermining the conclusions drawn from the data thus far.

AUTHORSHIP CONTRIBUTION STATEMENT

Emre DÜZENLİ: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing. **Gizem KAYİSOGLU:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing, Review and Editing, Visualization, Supervision. **Tayfun ACARER:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing, Review and Editing, Visualization, Supervision. **Pelin BOLAT:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing, Review and Editing, Visualization, Supervision. **Ayşe NAK:** Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing-Original Draft, Writing.

CONFLICT OF INTERESTS

The authors decelerate that they have no conflict of interest.

ETHICS COMMITTEE PERMISSION

No ethics committee permissions are required for this study.

FUNDING

This work was funded by Istanbul Technical University, Scientific Research Projects, General Research Project, which is titled as "Penetration Test Application and Analysis for ECDIS Cyber Security" with 44740 project code.

ORCID IDs

Emre DÜZENLİ:
https://orcid.org/0009-0009-5179-1627
Gizem KAYİSOGLU:
https://orcid.org/0000-0003-2730-9780
Tayfun ACARER:
https://orcid.org/0000-0003-2407-5552
Pelin BOLAT
https://orcid.org/0000-0003-4262-3612
Ayşe NAK:
https://orcid.org/0000-0003-2937-7007

5. REFERENCES

Androjna, A., Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science*, 10(2): 361–373. doi:10.7225/toms.v10.n02.w08.

Ben Farah, M.A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., Bellekens, X. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information (Switzerland)*, 13(1). doi: 10.3390/info13010022.

Bernsmed, K., Frøystad, C., Meland, P.H., Nesheim, D.A., Rødseth, Ø.J. (2017). Visualizing Cyber Security Risks with Bow-Tie Diagrams. International Workshop on Graphical Models for Security, p. 38–56.

Bolat, P., Yuksel, G., Uygur, S. (2016). A Study for Understanding Cyber Security Awareness Among Turkish Seafarers. GMC2016 - II.Global Conference On Innovation In Marine Technology And The Future Of Maritime Transportation, p. 278–289.

Capano, D.E., Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk Industrial Cyber Security Pulse, (2021). Accessed Date: 08.05.2024, https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/ is retrieved.

Davis, G., Garcia, A., Zhang, W. (2009). Empirical Analysis of the Effects of Cyber Security Incidents. *Risk Analysis*, 29(9): 1304–1316. doi: 10.1111/j.1539-6924.2009.01245.x.

Iaiani, M., Tugnoli, A., Bonvicini, S., Cozzani, V. (2021). Analysis of Cybersecurity-related Incidents in the Process Industry. *Reliability Engineering & System Safety*, 209: 107485. doi: 10.1016/j.ress.2021.107485.

Kaneko, T., Yoshioka, N., Sasaki, R. (2021). Cyber-Security Incident Analysis by Causal Analysis using System Theory (CAST). 2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 806–815. doi: 10.1109/QRS-C55045.2021.00123.

Karas, A. (2023). Maritime Industry Cybersecurity: A Review of Contemporary Threats. *European Research Studies Journal*, 26(4): 921–930. doi: 10.35808/ersj/3336.

Kyriakides, H. Marine cyberattacks: Analysis of liability and IMO 2021, (2021). Accessed Date: 17.05.2024, https://www.legal500.com/developments/thought-leadership/marine-cyberattacks-analysis-of-liability-and-imo-2021/ is retrieved.

Mednikarov, B., Tsonev, Y., Lazarov, A. (2020). Analysis of Cybersecurity Issues in the Maritime Industry. *Information & Security: An International Journal*, 47(1): 27–43. doi: 10.11610/isij.4702.

Meland, P.H., Bernsmed, K., Wille, E., Rødseth, J., Nesheim, D.A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav*, 15(3): 519–530. doi: 10.12716/1001.15.03.04.

Mraković, I., Vojinović, R. (2019). Maritime cyber security analysis – How to reduce threats? *Transactions on Maritime Science*, 8(1): 132–139. doi: 10.7225/toms.v08.n01.013

NHL STENDEN University of Applied Science, (2001). Maritime Cyber Attack Database (MCAD), NHL Stenden University of Applied Science.

Patterson, C.M., Nurse, J.R.C., Franqueira, V.N.L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, 132: 103309. doi: 10.1016/j.cose.2023.103309.

Schwarz, M., Marx, M., Federrath, H. (2021). A Structured Analysis of Information Security Incidents in the Maritime Sector. ArXiv Preprint ArXiv:2112.06545.

Silverajan, B., Vistiaho, P. (2019). Enabling Cybersecurity Incident Reporting and Coordinated Handling for Maritime Sector. 2019 14th Asia Joint Conference on Information Security (AsiaJCIS), pp. 88–95. doi: 10.1109/AsiaJCIS.2019.000-1

Söner, Ö., Kayisoglu, G., Bolat, P., Tam, K. (2023). Cybersecurity risk assessment of VDR. *Journal of Navigation*, 1–18. doi: 10.1017/S0373463322000595.

Tam, K., Jones, K.D. (2019). Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector. *International Journal on Cyber Situational Awareness*, 4(1): 40–68. doi: 10.22619/ijcsa.2019.100125.

Research Article
Turkish Journal of Maritime and Marine Sciences

DOI: 10.52998/trjmms.1523871
Volume: 10 Special Issue: 1 (2024) 62-80

The Share of Data in Maritime Communications is Increasing

Deniz Haberleşmesinde Datanın Payı Artıyor

Türk Denizcilik ve Deniz Bilimleri Dergisi

Cilt: 10 Özel Sayı: 1 (2024) 62-80

Tayfun ACARER[1,*]

[1]*Piri Reis University, Maritime Vocational School, Istanbul*

ABSTRACT

Communication is of great importance for the safe and delay-free navigation of ships. Especially life/property safety, navigational warnings, weather forecast reports, storm warnings, navigation maps, etc. Timely transmission of information to ships is only possible with effective maritime communications. In addition, communication is of great importance in making appropriate navigation plans based on the information received from the ships. In recent years, the share of data communication in individual and corporate communications has been increasing. In order to benefit from the great conveniences and opportunities provided by data communication in maritime communication systems, very radical decisions have recently been taken within IMO. These regulations made at the international level paved the way for data communication in close-range maritime communication systems. In line with these regulations, broadband data communication between the ship and the land will begin to be made via VHF devices in the next few years. Another development that will improve broadband data communication in maritime communication systems has been in Near Orbit Satellite systems. The technical features of these systems, the number of which has been increasing in recent years, are extremely suitable for data communication between ship and land. Among these, the Starlink system completes its network in space faster than other satellite systems. It is inevitable that the Starlink system, whose global satellite structure will be completed to a large extent by the end of 2025, will be used to a large extent in data communication between ships and land and between ships with each other. With the use of broadband data feature in the near future, it will be possible for ships to navigate much more safely, efficiently and with a reduced risk of accidents. For this purpose, maritime enterprises, ship personnel and land units must be informed about these developments and their communication infrastructure must be established by taking these systems into consideration.

Keywords: Maritime communications, Maritime businesses, Ship management, Broadband data communication, Maritime trade.

Article Info
Received: 29 July 2024
Revised: 05 September 2024
Accepted: 09 September 2024

[*] (corresponding author)
E-mail: tacarer@hotmail.com

To cite this article: Acarer, T. (2024). Effects of Developments in Data Communication on Ships on Maritime Trade, *Turkish Journal of Maritime and Marine Sciences*, 10 (Special Issue: 1): 62-80. doi: 10.52998/trjmms.1523871.

ÖZET

Gemilerin emniyetli ve gecikmeksizin seyirleri için haberleşmenin önemi çok fazladır. Özellikle can/mal emniyeti, seyir uyarıları, hava tahmin raporları, fırtına ihbarları, seyir haritaları, vb. bilgilerin gemilere zamanında iletilmesi ancak etkin bir deniz haberleşmesi ile mümkündür. Ayrıca gemilerden alınacak bilgilere göre uygun seyir planlarının yapılmasında da haberleşmenin önemi çok fazladır. Son yıllarda bireysel ve kurumsal iletişimde data haberleşmesinin payı giderek artmaktadır. Veri iletişiminin temin ettiği büyük kolaylıklardan ve olanaklardan deniz haberleşme sistemlerinde de azami ölçüde yararlanılabilmesi için yakın süreçte IMO bünyesinde çok radikal kararlar alınmıştır. Uluslararası düzeyde yapılan bu düzenlemeler ile yakın mesafe deniz haberleşme sistemlerinde data iletişiminin önü açılmıştır. Söz konusu düzenlemeler doğrultusunda önümüzdeki birkaç yıl içinde VHF cihazları üzerinden gemi kara arasında genişband veri haberleşmesi yapılmaya başlanacaktır. Deniz haberleşme sistemlerinde genişband veri haberleşmesini geliştirecek diğer bir gelişme Yakın Yörünge Uydu sistemlerinde olmuştur. Son yıllarda sayıları giderek artan bu sistemlerin teknik özellikleri gemi kara arasındaki veri haberleşmesi için son derece uygundur. Bunlar içinde Starlink sistemi diğer uydu sistemlerine göre uzaydaki şebekesini daha hızla tamamlamaktadır. 2025 yılı sonunda çok büyük oranda global uydu yapısı tamamlanacak olan Starlink sisteminin gemi kara arasında ve gemilerin birbirleri ile yapacakları data iletişiminde çok büyük oranda kullanılması kaçınılmazdır. Önümüzdeki yakın süreçte genişband veri özelliğinin kullanılması ile birlikte gemilerin çok daha güvenli, verimli ve kaza riski azaltılarak seyir yapmaları mümkün olacaktır. Bunun için deniz işletmelerinin, gemi personelinin ve kara birimlerinin söz konusu gelişmeler konusunda bilgilendirilmeleri ve iletişim alt yapılarını bu sistemleri de dikkate alarak tesis etmeleri gerekmektedir.

Anahtar kelimeler: Deniz Haberleşmesi, Deniz İşletmeleri, Gemi Yönetimi, Geniş Bant Veri İletişimi, Deniz Ticareti

1. INTRODUCTION

New developments that emerge every day in the IT sector leads to serious changes in the maritime sector, as in many other sectors. The possibilities provided by new communication systems range from ship bridge navigation systems to ECDIS, AIS, VDR, RADAR, etc. (Kayisoglu *et al.*, 2023). It provides very positive capabilities in the capabilities of electronic navigation aids and communication systems. Major developments, especially in data communications, inevitably lead to major changes in maritime communication systems. Maritime communication, which was previously done manually with conventional systems, later started to be done through automatic systems (Ekinalan, 2020). But in recent years, in parallel with the great development in the IT sector, maritime communication systems have also undergone serious structural changes.

One of the most radical changes in this form of communication in recent years has been the emergence of a differentiation similar to the development in broadband data communication in the IT sector. While written communication, especially in the maritime communication sector, was previously carried out in Morse, later with the developing technology, written communication turned into telex communication. Then narrow band data communication began to be made for the first time using Inmarsat systems (Demir, 2009). Although such studies dealing with broadband data of ship systems have been missing in the literature in recent years, today the emergence of new technologies and devices working in these technologies has paved the way for broadband data communication in maritime communications (Kayisoğlu, 2024).

A series of regulations have recently been made by IMO (International Maritime Organization) in order to start broadband data communication between ships and ship/land via different communication systems and with different features (Acarer, 2023). In addition, different alternatives have emerged in this regard with some new technologies that have become operational recently, and especially with near-orbit satellite systems. It is of great importance for the relevant parties of the maritime industry that the said facilities/capabilities and the features of these systems are known by both maritime companies, ship employees and port/cargo officials, and that these opportunities are utilized to the maximum extent.

In addition, in the article, the broadband data communication in question is used for ships' reporting, meteorological data, navigation maps, etc. It was emphasized that the speed and convenience it will provide for many important types of communication will make a very positive contribution to the safety of life and property in addition to the safe navigation of ships.

The remainder of this article is structured as follows. In Chapter 2, the materials and methods of the research are given. In Chapter 3, the findings obtained in this research are presented. In Chapter 4, the effects of new technologies on data communication at sea are discussed, according to the findings obtained in the research. In Chapter 5, the research in the article is concluded.

2. MATERIALS AND METHODS

In this study, first of all, it is emphasized that the share of data communication in the activities of both individual and corporate users is increasing and today, the transmission method of many correspondences, meetings and reports is explained as data communication.

In particular, the contribution of the convenience and benefits provided by this form of communication to the development of data communication is discussed. Then, the devices that must be kept on ships in different voyage zones by the GMDSS (Global Maritime Distress and Safety System) legislation, which determines maritime communication obligations, are presented as a table, and the systems in this table that can be used in data communication are evaluated separately. After explaining the features of the existing devices in the table in question, which are also defined as conventional systems, and the possibility of their use in data communication, information about new systems that can provide broadband data communication is given. The ability of these systems to be used in high-speed data communication in maritime systems was examined, especially considering their bandwidth and speed.

In this study, it is explained that sending large amounts of data with minimum delay is impossible with current maritime communication systems and that this will only be possible with broadband data communication. For this purpose, the decisions taken in the recent past within the IMO to enable ships to communicate with broadband data are explained and the importance of this issue in international maritime transportation is emphasized.

In addition, recent decisions taken by IMO for broadband data communication of ships were announced and the importance of this issue regarding international maritime transportation was drawn. The fact that the first regulation made by IMO on this subject was made on VHF, the most commonly used communication system on ships, was evaluated as an indication of the importance IMO attaches to this issue. Meanwhile, since Near Orbit Satellite systems are seen as the most suitable among the developing technologies related to broadband data communication in recent years, this issue has been discussed separately and the contribution of these systems to broadband data communication has been examined in detail. It is pointed out that the initial installation and communication costs of these systems are very low compared to existing systems, and the contribution that advances in this field will provide the communication environment of ships is explained in detail.

3. FINDINGS

Although many systems are used in maritime communication today, they generally have different structures from each other. All of these systems, which have different features, work in the form of radio communication and have two main structures: terrestrial and satellite systems. Marine communication devices, defined as Terrestrial systems, operate either as direct communication between ship-land or ships (such as VHF systems) or as electromagnetic waves reflected from the ionosphere (as in HF systems). In medium distance systems (Medium Frequency- Medium Wave), communication is carried out as Ground Waves.

In satellite systems, which is another type of maritime communication, communication between ship to ship and ship to land is provided through satellites. These non-terrestial systems should be considered differently from terrestrial systems (Gul *et al.*, 2024). Inmarsat and Cospas Sarsat satellite systems are used in this form of communication (Demir, 2009). Today, while commercial communication and danger/safety type communications are generally established through the Inmarsat system, only life/property safety and distress communications are provided through the Cospas Sarsat satellite system. While Inmarsat communication is commercial and requires a fee, distress communication using the Cospas Sarsat system is free.

It is not possible to transmit broadband data with minimum delay with these systems.

3.1. Terrestrial Marine Communication Systems

VHF system is the most intensive way of Terrestrial Marine Communication. The most important feature of this is that it is the most used system in voice communication between ship to ship and ship to land. The VHF system works on the principle that the antennas of these devices see each other directly. The frequency band used n VHF communication has been determined as 156-174 MHz by the International Maritime Organization (ITU) (Korkmaz, 2002).

The other terrestrial maritime communication system is Medium Wave devices (MF), and these devices have a medium distance (approximately 150-200 nautical miles) coverage area. In this system, a form of communication called Ground wave is used.

In Long Distance (High Frequency) radio systems, which is another type of Terrestrial Marine Communication system, communication between devices is carried out through waves reflected from the ionosphere. Since the ionosphere is naturally reflective, this type of communication is considered a very safe form of communication in strategic terms. In the HF system, different frequency bands are used between communicating devices according to day/night hours (Ekinalan T., 2020). In accordance with the GMDSS obligation, DSC terminals used with HF devices can also provide automatic communication to Long Distance systems.

3.1.1. Very High Frequency (VHF) System

Very High Frequency (VHF) System, communication is made on the principle that the antennas of VHF devices see each other optically, so this form of communication between ships is free. DSC (Digital Selective Calling) terminals working with VHF devices provide these devices with automatic calling capability for both routine communication and distress/safety calls.

Max. power 25 W, min. Its power is 1 W (Atmaca, 2009). Since VHF devices in Coastal Radio stations are generally installed in high places such as hills and mountains on the coastline, the coverage area of these stations is much greater than the VHF communication established between two ships, depending on the height at which they are installed. This distance is determined by the formula below.

The figure below shows graphically the VHF short distance maritime communication between ship-ship and ship-shore stations and the distance of this communication in nautical miles. This distance is determined by the formula below.

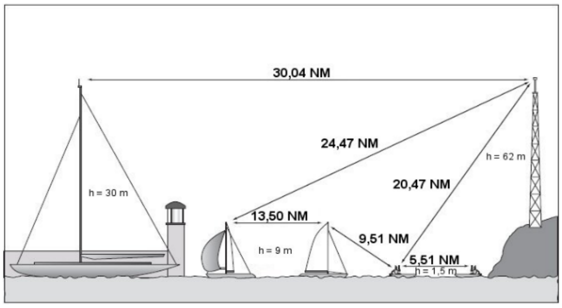


Figure 1. Distances between VHF devices (Ekinalan, 2020).

In the figure above, "h_1" and "h_2" show the heights above sea level of the antennas of VHF devices on ships.

"l" is the distance between the antennas of VHF devices on ships in nautical miles (nm).

$$l = 4.1 \times \left[\sqrt{h_1} + \sqrt{h_2} \right] (m) \quad \text{or}$$
$$l = 4.1 \times \left[\sqrt{h_1} + \sqrt{h_2} \right] (nautical\, mile) \tag{1}$$

In this formula;
l: communication distance
h_1 and h_2; These are the heights of the antennas on VHF devices (two different VHF Devices) above sea level in meters. (1 nautical mile=1852 m)
According to this formula, the coverage area of VHF communication between two ships is calculated as approximately 25 nautical miles (Demir, 2009).
Accordingly; the communication distance between a marine vessel with a VHF antenna 30 m above sea level and a VHF system (for example, a device in a coastal radio station) on the shore with an altitude of 62 m above sea level is;

$$\begin{aligned} &l = 2{,}21 \times [\sqrt{h_1} + \sqrt{h_2}] \\ &l = 2{,}21 \times [\sqrt{30} + \sqrt{62}] \\ &= 2{,}21 \times [5{,}477 + 7{,}84] \\ &= 2{,}21 \times 13{,}317\ nM \\ &l = 29{,}43\ nM \sim 30\ nM\text{‘dir.} \end{aligned} \tag{2}$$

Again, if the antenna heights of the VHF systems of the two marine vessels are shown in the figure above and are quite low at sea level (the height of the antennas of the VHF systems of both vessels is "9 m" above sea level), the communication distance of these two VHF devices is;

$$\begin{aligned} &l = 2{,}21 \times [\sqrt{h_1} + \sqrt{h_2}] \\ &l = 2{,}21 \times [\sqrt{9} + \sqrt{9}] = 2{,}21 \times [3 + 3] \\ &= 2{,}21 \times 6\ nM \\ &l = 13{,}26\ nM \sim 13{,}5\ nM\text{‘dir.} \end{aligned} \tag{3}$$

With the regulations made within IMO in recent years, it is aimed to provide data communication in VHF devices. For this purpose, duplex channels (channels with different receiving and sending frequencies) in the VHF system are allocated for data communication (ITU, Final Acts., 2019). These regulations aim to ensure data transmission in close-range wireless maritime communication and to provide this written communication free of charge or at a very low cost.
Another VHF system used under GMDSS legislation is Handheld VHF. (Portable VHF) Since the coverage area of handheld VHFs is less than 1 km, these devices are mostly used for in-ship voice communication and during cargo handling in ports (Acarer, 2018). Currently, Portable VHF devices cannot communicate with data.

3.1.2. MF and HF Systems

Another device that is compulsorily installed on ships due to GMDSS obligations is MF. In addition to voice communication through these devices, automatic communication between DSC terminals and ships and between ship and land is also possible. Although DSC technology provides automatic data communication to VHF, MF and HF devices, mutual broadband data and internet communication cannot be made between these devices.
In addition, since the width of the channels used in medium distance systems is 3 KHz (Ekinalan, 2020) more than one MF channel must be combined to enable data communication through this system. Since there is still no regulation made by IMO on this issue, there is no possibility of data communication in the MF band in the near future.
In long distance wireless systems, transmission is made between the receiver and transmitter units through waves reflected from the ionosphere. Since there are no satellites etc. and completely natural reflectors are used, this system is extremely safe from a strategic point of view. Since different bands are used in the long-distance system, the distance to the communicating units also includes different distances depending on these band values and day/night hours.

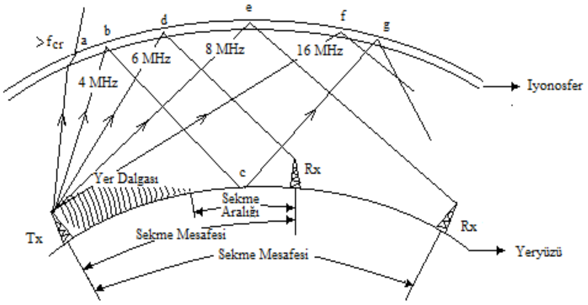


Figure 2. Different Frequency Bands Used in HF System (Ekinalan, 2020).

Again, IMO has not allocated channels for data communication in HF systems, as in MF. There is still no regulation or planning in the short term on this issue. Again, since the channel width in the HF band is determined as 3 KHz, it will be necessary to bring together many more channels than VHF for broadband data communication to reach the required channel width for broadband. (Carrier Aggregation)

Although this process is theoretically possible, it is impossible to implement in practice because dozens of HF channels would need to be combined to achieve the required channel width for wideband.

3.1.3. Navtex System

Navtex is a device that is mandatory on all ships related to the Terrestrial Marine Communication System. This device is a receiver only on ships and is a device where one-way broadcasts made by Coastal Radio stations are received and automatically recorded. Since this system, which operates in the medium wave band, contains extremely important information for the safe navigation of ships, Navtex devices are mandatory on all ships. Since this system involves broadcasting from land to ships, there is no possibility of mutual communication between ship/land units.

For this reason, it is not possible to benefit from broadband data communication from Navtex devices on ships.

3.2. Satellite Systems

Other wireless communication systems that, must be kept on ships in accordance with GMDSS rules are Satellite equipment. Some of these are required to be installed on ships only for distress and safety purposes, while some (such as the Cospas Sarsat satellite system) are devices capable of voice and internet communication. Although there are terminal devices with many different features in the Inmarsat satellite system (such as the Inmarsat satellite system), the only devices that can perform distress communication and therefore fulfill GMDSS obligations are the Inmarsat C and Inmarsat F77 satellite terminals.

Although voice communication is still not possible with Inmarsat C, written communication and long-distance navigation safety broadcasts (Enhanced Group Call-EGC) are possible. With Inmarsat F77, both voice and low-speed data communication can be provided (Ekinalan, 2020).

3.2.1. Inmarsat System

Designed as the International Maritime Satellite system and briefly defined as Inmarsat, the establishment target of the satellite system is maritime communication services. In the following years, land and air satellite communication services began to be provided through this system. Inmarsat satellites were designed as Geostationary Earth Orbit (GEO) satellites and launched into orbit at an altitude of 36,000 km. Figure 3 shows the names of long-distance Inmarsat satellites and areas they cover (INMARSAT, 2012).

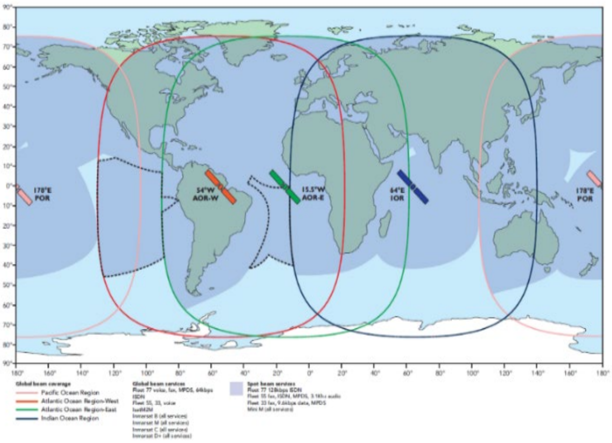

178°E POR
54°W AOR-W
15.5°W AOR-E
64°E IOR
178°E POR
Global beam coverage
Pacific Ocean Region
Atlantic Ocean Region-West
Atlantic Ocean Region-East
Indian Ocean Region
Global beam services
Fleet 77 voice, fax, MPDS, 64kbps ISDN
Fleet 55, 33, voice
IsatM2M
Inmarsat B (all services)
Inmarsat M (all services)
Inmarsat C (all services)
Inmarsat D+ (all services)
Spot beam services
Fleet 77 128kbps ISDN
Fleet 55 fax, ISDN, MPDS, 3.1kHz audio
Fleet 33 fax, 9.6kbps data, MPDS
Mini M (all services)

Figure 3. Inmarsat Satellites (INMARSAT, 2012).

There are 4 Geostationary Inmarsat satellites these are.

- AOR - E (Atlantic Ocean Region East)
- AOR - W (Atlantic Ocean Region West) is the satellite of the Atlantic Ocean Region West.
- IOR (Indian Ocean Region)
- POR (Pacific Ocean Region)

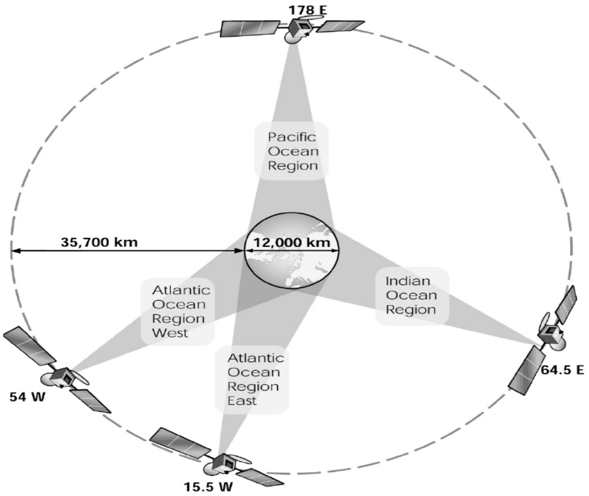


Figure 4. Locations of satellites& the distance from Earth (Yılmaz, 2014).

The main forms of communication using the Inmarsat system are;
- Voice,
- Emergency communication,
- Narrowband data communication and
- M2M (Machine to Machine) access.

Many different terminals are used on ships in M2M communication and narrowband data communication. Although there are many Inmarsat terminals, only Inmarsat C and Fleet 77 are compatible with GMDSS. Among these, data communication can be made especially through Inmarsat C and Fleet 77 terminals. Among these, Inmarsat C has a speed of 600 Bits and is quite slow. Data communication up to 64 kbps is possible via Inmarsat Fleet (ITU, 2013).
These terminals are;
- BGAN M2M
- BGAN Broadband Global Area Network
- IsatData Pro Terminal (ISATM2M)
- Isatdata Pro
- Inmarsat Fleet Services

Since the channel width allocated to this device is small, only narrowband data communication is possible. Therefore, it is not possible to perform wideband data communication with Inmarsat C and other Inmarsat devices.

3.2.2. Cospas Sarsat System

Cospas-Sarsat satellite system is an international organization with members of 45 countries, including Turkey. The purpose of this organization is to detect the position and identity of the marine vessel through radio transmitters (EPIRB - Emergency Position Identification Radio Beacon) activated in distress situations of the ships and to inform the relevant units in different countries. In such a danger situation, after the distress signal sent from EPIRB devices on ships, search and rescue units in the nearest country are notified and search and rescue process is initiated.
These orbits are mainly**.**
- Low-altitude Earth Orbit-LEO,
- Medium orbit (Medium-Altitude Earth Orbit-MEO),
- It is a fixed distant orbit. (Geostationary Earth Orbit-GEO)

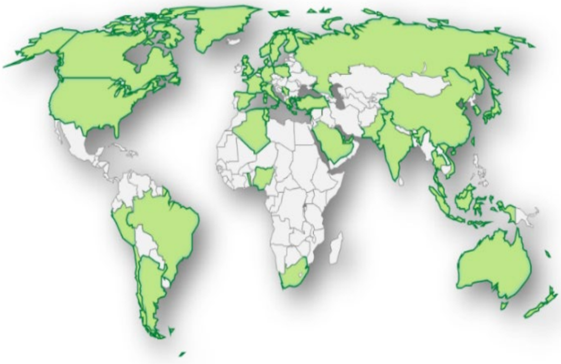


Figure 5. Cospas Sarsat Satellite System (Participants shown in green) (Cospas-Sarsat., 2023)**.**

In the Cospas-Sarsat satellite system, the signal sent from the EPIRB devices for the ship in distress is first sent to the satellite and from there to Satellite Ground stations in different countries called LUT (Local User Terminal). This information coming to the LUT is then sent to the unit defined as the Mission Control Center (MCC), and from there to the Search and Rescue Center (RCC) of the country closest to the EPIRB where the distress broadcast is broadcast. RCCs, who are informed of the distress, initiate the rescue function by notifying the Search and Rescue (SAR) units as soon as possible. Cospas-Sarsat satellite orbits in different orbits are shown below.

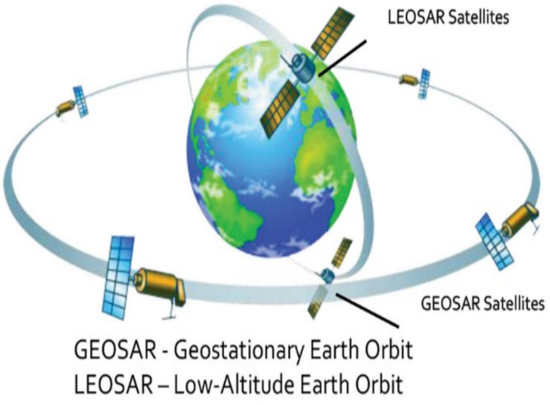

LEOSAR Satellites
GEOSAR Satellites
GEOSAR - Geostationary Earth Orbit
LEOSAR – Low-Altitude Earth Orbit

Figure 6. LEOSAR and GEOSAR Orbits (International Civil Aviation Organization, 2023)

In the Cospas-Sarsat system, only EPIRB devices are used on ships. Since the channel range used in this system is very narrow, it is not possible to establish wideband data communication with EPIRB devices on ships.

3.3. Mandatory Devices on Ships According to International Legislation

Decisions regarding inter-ship and ship/land communications are taken at regular meetings under the coordination of the International Maritime Organization. From time to time, these decisions are collected under different headings and turned into a set of rules. The most important and well-known set of decisions regarding maritime communications is "SOLAS" (Safety Of Life At Sea Convention) and GMDSS, which is a part of it. (Global Maritime Distress and Safety System) With these and similar regulations, which devices will be installed on ships depending on the regions they sail to and their tonnage, the qualifications of the personnel who will use them, the types of licenses, the features of the devices in question, how many of them will be kept on the ship, etc. obligations have been introduced. As long as developments in technology continue, it will be inevitable for these regulations to continue.

The most important body of legislation that still maintains its validity regarding maritime communications and determines the obligations of ships regarding maritime communications is GMDSS. The authorization of marine vessels, their inspections in ports, the types of licenses of the personnel who will use the communication devices, the maintenance/handling obligations that these personnel have to carry out regarding the devices, their testing and control processes, and the procedures and principles regarding communication are explained in detail in these regulations.

The table below shows the communication devices and their features that must be available on ships operating in different voyage zones according to IMO regulations, depending on tonnage (Ekinalan, 2020). All member countries of IMO must fulfil their obligations in this legislation and equip their ships accordingly.

Table 1. GMDSS Regions and Mandatory Equipment (Ekinalan, 2020).

	A1	**A2**	**A3 (INM)**	**A3 (HF)**	**A4**
VHF DSC	X	X	X	X	X
POR. VHF	X	X	X	X	X
EPIRB	X	X	X	X	X
SART	X	X	X	X	X
NAVTEX (RX)	X	X	X	X	X
MF DSC (TLF/DSC)	X	X	-	-	-
HF DSC (TLF/DSC/TLX)	-	-	-	X	X
EGC	-	-	X	X	-
INM (C/77)	-	-	X	-	-

As can be seen from the table above, some of the devices in different voyage areas are Terrestrial, as explained in the previous articles, and some are Satellite systems. While some of the devices in question are used only for distress/safety communication, some are installed on ships for both distress and commercial/routine communication purposes. Again, it is not possible to establish broadband data communication with the devices listed in this table and kept on ships as required by legislation.

3.4. New Generation Low Orbiting Satellite Systems

Until recently, communication satellites were designed as Very High Geostationary Orbit satellite systems. (Geostationary Earth Orbit-GEO) On the other hand, observation, meteorology, scientific, etc. The architectural structure was dominant for satellites to be low-altitude Earth Orbit (LEO) satellites. However, in recent years this structure has changed greatly. Especially after broadband data communication became widespread, communication satellites began to be used in Very Low Orbits. The goal of minimizing the delay time in broadband data communication also plays a major role in this change. Because as the distance between the satellite and the earth increases, the delay time inevitably increases.

This delay time is minimum for a satellite at 36,000 km;

72,000/300,000 seconds = 0.24x2=0.48 seconds is happening. (The distance is doubled, taking into account the signal's travel to/from the satellite)

This is especially the case in new generation communication systems, autonomous technologies, online transactions, etc. It contains very serious negative aspects. For this reason, new generation satellites for communication purposes are inevitably placed in close-range orbits, thus minimizing this time. In addition, it is possible to conduct broadband data communication with all of these systems.

It is possible to group these satellite systems, the number of which has been increasing in recent years, under the following headings.

3.4.1. Starlink Satellite System

It is a satellite system developed by SpaceX company. This company was founded by Elon Musk in 2002 and is an American organization that aims to provide aviation/space transportation services. "Reducing space transportation costs and colonizing Mars" are among the main goals of the company in question.

SpaceX company became the first private company to successfully send a spacecraft into space and return it from the ground. The company's “Falcon 9” rockets have landed and flown again more than 200 times. This company has created an internet network around the world by placing more than 4,500 small satellites in low orbit from January 2020 until the end of 2023 (Space.com, 2023). The height of these satellites above the ground is 360-400 km. between. The architectural structure of Starlink and similar satellite systems is shown Starlink Architecture.

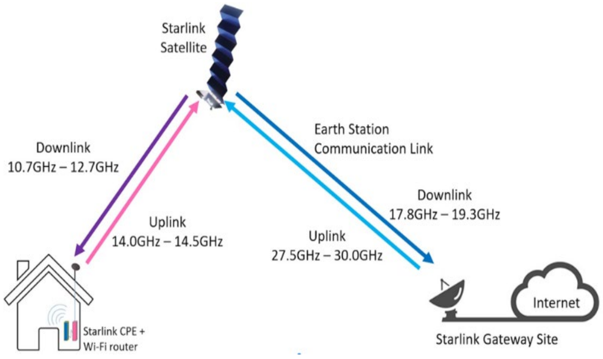

Starlink Satellite
Earth Station Communication Link
Downlink 10.7GHz – 12.7GHz
Uplink 14.0GHz – 14.5GHz
Downlink 17.8GHz – 19.3GHz
Uplink 27.5GHz – 30.0GHz
Starlink CPE + Wi-Fi router
Internet
Starlink Gateway Site

Figure 7. Starlink Architecture (Learning, 2022).

The antenna of the system in question must be installed in individual or corporate buildings that constitute the user side of the Starlink architecture. It is sufficient to install this antenna on the roof of the building or in a location that will not obstruct the view of the satellites. Although a single satellite configuration is shown in the figure above, there are thousands of satellites in the architectural structure. It is aimed to have a total of 42,000 SpaceX satellites in the architectural structure of the Starlink satellite system in the future.

The Starlink satellite system, many satellites are used effectively during a user's communication, and the smart satellite receiver on the user's side is automatically positioned by the system according to the satellites in low orbit.

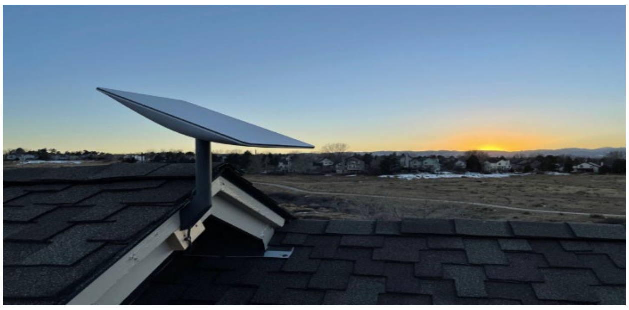


Figure 8. Starlink Smart Satellite Receiver (Starlink Mag, 2023).

In the Starlink system, there is a need for a bridge between the satellite placed in low orbit and the fiber internet network on the ground. These bridges are called gateways. In the Starlink system, these crossings are made through ground stations. With these ground stations, communication is provided between the internet network on earth and satellite systems in low orbit. In this way, it is possible to manage the satellite fleet and the network in question. As of the end of 2023, Starlink has approximately 160 active ground stations and gateways in the world. Below is an image of Starlink's ground stations.

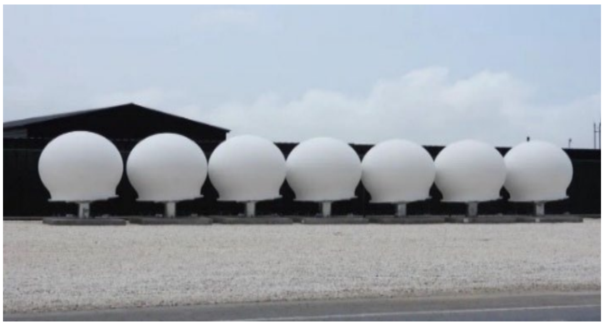


Figure 9. Starlink Ground Station (Starlink, 2023).

From time to time in our country, as in various parts of the world, Starlink satellites become visible at night and are followed with interest by people.

Figure 10. Starlink Satellite Constellation Migration (Starlink, medium.com, 2023).

In the Starlink Satellite system, Mobile Fixed Broadband Access allows mobile devices such as smartphones or tablets to be directly connected to the Starlink system without a smart satellite receiver. In this way, it is aimed to provide high-speed internet access to mobile devices located in remote or rural areas outside the limited coverage area of mobile cellular networks. In the coming period, on this system; SMS in 2024, data and voice in 2025, and internet of things (IOT) communication in 2026 will also be possible through this system. The general operating structure of the system is as follows.

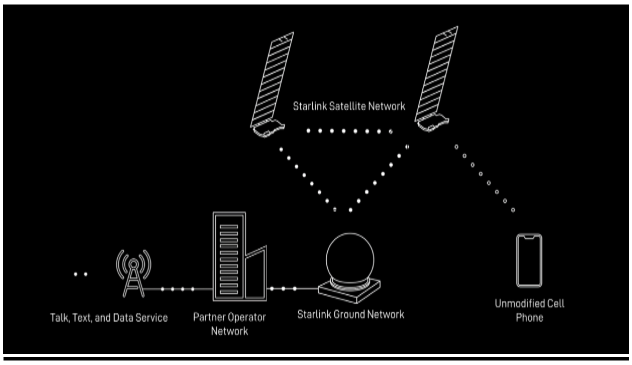


Figure 11. Mobile Fixed Broadband Access (Starlink, pocket-lint, 2023).

In this architectural structure, mobile devices are connected to Starlink satellites and the data transmitted in this way reaches Starlink's ground station. This access is then connected to the mobile operator's network, thus establishing a convergence of the classical telecommunication system and the Starlink satellite system. In this regard, the FCC aims to allocate a part of the US Frequency Plan to these functions and to implement other regulations on the subject in the near future (FCC, 2023).

Due to the features of the Starlink system, it is inevitable that it will be the system that will use the most broadband data communication on ships in the future.

3.4.2. Amazon Kuiper Satellite System

The project called "Kuiper", which aims to place 3,236 satellites in low orbit to provide global broadband internet service, was announced to the public by the US e-commerce company Amazon in 2019. In this way, it is aimed to establish a satellite constellation within 10 years.

Users of this system include users on sea and air vehicles, especially passengers on ships and yachts, oil refineries on land and at sea, buoys on the high seas, etc. Amazon company has received the necessary permission from the FCC in this regard and aims to complete half of the satellite architecture in question by 2026. The remaining half of this project is expected to be completed by the end of 2029.

Due to the features of the Amazon Kuiper Satellite system, it is inevitable that it will be one of the systems that will provide the most broadband data communication on ships in the future.

Figure 12. Kuiper Smart Satellite Receiver (Amazon, 2023).

3.4.3. Eutelsat-OneWeb Satellite System

Bharti, an Indian company with a similar architectural structure to the Starlink and Kuiper satellites, and "OneWeb", jointly owned by the United Kingdom, were established as low-orbit satellite internet service providers. This system is approximately 1200 km. It aims to launch 7000 satellites into high orbits and thus establish a satellite constellation. This system aims to provide data access and emergency communication to areas where there is no internet or broadband is insufficient. Eutelsat-OneWeb's smart satellite receiver systems are shown below.

Figure 13. Oneweb Smart Satellite Receiver (Chandaphan, 2022).

Due to the features described in the Eutelsat-OneWeb Satellite system, it is inevitable that it will be one of the systems that will provide the most broadband data communication on ships in the future.

3.5. Arrangements Made on VHF Channels

3.5.1. Available VHF Channels

Currently, channels between "01-28 and 60-88" are actively used in marine VHF systems in Europe and the MENA (Middle East and North Africa) region, including Turkey (Atmaca, 2009) Accordingly, channels "28 and 60" are not used in marine VHF systems. Some of the VHF channels in question are allocated as duplex (receiving and transmitting frequencies are different from each other), while others are allocated as simplex channels (receiving and transmitting frequencies are the same).

The reception/transmission frequencies and usage purposes of these channels are shown in detail in the Radio Regulations. The most functionally important of these simplex channels and their intended use in maritime communications are listed below.

Table 2. VHF Channels "01-28 and 60-88" (Ekinalan, 2020).

Channels	**Allocation**
01-05	(included)
07	X
06-17	(included, 07 excluded)
18-28	"
60-66	"
67-77	"
78-86	Duplex channels
87-88	Simplex channels

The diagram below shows the configuration of VHF channels in RR Annex 18 (Radio Regulation 18) and the output frequencies according to the use of Ship and Shore Radio stations

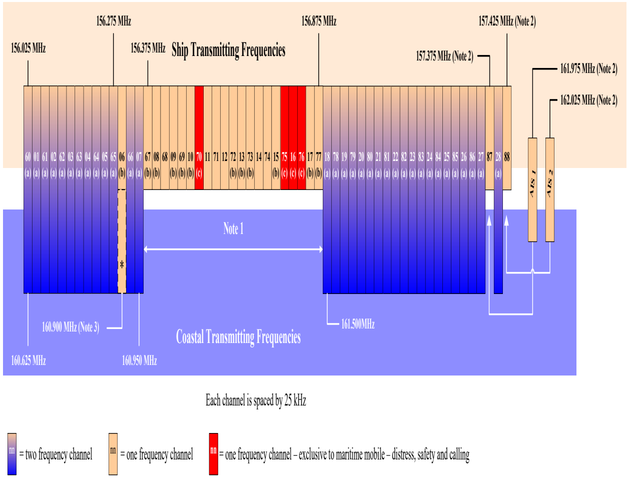


Figure 14. VHF marine channels (ITU, Manuel, 2009).

3.5.2. VHF Channels Allocated to Data Communication

As can be seen from the graph below, data communication has increased significantly in recent years, and it is calculated that this rate of increase will continue soon. Today, the communication of many services is done in the form of data, and this form of broadcasting is technically necessary for digital technology.

The most important factor in choosing the data communication method is that it is possible to transmit large amounts of data quickly and securely. The most important of these methods is combining adjacent channels and thus increasing the channel spacing (carrier aggregation). Since the more channels are combined in this way, the channel spacing will increase, the speed of data communication will be equally high.

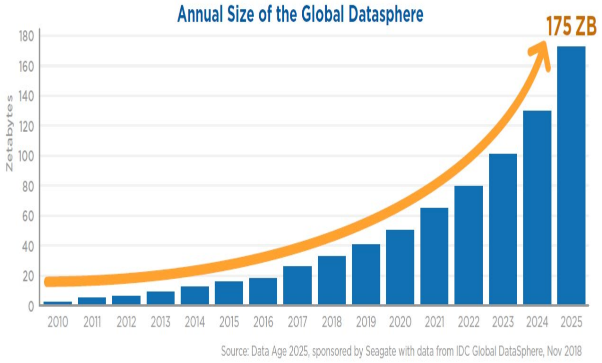


Figure 15. Increase in Data Traffic by Year (IDC, Data Age 2025 Report, 2021).

Increasing the channel width by combining adjacent channels is a suitable method for VHF maritime communication. Because the VHF maritime communication band determined by ITU is the standard and this range is 156-174 MHz (Acarer, 2014). In addition to maritime communications in the 30-300 MHz VHF band in electronics, television, radio, security, air traffic, etc. Since many different communication services are provided, it is not possible to further expand the 156-174 MHz band range allocated for VHF maritime communication.

In addition, since all existing VHF devices on ships operate in this band, it will be inevitable for millions of devices to remain idle and unusable if the marine VHF band changes. For this reason, combining adjacent existing VHF marine channels and thus obtaining wider channel spacing is technically the most realistic method. For this purpose, as a result of the decision taken at the World Radiocommunication Conference (WRC-19) held in November 2019 within the ITU, it was decided to combine adjacent duplex channels and convert them into simplex channels (ITU, Final Acts, 2019). It was decided that the channels combined in this way would be allocated to data communication and for this purpose, the maritime authorities of the countries would carry out the necessary tests and share them with the International Telecommunications

Organization (ITU).

3.6. Communication Facilities Provided by Data Channels in the VHF System

The regulations regarding VHF channels described in the regulation manuel (ITU, Manuel, 2009) are the most serious regulations made in the field of maritime communications in the recent past. These regulations aim to provide channels of the required width for broadband data transmission by combining existing duplex channels. In this way, it will be possible to communicate at high speeds in close-range maritime communications. It is possible to define this regulation as the most important changes in maritime communications after GMDSS to date. Because today, fixed and mobile communications are increasingly shifting to Internet Protocol. This form of communication, also briefly defined as IP, will soon be the only form of communication both corporate and individual. Because soon, communication methods such as voice, SMS and video will begin to be carried out entirely over the Internet Protocol.

The above-mentioned regulations regarding VHF channels are extremely important to ensure that similar developments in our daily lives can be made in close-range maritime communications. As a result of these changes, it will be possible to send files, maps, pictures, meteorological maps and written documents of different sizes in the form of data in close-range maritime communication. In addition, with this infrastructure, mutual internet communication will be possible between the ship and the land. Another important advantage of wireless data communication via VHF systems will be the reduction in communication costs. Since the communication medium in the VHF system is direct transmission between antennas, there is no charge for the establishment and operation of this medium. After the expansion of the band and therefore the communication channels, the communication cost for big data transmission through these channels will be almost free, and this will provide a very significant cost advantage for ships. In this way, ships will have the opportunity to communicate quickly and cheaply with the data facility brought to VHF systems in their communications with agencies, cargo persons, port authorities, companies and support units.

Again, it is inevitable that the regulations regarding VHF channels will contribute significantly to the navigational safety of ships. Because many marine vessels serve for different purposes in close-range sea areas. With data communication via VHF systems, it will be possible to transmit information in a very short time and in very wide content to the marine vessels in this area. Any information regarding navigational safety is of great importance for the safe navigation of ships.

4. DISCUSSION

First, the increasing possibility of using these new technologies in marine communication and the changes they have brought about are examined. Afterwards, the installation and operating costs of existing communication devices on ships and new generation communication devices are compared. Finally, the need for evaluation and regulation regarding this situation is highlighted.

4.1. Factors Causing the Increased Need for Broadband Data Communication on Ships

Today, data communication has been increasingly used in social and business life in recent years and provides great convenience in terms of communication. For this purpose, in recent years, the communication traffic between ship and land has increased due to many issues such as the delivery of the cargo to be carried in maritime transportation to the recipient in the shortest time, its damage-free transportation, safe navigation, insurance rules, ISM, etc. This form of communication is very important in terms of meeting the information needs of both ships and all parties related to maritime trade. In particular, the goal of reducing transportation time and increasing efficiency naturally causes the amount of information and reports sent from ships to land to increase. The same applies to information transmitted from land to ships. It has become almost impossible to transmit the increasing data traffic manually and without interruption. In order to meet this need, the International

Maritime Organization (IMO) has initiated a study using both existing systems and new generation communication systems.

The effective use of new systems will not only affect the commercial activities of ships but will also make a very positive contribution to the safe navigation of ships.

4.2. Increasing Usage Opportunities of New Generation Systems in Maritime Communications and the Emerging Changes

It is technically very natural to start the arrangements in question from VHF systems. Because VHF systems are the most used system in ships and in communication between ships and land, it will be a very serious example for the arrangements to be made from now on. It is inevitable that similar arrangements will be made in MF and HF systems in the future. Therefore, it is possible to say that the arrangements made regarding VHF channels will continue in other terrestrial maritime communication systems.

Although data exchange/transmission is not needed as much as close distance for ships in medium and long-distance navigation, many reports and information are sent/received regularly with land in ships at these distances.

Today, the most important development in broadband data communication between ships and land at medium and long distances has been in short-range satellite systems. Among these systems, the Starlink system in particular is developing faster than other short-range satellite systems. This system has also started to be used on ships in a short period of time. The installation and call costs of these systems, which are extremely easy to install, are extremely low compared to the current systems within the scope of GMDSS.

In the Starlink system, the download network speed (download) reaches 220 Mbps, and the upload network speed (upload) reaches 25 Mbps. It is possible for this speed to increase even more in the future. The invoices issued to ships are flexible and can be paused when desired.

Table 3. Data fee according to the currently valid tariff

Data Usage	**Data Fee**
50 GB	250 Euro/Month
1 TByte	1000 Euro/Month
5 TByte	5000 Euros/Month

To observe the trend in Table 3 better, we provide the following figure. For less data usage like 50 GB, data fee becomes 250 Euro/Month which is equivalent to a tariff with 1000 GB usage with 5000 Euros/Month. However, we observe that 1000 GB data usage and 5000 GB data usage are provided with data tariffs with 1000 Euros/Month and 5000 Euros/Month, respectively, which are just 20% of the data tariff for 50 GB usage. Hence, it can be observed that high data usage can be provided with 5 times cheaper data tariffs.

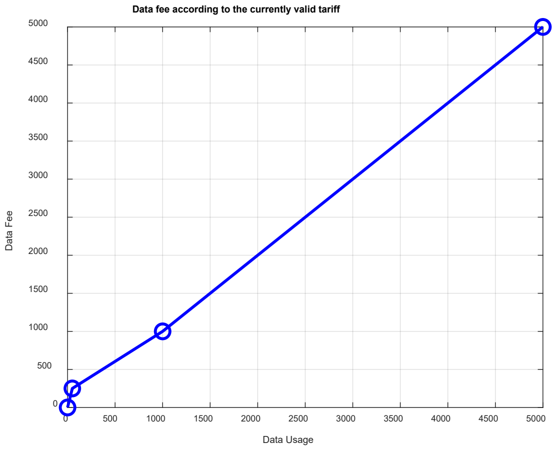


Figure 16. Data fee trend vs. Data Usage

In existing conventional systems, especially the Inmarsat satellite system, which currently provides maritime communication services, the installation fee of the terminals on the ship and the call fees over these systems vary depending on the Earth stations used and the tariffs determined by the countries where these Earth stations are located. The usage fee is determined as approximately 4,000 Euro/Month. Considering this price is relatively proportional, it is possible to say that the speeds achieved in the Starlink system, where broadband data service is provided, are 10 times higher than the existing data communication systems in the

GMDSS system, and the data cost per Gbyte is at least 10 times lower than the existing systems. Due to these features, the Starlink system will inevitably contribute greatly to data communication between ship and land. Because, inevitably, this system will greatly increase both the speed and bandwidth of data communication on ships.

4.3. Comparison of GMDSS Required Systems on Ships and New Generation Communication Systems in Terms of Installation and Operational Features

In the previously explained article titled "Devices Mandatory on Ships Due to International Legislation", the devices that must be installed as required by international legislation called GMDSS are explained in detail. Depending on the sea region they sail in, some or all of these devices are installed on ships. Some of the communication devices on ships are used only for distress/safety communication, and some are used for both commercial and distress/safety communication. Which devices will be used in different voyage regions are collected in international legislation under the name GMDSS, in line with the decisions taken at IMO.

The devices that must be installed on marine vessels are generally equipment with distress/safety communication capabilities. On the other hand, different systems are used on ships, especially for commercial communication purposes, in addition to the devices required in GMDSS. The most important of these is the Inmarsat terminals described above, which are not in the category of mandatory devices. However, the majority of these devices either only can communicate with voice or can communicate with data at very low speed. Low-speed data communication includes navigational and meteorological maps, observation reports, etc. It causes major problems in the transmission of files requiring large data to ships.

Commercial maritime communications can be made between ships and ship/land by using VHF, MF and HF systems and Inmarsat C and F77 devices, which are required to be installed on marine vessels in accordance with the GMDSS obligation. However, the desired speeds cannot be reached, especially since Inmarsat communication is at least 10 times more expensive than Starlink and the bandwidth for data transmission is insufficient. For this reason, maritime companies use Starlink for data communication that requires high speed and bandwidth. It will be a natural process for them to turn to new generation systems.

On the other hand, the fact that in practice only manual communication can be made via the VHF, MF and HF systems explained in the "Terrestrial Marine Communication Systems" article as a terrestrial system and that the cost of this communication is higher than automatic communication will naturally increase the interest in the Starlink satellite system in the near future.

For this reason, even though the installation of Starlink devices is not mandatory according to GMDSS rules, especially on marine vessels where official and private meetings are frequently held, it will be the most important factor in the rapid increase in the use of these devices on ships due to the advantages listed above.

4.4. Need for Evaluation and New Regulation

Although terrestrial and satellite systems, which are currently defined as conventional maritime communication systems, have taken on a digital structure with GMDSS, the general form of communication between ships and ship/land is manual. However, the recent regulations made within the IMO have paved the way for serious changes in the structure of existing maritime communications.

In recent years, data communication has become increasingly widespread in both corporate and individual communication and the use of Voice, SMS, Video, etc. As communication methods began to be made via data, the structure of communication began to change significantly. The confidentiality, speed and ability to transmit large amounts of data very quickly and securely provided by data communication, etc. Factors increasingly bring this form of communication to the fore. Again, the fact that data is much cheaper than other forms of communication and that it enables written and visual communication (maps, figures, graphics, etc.) are other important factors in the spread of this form of communication.

For this reason, to benefit from these developments in communication between companies and individuals to the maximum extent in maritime communication between ships and ship/land, it has become necessary to make these regulations. In parallel with these developments, the most important technical developments regarding maritime communications in the near future are Starlink etc. low orbit satellites were used and marine VHF channels were allocated to digital communications. The common point of the arrangements made in both systems is that they enable broadband data communication. Since in the VHF system, communication is provided between ships and ship/land on the basis that the antennas are visible to each other, the transmission medium between them is free.

This feature is extremely important for the development of data communication over the VHF system. When this regulation, made by IMO and accepted by all member countries, is put into practice, the necessary data communication will be possible for the safe navigation and more effective activities of ships in close proximity.

In addition, great conveniences and opportunities in broadband data communication have been provided through the communication via the SpaceX satellite system via Starlink satellite terminals, which have recently started operating. Since both the initial installation cost and the communication cost of this system are quite low, it is inevitable that this system will contribute greatly to the broadband data communications of ships. For this reason, if the system in question begins to be used both in long-distance vessels and in the large number of yachts and cruise ships, there will be significant changes in the communication capabilities of marine vessels. The biggest disadvantage of the Starlink system is that it is not on the list of devices that must be kept on ships in different sea regions in accordance with GMDSS obligations. In other words, this system is not required to be installed on large tonnage ships, nor on yachts, cruise ships and offshore fishing vessels, in accordance with international rules. For this reason, installing Starlink devices on marine vessels is not mandatory, but optional.

5. CONCLUSIONS

Currently, many communication systems are used in maritime communications in accordance with GMDSS obligations. Although the number and types of these devices vary depending on the tonnage of the ships and the sea region they sail in, as per the GMDSS legislation, their common feature is the ability to make automatic danger/safety communication. The term GMDSS stands for maritime distress and safety communications.

Today, as a result of developing technology and the increasing need for communication, the need for uninterrupted communication from anywhere and at any time is increasing. In particular, the safe navigation of ships, the increase in reports coming to and from the ship, the change in the structure of ships, the documents required by maritime and port authorities, etc. As a result of these reasons, voyage processes are getting faster and faster. In addition, the increasing need for information and document requirements in the inspection legislation greatly increases the communication needs of ships.

These developments also necessitate regulations for data communication in terrestrial and satellite systems (Inmarsat and Cospas Sarsat satellites), which we define as conventional systems in maritime communications. For this reason, IMO has recently allocated duplex channels used in VHF systems, where maritime communications are most intensive, to data communication. For this purpose, adjacent duplex channels in the VHF system have been combined, increasing the channel width and paving the way for broadband data communication to be used in ships navigating at close distances. However, since the possibility of using the regulations regarding VHF systems in long-distance vessels is limited, new generation satellite systems have emerged as a serious alternative to meet the need for broadband data communication.

There have been very important technological developments in this regard in recent years. There are serious developments especially in new generation satellite systems operating as global networks. In particular, the technical capabilities of these systems will be able to easily provide a solution to the broadband data communication needs of ships. Meanwhile, the satellite capacities of many Low Orbit satellite systems, whose development continues rapidly, are rapidly increasing on the space side.

The technical capabilities and especially the broadband data capabilities provided by these systems have emerged as a very important solution for ships. These systems have more bandwidth and latency than High Orbit Satellites. *Because High Orbit Satellite Systems are generally 36,000 km above the earth, and Low Orbit Satellite Systems are 400 km above the earth, the delay in these is 180 times [(36.00/400)x2)] less than High Orbit systems.*

This feature is extremely important for broadband maritime communications. This reduction in latency will contribute greatly to both the transmission of large amounts of data with minimal delay and the development of autonomous ships, whose trial runs have started in the near future. Because even in semi-autonomous systems, the delay time in communication between relevant units and central control elements must be minimized. Otherwise, it is inevitable to encounter serious accidents and disruptions. For this reason, it is imperative that the data rate of the systems used in the communication infrastructure of autonomous systems is high and the delay time is minimum.

As explained today, although there are many Low Orbit Satellite systems, the most advanced among them is Starlink, which became operational a few years ago. The architectural structure of this system, its low orbit (below 400 km) and its focus on broadband data communication have made these devices a very important alternative system, especially in commercial maritime communications. In addition, since both the facility costs and communication costs of the Starlink terminals to be installed on ships are quite cheap compared to other maritime communication systems, this system will provide a serious solution to the ever-increasing broadband data communication for ships. Another important advantage of this system over the existing satellite systems on ships is that the terminals are small in size and extremely easy to install.

Nowadays, in the communication sector, where all forms of communication are provided via data, it is inevitable that a similar process will occur in maritime communication between ships and ship/land. In parallel, both the regulations regarding VHF devices and the opportunities provided by Starlink satellite terminals regarding broadband data communication will inevitably lead to major changes in the use of existing marine communication systems.

Even though it is still mandatory to have different maritime communication systems in use on ships by the GMDSS provisions, their high communication costs and the fact that they do not allow broadband data communication will cause these systems to function only as distress/safety communication after a few years. On the other hand, routine maritime communication will shift to new generation satellite systems where broadband data communication can be made.

In addition, with new regulations to be made within the International Maritime Organization in the future, Starlink and similar Low Orbit Satellite systems may also be given the ability to make automatic distress/safety broadcasts. In this way, it is possible to say that the use of many existing marine radio communication systems on ships will be eliminated and they will be replaced by new generation communication systems.

AUTHORSHIP CONTRIBUTION STATEMENT

Tayfun ACARER: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing - Original Draft, Writing-Review and Editing, Funding acquisition.

CONFLICT OF INTERESTS

The author declares that for this article they have no actual, potential or perceived conflict of interests.

ETHICS COMMITTEE PERMISSION

No ethics committee permissions is required for this study.

FUNDING

No funding was received from institutions or agencies for the execution of this research.

ORCID IDs

Tayfun ACARER:
https://orcid.org/0000-0003-2407-5552

6. REFERENCES

Acarer, T. (2014). *Amatör Denizcilik Kitabı*, s.7, İstanbul, Boyut Yayınları.

Acarer, T. (2018). VHF EPIRB Cihazı ile ilgili GMDSS Mevzuatının İncelenmesi ve Alternatif Mevzuat Önerileri. *Social Sciences Research Journal*, 7(2): 126-150.

Acarer, T. (2023). Endüstrideki Gelişmelerin Denizcilik İşletmelerine Ait Gemilerin Yönetiminde Temin Ettiği Olanaklar ve İnsansiz Gemiler. *Mersin Üniversitesi Denizcilik ve Lojistik araştırmaları Dergisi*, 5(2): 122-153.

Amazon, (2023). space.com, 05 July 2024, https://www.space.com/fcc-approves-amazon-constellation-kuiper is retrieved.

Atmaca, S.T. (2009). *Kısa Mesafe Telsiz El Kitabı,* s.11, İstanbul.

Cospas-Sarsat, (2023). Cospas-Sarsat System. www.cospas-sarsat.int, Accessed Date: 8 June 2023, https://www.cospas-sarsat.int/en/system-overview/cospas-sarsat-system is retrieved.

Cospas-Sarsat, (2023). Transition to MEOSAR. cospas-sarsat.int, Accessed Date: 13 June 2023, https://www.cospas-sarsat.int/en/system-overview/transition-to-meosar is retrieved.

Demir, C. (2009). *Maritime English,* s.5, Kocaeli, Akademi Denizcilik.

Ekinalan T., A. T. (2020). *Küresel Denizde Tehlike ve Emniyet Sistemi (GMDSS) El Kitabı*, s. 25, İstanbul, Akademi Kitap Evi.

FCC, (2023). docs.fcc.go, 12 July 2024, https://docs.fcc.gov/public/attachments/DA-23-338A1.pdf is retrieved.

Gul, O.M., Erkmen, A.M., Kantarci, B. (2024). NTN-Aided Quality and Energy-Aware Data Collection in Time-Critical Robotic Wireless Sensor Networks. *IEEE Internet of Things Magazine*, 7(3): 114-120.

IDC, (2021). Data Age 2025 Report, IDC.

INMARSAT, (2012). Inmarsat Uyduları, London, Inmarsat.

International Civil Aviation Organization, (2023). www.icao.int/Meetings, 05 July 2024, https://www.icao.int/Meetings/GTM/Documents/COSPAS-SARSAT.pdf is retrieved.

ITU, (2009). Manuel. Geneva, International Telecommunication Union.

ITU, (2019). Final Acts. (2014). Geneva, ITU.

ITU, (2013). Maritime Mobile Satellite Services (Vol. 1), Geneva, International Telecommunications Union.

Kayisoglu, G., Bolat, P., Tam, K. (2023). A novel application of th CORAS framework for ensuring cyber hygiene on shipboard RADAR. *Journal of Marine Engineering & Technology*, 23(2): 67–81. doi: 10.1080/20464177.2023.2292782.

Kayişoğlu, G. G. (2024). ECDIS Cyber Security Dynamics Analysis based on the Fuzzy-FUCOM Method. Transactions on Maritime Science. Split, Croatia, 13(1). doi: 10.7225/toms.v13.n01.w09.

Korkmaz Y, Acarer, T. (2002). *GMDSS Deniz Telsiz Haberleşme ve GMDSS Kuralları,* s.33, İstanbul, Akademi Kitap Evi.

OpenWorldLearning, The Future of High-Speed Internet, (2022). 19 July 2024, https://www.openworldlearning.org/spacexs-starlink-the-future-of-high-speed-internet-3 is retrieved.

Atmaca. S., Tokay, T. (2009). *Kısa Mesafe Telsiz El Kitabı.* s.15, İstanbul, Amatör Denizcilik Federasyonu.

Space.com, S. S. (2023). www.space.com/spacex-starlink-satellite. Starlink Satellites, 05 July 2024 https://www.space.com/spacex-starlink-satellites.html is retrieved.

Starlink, (2023). medium.com, 12 July 2024, https://medium.com/geekculture/how-spacex-is-pacifying-astronomers-anger-78fc15320e36 is retrieved.

Starlink, (2023). pocket-lint. www.pocket-lint.com, 12 July 2024, https://www.pocket-lint.com/starlink-direct-to-cell-when-will-it-launch is retrieved.

Starlink, (2023). the-starlink-exit-pla. www.theinformation.com, 05 July 2024, https://www.theinformation.com/articles/the-starlink-exit-plan-how-spacexs-satellites-are-bringing-remote-workers-to-the-wilderness is retrieved.

Starlink Mag, (2023). Starlink Ground Station Locations, 12 July 2024, https://starlinkmag.com/starlink-ground-station-locations is retrieved.

Suwijak, C., Li, S. (2022). Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space. *Journal of East Asia and International Law*, 15(1): 193-108.

Yılmaz, L.A. (2014). *Küresel Denizde Tehlike ve Emniyet Sistemi (GMDSS), Genel Telsiz Operatör Ehliyeti (GOC),* s. 21, İstanbul, Akademi Yayınları.

Research Article
Turkish Journal of Maritime and Marine Sciences

DOI: 10.52998/trjmms.1531141
Volume: 10 Special Issue: 1 (2024) 81-94

A Novel Energy-Aware Path Planning by Autonomous Underwater Vehicle in Underwater Wireless Sensor Networks

Sualtı Kablosuz Sensör Ağlarında Otonom Sualtı Aracı Tarafından Yenilikçi bir Enerji Farkında Yol Planlaması

Türk Denizcilik ve Deniz Bilimleri Dergisi

Cilt: 10 Özel Sayı: 1 (2024) 81-94

Ömer Melih GÜL[1]

[1]*Istanbul Technical University, Informatics Institute, 34469, Istanbul, Turkiye*

ABSTRACT

Wireless sensor networks can monitor the environment to detect anomalies and reduce the risk of maritime traffic. Energy is necessary for low-power conditions where wireless sensor networks are used. Ensuring the lifespan of energy constraints and providing continuous environmental observation, data collecting, and communication requires management. Battery replacement and energy consumption issues can be resolved with path planning and energy-efficient autonomous underwater vehicle charging for sensor nodes. The nearest neighbour technique is used in this study to solve the energy-aware path planning problem of an autonomous underwater vehicle. Path planning simulations show that the nearest neighbour strategy converges faster and produces a better result than the genetic algorithm. We develop robust and energy-efficient path-planning algorithms that efficiently acquire sensor data while consuming less energy, allowing the monitoring system to respond to anomalies more rapidly. Increased sensor connectivity lowers energy usage and increases network longevity. This study also considers the situation when it is recommended to avoid taking direct travel paths between particular node pairs for a variety of reasons. This recommendation is considered in this study. We present a strategy based on a modified Nearest Neighbour-based Approach from the Nearest Neighbour method to address this more challenging scenario. The direct pathways between such nodes are constrained within the context of this technique. The modified version of Nearest Neighbor-based approach performs well even in that particular situation.

Keywords: Autonomous underwater vehicle; artificial intelligence; environmental monitoring; energy-aware path planning; wireless sensor networks; underwater communication

Article Info
Received: 09 August 2024
Revised: 17 September 2024
Accepted: 21 September 2024

*(corresponding author)
E-mail: omgul@itu.edu.tr

To cite this article: Gül, Ö.M. (2024). A Novel Energy-Aware Path Planning by Autonomous Underwater Vehicle in Underwater Wireless Sensor Networks, *Turkish Journal of Maritime and Marine Sciences*, 10 (Special Issue: 1): 81-94. doi: 10.52998/trjmms.1531141.

ÖZET

Kablosuz sensör ağları, anormallikleri tespit etmek ve deniz trafiği riskini azaltmak için çevreyi izleyebilir. Kablosuz sensör ağlarının kullanıldığı düşük güç koşulları için enerji gereklidir. Enerji kısıtlamalarının ömrünün sağlanması ve sürekli çevresel gözlem, veri toplama ve iletişim sağlanması yönetim gerektirir. Pil değişimi ve enerji tüketimi sorunları, sensör düğümleri için yol planlaması ve enerji açısından verimli otonom su altı araç şarjı ile çözülebilir. Bu çalışmada, otonom bir su altı aracının enerji farkında yol planlama problemini çözmek için en yakın komşu tekniği kullanılmıştır. Yol planlama simülasyonları, en yakın komşu stratejisinin daha hızlı birleştiğini ve genetik algoritmadan daha iyi sonuç ürettiğini göstermektedir. Daha az enerji tüketirken sensör verilerini verimli bir şekilde toplayan ve izleme sisteminin anormalliklere daha hızlı yanıt vermesini sağlayan sağlam ve enerji açısından verimli yol planlama algoritmaları geliştiriyoruz. Artan sensör bağlantısı enerji kullanımını düşürür ve ağ ömrünü artırır. Bu çalışma ayrıca çeşitli nedenlerle belirli düğüm çiftleri arasında doğrudan seyahat yolları kullanmaktan kaçınılmasının önerildiği durumu da ele almaktadır. Bu öneri bu çalışmada dikkate alınmıştır. Bu daha zorlu senaryoyu ele almak için En Yakın Komşu yönteminden değiştirilmiş En Yakın Komşu tabanlı Yaklaşıma dayalı bir strateji sunuyoruz. Bu tür düğümler arasındaki doğrudan yollar bu tekniğin bağlamında kısıtlanmıştır. En Yakın Komşu tabanlı yaklaşımın değiştirilmiş versiyonu, o belirli durumda bile iyi performans gösterir.

Anahtar sözcükler: Otonom su altı aracı; yapay zeka; çevresel izleme; enerji bilinçli yol planlama; kablosuz sensör ağları; su altı iletişimi

1. INTRODUCTION

1.1. Motivation

Wireless sensor networks (WSN) are becoming increasingly important for resource exploration, navigation, and data collection due to their rapid expansion (Felemban *et al*., 2015). Intelligent Ocean Undersea Technology, or IoT, has been proposed recently (Qiu *et al*., 2020) and has a lot of potential uses. Many submerged sensor nodes transmit climate data to a data hub. Battery replacement for battery-operated nodes in extreme maritime circumstances necessitates costly and intricate technologies. Given limited energy capacity and short lifespan of underwater wireless sensor network (UWSN), energy efficiency must be increased to enhance UWSN performance and reliability. As a result of their short lifespan and limited energy source, UWSNs depend on increased energy economy for proper operation (Akyildiz *et al*., 2005).

The suggested metaheuristic-based path planning technique for WSN accelerates sensor data collecting while saving energy, enabling faster monitoring system reaction to ship disaster hazards. By getting closer to the sensors, you can communicate with them and use less energy. WSN will therefore last longer, monitoring the environment to detect anomalies and prevent accidents.

Numerous studies have been conducted on this issue. Wireless sensor networks (WSNs) use a lot of energy to transmit data. Energy consumption and transmission are reduced by optimising and compressing sensory data (Li *et al*., 2020). Furthermore, by strategically placing and routing nodes, UWSN energy efficiency can be raised. By streamlining the deployment and routing procedures, energy consumption can be decreased and network lifetime can be extended. This is because there may be variations in the energy usage and distance between data sensor nodes (Cheng *et al*., 2014).

Even with these techniques, replacing the battery when it runs low is still important. Energy transfer technology can be used to charge underwater sensors so they can be used for long-term monitoring and data transmission without the need for new batteries (Khan *et al*., 2018). Through addressing high water pressure and short circuits, the team (Pendergast *et al*., 2011) produced a rechargeable lithium-ion battery module that may be used underwater. Due to limitations on the distance over which energy can be transferred, autonomous underwater vehicles require help planning their routes and charging.

An autonomous underwater vehicle, or AUV, is a self-propelled submersible that can do moderate activities without the need for human help (Blidberg *et al*., 2001). Underwater research, environmental monitoring, and marine safety have all made extensive use of AUVs because to their affordability and security in seabed inquiry, search, identification, and rescue (Ghafoor *et al*., 2019). The AUV's constrained charging space and power carrying capabilities make data loss from subsequent nodes troublesome. Therefore, it is difficult to guarantee that the AUV would be advantageous for broader detection zones, especially in maritime conditions.

1.2. Main Contributions

The main contribution can be briefed as follows:

- This paper offers a comparative examination of AI-based techniques for three-dimensional path planning for autonomous underwater vehicles (AUV). The main focus of the presentation is the challenges that arise when collecting data in wireless sensor networks.
- The Nearest Neighbour (NN)-based Approach is recommended as a workable solution for the three-dimensional path planning problem. This technique considers the current computer limitations during the procedure.
- We introduce a modified Nearest Neighbour-based Approach, which modifies the Nearest Neighbour algorithm to avoid obstacles in the three-dimensional path planning issue. The travelling restrictions between certain sensor pairs are considered whenever this technique is used.
- Our approach provides not only an energy-efficient but also computationally efficient and fast solution.

1.3. Organization

The remainder of the paper will follow this format. A succinct synopsis of pertinent studies from the literature is given in Part 2. In Section 3, the issue is outlined and a system model is supplied. A few methods for solving the 3D path planning problem are shown in Section 4. In Section 5, we propose a novel solution to the problem with some limitations between some of the sensor pairs. We evaluate effectiveness of the proposed strategies in Section 6. Section 7 concludes the work. Section 8 gives future work.

2. RELATED LITERATURE

This section considers the necessary literature to address path planning in WSN. Energy-efficient communication techniques must be created as alternatives because of battery limitations. Lee et al. looked at network topology-based energy-efficient WSN MAC techniques. As in the works (Le *et al*., 2011, Zenia *et al*., 2016) investigate secure and energy-conserving WSN MAC and routing techniques. (Khan *et al*., 2019) presents a packet-sending strategy that aims to improve channel quality and decrease redundancy. The hybrid-coding-aware routing technique created by a work (Su *et al*., 2023) has applications for underwater acoustic sensor networks (UASNs). This method reduces gearbox overhead and increases reliability.

Clustering improves resource management, energy efficiency, longevity, and data aggregation in wireless sensor networks (Kumar *et al*., 2018). To reduce unnecessary transfers inside the network, a cluster head (CH) disseminates information throughout each cluster (Xie *et al*., 2013). Energy and bandwidth reductions are attainable at challenging fields with restricted communication resources (Yadav *et al*., 2019).

Using a clustering-based communication protocol, the work (Sun *et al*., 2022) reduced the energy usage of sensor nodes. The topology management system developed by Jin et al. guarantees reliable connectivity while simultaneously improving coverage and longevity (Fan *et al*., 2023). Liu *et al*. (2019) developed a virtual force-based distributed node deployment technique to expand WSN network coverage. In Wei *et al*. (2020), a network topology control model that prolongs network lifetime qualities such resilience, energy consumption balance, and topology is presented.

It improves data transmission while doing so.

AUVs charge and collect data concurrently with the UAV. AUVs equipped with sensors can collect data on marine life, geology, and water quality. AGV assisted communication was tested in (Zhu *et al.*, 2023), where the AUV was employed as a mobile node to gather energy-saving data. For data gathering and K-means path planning, AUVs were proposed in (Yan *et al.*, 2023), and (Shen *et al.*, 2020). AUVs are used for two purposes: data collection and multi-hop detection (Gjanci *et al.*, 2017, Yan *et al.*, 2018).

AUVs may network and communicate underwater. AUVs or central stations can receive data from mobile or fixed sensors. The activities can be managed in real time. Kan *et al.* (2018) field-deployable three-phase wireless charging system offers quick and easy AUV charging. According to Ramos *et al.* (2018), using dynamic system theory for AUV navigation at depths of 0–100 m resulted in a faster battery life.

Building battery-charging, autonomous docking AUVs allow for continuous operation without requiring human intervention. The dock charges the batteries in the AUVs and the sensor nodes. Their efficiency and independence increase in the absence of retrieval and recharging. The efficiency of the AUV path design is increased. Cheng et al. apply kinematic and dynamical models to plan AUV routes, avoid obstacles, and evaluate energy usage for energy savings and network longevity (Cheng *et al.*, 2021). The work (Kumar *et al.*, 2021) have presented a hybrid underwater AUV exploration strategy that drastically reduces its range. Using data collecting points, the exploring region is subdivided in (Golen *et al.*, 2010). Prepared paths save AUV energy during data collection. Rechargeable method increases network life (Yhi *et al.*, 2022).

3. SYSTEM MODEL AND PROBLEM DEFINITION

Our research focusses on the energy-aware path planning problem for an AUV's sensor visit. We define this challenge and provide an illustrative case. We examine the UWSN system model first. The energy-aware path planning problem is then defined more precisely.

3.1. System Model

In this network system, every sensor node sends data to the cluster head node using a wireless network. Magnetic resonance coupling AUVs charge each sensor node before returning to a charge station (CS) for resting and data gathering.

The maintenance of energy consumption balance in sensors is a critical consideration for Wireless Sensor Networks (WSNs). autonomous underwater vehicle (AUV) collect data from several studies (Pop *et al.*, 2024, Davendra, 2010, Johnson *et al.*, 1997) to examine and address discrepancies in energy usage. The AUV methodically visits each sensor node according to a pre-established plan to ensure an equitable distribution of energy usage.

3.2. Problem Definition

The difficulty of optimising energy consumption in path planning using AUV is classified as the travelling salesman problem (TSP) (Pop *et al.*, 2024, Davendra, 2010, Johnson *et al.*, 1997). The TSP is commonly solved using classical search algorithms and evolutionary algorithms, which are the primary approaches used in this procedure. The artificial potential field technique, greedy algorithm, and quick progress algorithm are all examples of algorithms that fall within the previously mentioned category. The latter group includes techniques such as genetic algorithm and nearest neighbour algorithm, which are derived from biological algorithms.

4. PROPOSED ENERGY-AWARE PATH PLANNING (EAPP) APPROACHES

This section focuses on the challenge of energy-conscious path planning for an AUV. The primary area of concern is the separation between each pair of sensor nodes. The TSP is widely recognised as the most prominent NP-hard optimisation problem (Davendra, 2010, Johnson *et al.*, 1997). The TSP aims to construct an optimised itinerary for a salesperson, starting from his apartment, visiting many places, and returning to the starting point, to decrease travel time (Gutin *et al.*, 2002).

By considering the EAPP problem as a TSP problem, we propose three approaches: Nearest Neighbour (NN)-based Approach, the Grey Wolf Optimiser (GWO)-based Approach, and the Genetic Algorithm (GA)-based Approach.

4.1. Nearest Neighbour (NN)-Based Approach

Concurrently, we suggest employing the Nearest Neighbour Algorithm (Gutin *et al.*, 2007) to address the EAPP problem by seeing it as a Travelling Salesman Problem (TSP).

4.2. Grey Wolf Optimizer (GWO)-based Approach

Our methodology consists of tackling the EAPP issue by seeing it as a Travelling Salesman Problem (TSP) and creating a solution for 3D path planning using the Grey Wolf Optimiser Algorithm (Mirjalili *et al.*, 2014). To do this, we have formulated a solution.

4.3. Genetic Algorithm (GA)-based Approach

To address the EAPP issue, also referred to as the TSP, we offer a solution that employs the Genetic Algorithm. This technique is specifically tailored for planning paths in three-dimensional space (Goldberg, 1989, Bonabeau *et al.*, 1999). Genetic algorithms are designed to address complex optimization problems by simulating the processes of biological evolution. This is done to address optimal issues. To address the issues of the Travelling Salesman Problem (TSP), a genetic algorithm is used. This approach begins by identifying the people that make up the TSP solution and initializing the population. These stages signify the beginning phase of the procedure. Throughout the genetic processes of selection, crossover, and mutation, individuals in the population are evaluated based on a fitness function. Individuals who have been identified as the most physically competent are selected. The maximum number of iterations is the decisive parameter that will determine the termination of the GA. In this study, individual fitness is assessed by either the overall distance travelled or the total amount of energy used by the AUV. Both factors are taken into account.

5. MODIFIED NEAREST NEIGHBOUR-BASED APPROACH

This section focuses on the problem of energy-efficient path planning, considering the constraints imposed by specific sensor pairs that are located close to each other. Placing barriers between sensors may obstruct the direct transfer of data between them. The AUV has multiple reasons for avoiding a straight transition between the first and second sensors. Each of these elements will be expounded upon in more detail below. These considerations include potential hazards, obstructed paths, such as those covered in mud, between the two sensors, and temperatures that constantly vary. In this specific case, the AUV will move towards a sensor or sensors positioned between the two sensors.

Our proposed solution to the problem of three-dimensional path planning is the modified version of Nearest Neighbour-based Approach proposed in the works (Gul *et al.*, 2024, Gul, 2024). This technique aims to address minor barriers that frequently occur in the space between certain pairs of sensors.

$$\boldsymbol{D} = \begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1(n-1)} & d_{1n} \\ d_{21} & d_{22} & \cdots & d_{2(n-1)} & d_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{(n-1)1} & d_{(n-1)2} & \cdots & d_{(n-1)(n-1)} & d_{(n-1)n} \\ d_{n1} & d_{n2} & \cdots & d_{n(n-1)} & d_{nn} \end{bmatrix} \quad (1)$$

If some obstacles or obstructions hinder movement from node $\boldsymbol{n-1}$ to node $\boldsymbol{n}$, then the distance between node $\boldsymbol{n-1}$ and node $\boldsymbol{n}$, denoted by $\boldsymbol{d_{(n-1)n}}$ is assigned a value of $\boldsymbol{M}$, where $\boldsymbol{M}$ denotes a considerably large number.

The distance cost matrix $\boldsymbol{D_{mod}^{OA}}$, which is updated prior to using the Nearest Neighbour approach for $\boldsymbol{n}$ nodes, can be constructed by assigning a large integer value $\boldsymbol{M}$ to the entry $\boldsymbol{d_{(n-1)n}}$.

$$\boldsymbol{D}_{mod}^{OA} = \begin{bmatrix} d_{11} & M & \cdots & d_{1(n-1)} & d_{1n} \\ d_{21} & d_{22} & \cdots & d_{2(n-1)} & d_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{(n-1)1} & d_{(n-1)2} & \cdots & d_{(n-1)(n-1)} & M \\ d_{n1} & d_{n2} & \cdots & d_{n(n-1)} & d_{nn} \end{bmatrix} \quad (2)$$

Using the updated distance cost matrix $\boldsymbol{D}_{mod}^{OA}$, we implement the 3D Nearest Neighbour algorithm. Thus, we have proposed a modified Nearest Neighbour approach.

6. NUMERICAL RESULTS

This section assesses the effectiveness of algorithms used to solve the 3D energy-aware path planning problem of an AUV. The decisive factor is the distance separating each pair of sensor nodes. Through the random deployment of sensor nodes, we were able to establish a three-dimensional zone with dimensions of 500 meters in length, breadth, and height. This enabled us to carry out the simulations. The selected works utilised a range of dimension lengths and distances that were in line with our approach.

6.1. 50-node scenario

This article specifically examines the quantitative evaluation of the proposed algorithms in a particular scenario involving a single AUV and 50 nodes. Figure 1 illustrates the configuration of 50 nodes in a three-dimensional space, with each dimension measuring 500 m.

Locations are given as ((442, 22, 474), (502, 59, 327), (285, 291, 67), (294, 311, 108), (57, 149, 390), (454, 22, 47), (238, 383, 180), (425, 11, 18), (159, 463, 38), (77, 30, 452), (143, 74, 155), (292, 356, 348), (4, 215, 113), (148, 179, 127), (158, 209, 285), (448, 263, 362), (108, 141, 230), (450, 484, 172),(428, 112, 223), (489, 281, 23), (259, 242, 186), (325, 162, 227), (141, 22, 386), (296, 108, 402), (414, 355, 411), (439, 62, 14), (241, 7, 29), (258, 272, 221), (319, 390, 244), (209, 299, 390), (169,156, 443), (150, 465, 96), (187, 105, 280), (272, 447, 28), (348, 263, 305), (389, 234, 382), (399, 416, 213), (31, 370, 63), (152, 120, 371), (207, 67, 491), (118, 352, 126), (225, 361, 460), (460, 203, 139), (15, 100, 244), (340, 188, 20), (60, 447, 316), (430, 154, 168), (214, 158, 283), (210, 332, 95), (102, 335, 422)).

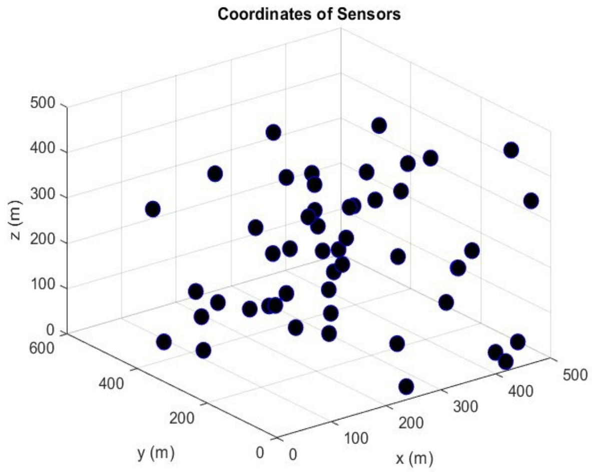


Figure 1. Locations of sensors

We evaluate the efficacy of Nearest Neighbour (NN), Grey Wolf Optimiser Algorithm (GWO), and Genetic Algorithm (GA)-based Approaches by analysing different combinations of these parameters.

6.1.1. NN-based Approach

This subsection evaluates performance of an NN-based solution. Figure 2 demonstrates the NN's achieved path planning solution in a scenario in Figure 1.

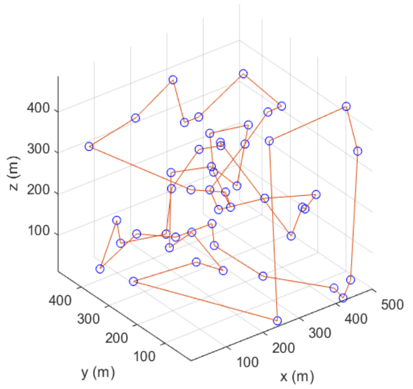


Figure 2. Achieved (6293 m) path planning solution by Nearest Neighbor

6.1.2. GA-based Approach

This subsection evaluates performance of an GA-based solution. Figure 3 demonstrates the GA's achieved path planning solution in 1000 iterations in a scenario in Figure 1.

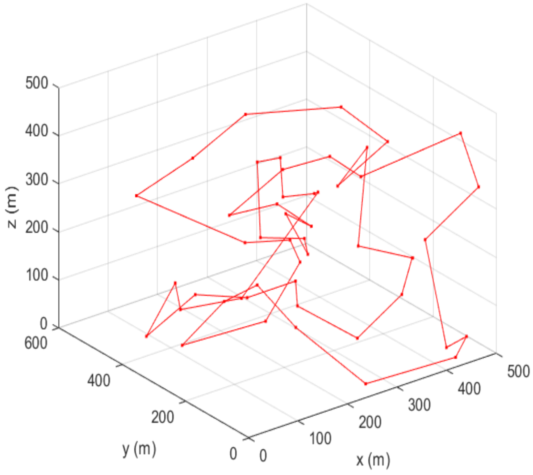


Figure 3. Achieved (6198 m) path planning solution with GA in 1000 iterations

6.1.3. GWO-based Approach

This subsection evaluates performance of an GWO-based solution. Figure 4 demonstrates the GWO's achieved path planning solution in 1000 iterations in a scenario in Figure 1.

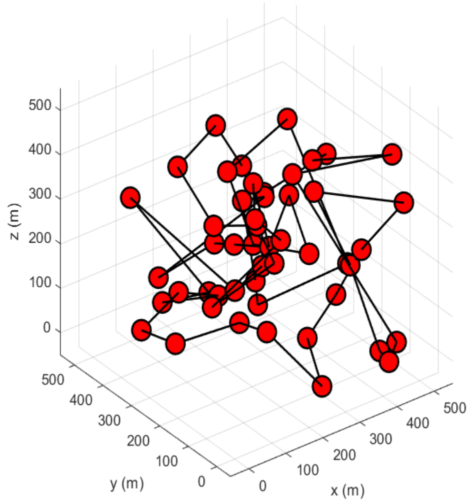


Figure 4. Achieved (8788 m) path planning solution with GWO in 1000 iterations

6.1.4. Discussion

In general, NN-based Approach achieves shorter path than GA-based Approach.

Figure 5 illustrates the total distance travelled by AUV employing multiple algorithms (NN Based Approach, GWO Based Approach, and GA Based Approach) to visit the 50 sensor nodes shown in Figure 1. Based on the data presented in Figure 5, we can make the following inferences about the performance of the algorithms in the scenario involving 50 nodes. According to the general pattern, the NN-based method and GA-based approach are more effective than the GWO-based approach. The neural network-based approach demonstrates superior performance compared to the genetic algorithm-based approach in terms of results up to the 500th iteration. In addition, the NN-based Approach is significantly faster in solving the problem, taking only 0.094679 seconds compared to the GA-based approach's time of 3.598634 seconds (38 times faster).

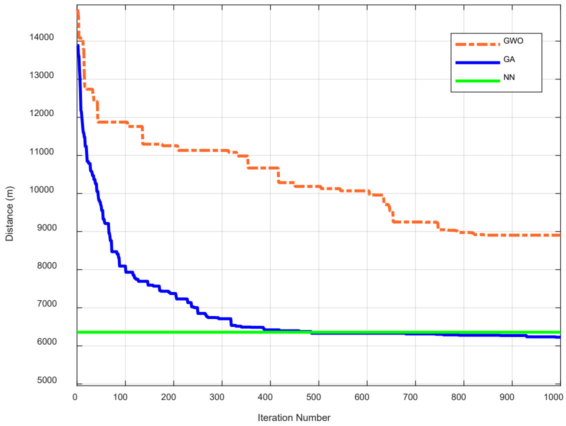


Figure 5. Achieved path lengths for visiting 50 nodes by NN, GWO, and GA-based Approaches

Figure 5 enables us to derive the following conclusions. Although the NN-based strategy quickly found a solution of around 6.27 km, both the GA-based method and the GWO-based approach initially had longer road lengths of 15 km in the first iteration. The GA-based strategy outperforms the GWO-based technique significantly at the 100th iteration, achieving a distance of 2.90 Km, which is 30% less. The NN strategy performs better than the GWO and GA strategies at the 300th iteration. The GA strategy achieves superior performance compared to the NN approach at the 600th iteration. Although the NN-based technique offers a speedier and more practical solution, it does not provide a shorter path compared to other methods. At the 1000th iteration, the GA-based technique significantly beats GWO-based approaches, with a performance of 2510 m, which is 28.5% lower than the GWO-based approach.

6.2. 100-node scenario

This article specifically examines the quantitative evaluation of the proposed algorithms in a particular scenario involving a single AUV and 100 nodes. Figure 6 illustrates the configuration of 100 nodes in a three-dimensional space, with each dimension measuring 500 m.

Locations are given as ((410, 84, 325), (455, 400, 192), (66, 158, 408), (459, 267, 269), (319, 85, 178), (51, 303, 472), (142, 134, 440), (276, 330, 278), (481, 347, 314), (485, 377, 296), (81, 228, 106), (488, 44, 153), (481, 117, 238), (245, 459, 118), (403, 79, 425), (73, 415, 100), (213, 272, 115), (460, 501, 88), (399, 42, 116), (482, 224, 220), (330, 56, 158), (20, 483, 464), (427, 5, 218), (469, 390, 95), (342, 411, 455), (381, 437, 492), (374, 45, 222), (199, 202, 58), (330, 132, 132), (88, 403, 207), (356, 218, 300), (18, 458, 134), (141, 93, 304), (26, 134, 358), (51, 75, 113), (414, 71, 61), (350, 437, 151), (161, 292, 162), (478, 277, 215), (20, 75, 256), (222, 429, 45), (193, 314, 134), (385, 178, 403), (400, 259, 17), (96, 203, 467), (247, 40, 368), (225, 122, 247), (326, 64, 292), (357, 94, 121), (380, 122, 232), (141, 211, 484), (342, 27, 276), (330, 454, 263), (84, 475, 118), (62, 248, 247), (252, 247, 315), (482, 171, 342), (173, 453, 200), (295, 187, 186), (114, 58, 496), (378, 393, 21), (130, 197, 445), (255, 123, 459), (352, 204, 401), (448, 51, 52), (482, 68, 133), (276, 474, 170), (72, 481, 342), (77, 290, 71), (131, 32, 363), (423, 120, 56), (130, 179, 329), (410, 413, 250), (124, 10, 392), (467, 24, 360), (177, 87, 454), (101, 327, 448), (128, 368, 170), (311, 326, 352), (239, 228, 101), (178, 276, 18), (418, 151, 375), (295, 375, 253), (277, 97, 242), (461, 346, 455), (145, 94, 307), (381, 187, 311), (379, 315, 432), (193, 393, 405), (286, 43, 291), (40, 467, 94), (29, 390, 122), (268, 246, 446), (392, 220, 17), (470, 226, 247), (67, 156, 86), (287, 257, 492), (237, 258, 359), (8, 411, 253), (171, 400, 238)).

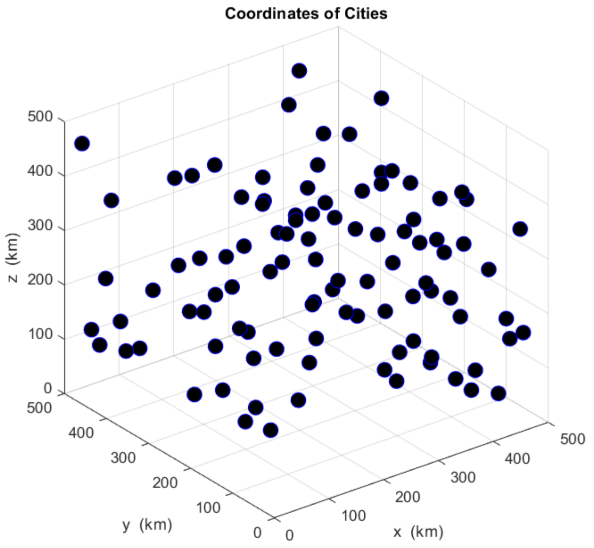


Figure 6. Locations of sensors

We evaluate the efficacy of Nearest Neighbour (NN), Grey Wolf Optimiser Algorithm (GWO), and Genetic Algorithm (GA)-based Approaches by analysing different combinations of these parameters.

6.2.1. NN-based Approach

This subsection evaluates the performance of an NN-based solution. Figure 7 demonstrates the NN's achieved path planning solution in a scenario in Figure 6.

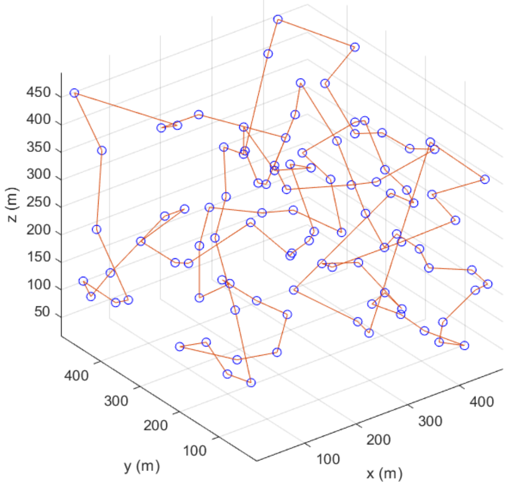


Figure 7. Achieved (9046 m) path planning solution by Nearest Neighbor

6.2.2. GA-based Approach

This subsection evaluates performance of an GA-based solution. Figure 8 demonstrates the GA's achieved path planning solution in 1000 iterations in a scenario in Figure 6.

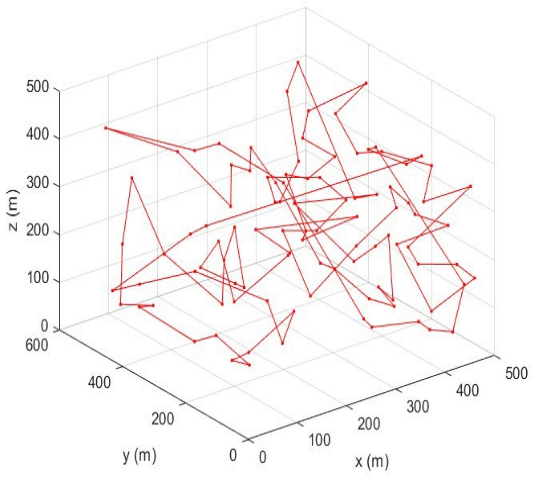


Figure 8. Achieved (11441 m) path planning solution with GA in 1000 iterations

6.2.3. GWO-based Approach

This subsection evaluates performance of an GWO-based solution. Figure 9 demonstrates the GWO's achieved path planning solution in 1000 iterations in a scenario in Figure 6.

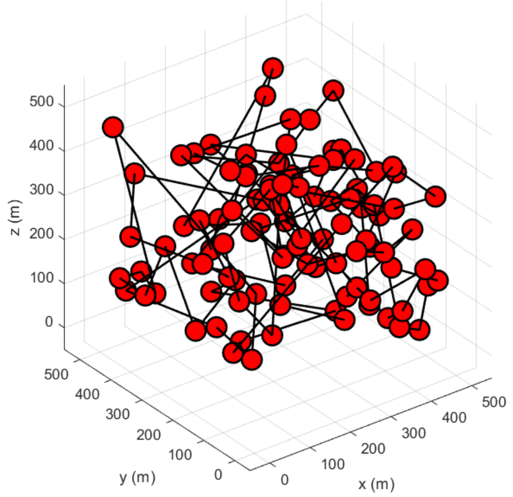


Figure 9. Achieved (17686 m) path planning solution with GWO in 1000 iterations

6.2.4. Discussion

In general, NN-based Approach achieves shorter path than GA-based Approach.

Figure 10 illustrates the total distance travelled by AUV employing multiple algorithms (NN Based Approach, GWO Based Approach, and GA Based Approach) to visit the 100 sensor nodes shown in Figure 6. Based on the data presented in Figure 10, we can make the following inferences about the performance of the algorithms in the scenario involving 100 nodes. According to the general pattern, the NN-based method and GA-based approach are more effective than the GWO-based approach. The neural network-based approach demonstrates superior performance compared to the genetic algorithm-based approach in terms of results up to the 500th iteration. In addition, the NN-based Approach is significantly faster in solving the problem, taking only 0.094679 seconds compared to the GA-based approach's time of 3.508634 seconds (37 times faster).

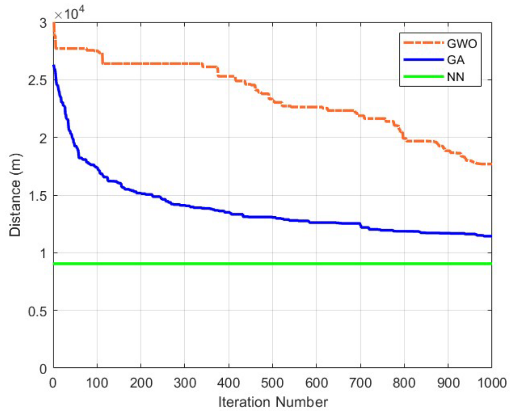


Figure 10. Achieved path lengths for visiting 100 nodes by NN, GWO, and GA-based Approaches

Figure 10 enables us to derive the following conclusions. Although the NN-based strategy quickly found a solution of around 9.05 km, both the GA-based method and the GWO-based approach initially had longer road lengths of 27 km and 30 km in the first iteration. The GA-based strategy outperforms the GWO-based technique significantly at the 100th iteration, achieving a distance difference of 10.07 Km, which is 36.6% less. The NN strategy performs better than the GWO and GA strategies at the 400th iteration where GA strategy achieves 13500 m, nearly half of the path achived by GWO approach 25294 m (46.6% difference with 11794 m). With a distance of 12369 m, the GA strategy keeps its superior performance compared to the GWO approach with 21879 m at the 700th iteration (43.42% difference with 9510 m). The NN-based technique offers not only a speedier and more practical solution but also it provides a shorter path compared to other methods. At the 1000th iteration, the GA-based technique with 11440 m achieved distance significantly beats GWO-based approach with 17686 m, with a performance of 6246 m, which is 35.3% lower than the GWO-based approach.

6.3. Obstacle Avoidance scenario

We evaluate the efficacy of the modified Nearest Neighbor-based method for solving the 3D TSP problem. However, we impose a constraint that makes it prohibitively expensive and impractical to visit node i immediately after node $i-1$.

6.3.1. Modified NN-approach with 50 nodes

This subsection examines the solution to the 3D TSP issue using the modified Nearest Neighbour approach. The path planning solution generated by modified NN for visiting 50 nodes depicted in Figure 1 is illustrated in Figure 11.

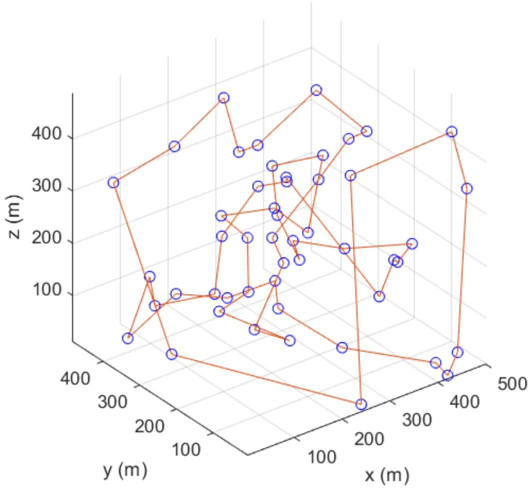


Figure 11. Achieved path planning solution for visiting the 50 nodes by AUV with modified NN under limitations

6.3.2. Modified NN-approach with 100 nodes

This subsection examines the solution to the 3D TSP issue using the modified Nearest Neighbour approach. The path planning solution generated by modified NN for visiting 100 nodes depicted in Figure 6 is illustrated in Figure 12.

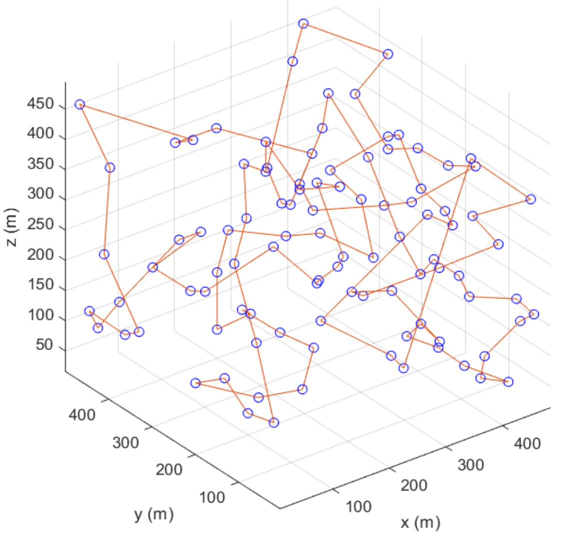


Figure 12. Achieved path planning solution for visiting the 100 nodes by AUV with modified NN under limitations

6.3.3. Discussion

Taking into consideration the overall trend, the NN-based Approach outperforms the modified NN-based Approach. Table 1 shows the total distance travelled by AUV utilising NN-based Approach and modified NN-based Approach under the 50-node scenario in Figure 1 and the 100-node scenario in Figure 6.

We can infer the following conclusions from Table 1. Under the 50-node situation, NN-based approach and modified NN-based Approach achieve virtually comparable performance, with only a slight deviation (134 m, or 2.04\% less than modified NN-based technique). Under the 100-node situation, the NN-based approach and modified NN-based Approach achieve virtually comparable performance, with only a slight deviation (18 m, or 0.2\% less than the modified NN-based technique).

7. CONCLUSION

Research is concentrating on longer and wider exploratory ranges as environmental monitoring becomes increasingly important. Using an autonomous underwater vehicle with a limited battery pack, we theoretically evaluate the energy consumption of the wireless sensor network (WSN) and propose an efficient path-planning strategy for charging it. The WSN has limited energy, therefore we concentrate on charging. To extend the exploration network, many AUVs efficiently charge the WSN. It is possible to significantly increase exploration range and charge efficiency by selecting appropriate diving places and building a path that takes the node's location and data flow into account.

Table 1. Total distance by NN-based Approach and OANN-based Approach under 50-node and 100-node scenarios.

Iteration	Achieved Length
NN with 50 nodes	6322 (m)
Modified NN with 50 nodes	6456 (m)
NN with 100 nodes	9045 (m)
Modified NN with 100 nodes	9063 (m)

Data collection problems for AUVs can be handled using Nearest Neighbour, Grey Wolf Optimiser, and Genetic Algorithm approaches. Based on simulations, the AUV route planning system finds a better solution and converges more quickly than previous algorithms by using Nearest Neighbour.

A physical constraint or obstacle that renders visiting node $\boldsymbol{i}$ soon after node $\boldsymbol{i-1}$ impractical owing to large distance costs is the basis for the Obstacle-Avoided Nearest Neighbour-based solution for the 3D TSP problem. Even yet, the Obstacle-Avoided Nearest Neighbour-based method functions similarly.

8. FUTURE WORKS

In the future, this research can be extended in the following ways. In addition to underwater communication networks, autonomous vehicles for data collection are widely used in the framework of terrestrial wireless sensor networks. The research works (Gul *et al.*, 2020, Gul *et al.*, 2022, Gul *et al.*, 2023, Gul *et al.*, 2024) have investigated data gathering problem from clustered robotic and wireless sensor networks, hence reducing the energy consumption of cluster heads by considering a UAV with limited battery capacity. In underwater communication networks, the data gathering problem can be investigated with autonomous underwater vehicle with a limited battery capacity.

As another future work, we can tackle the problem by considering the energy harvesting models and approaches in the works (Eriş *et al.*, 2023, Eriş *et al.*, 2024a, Eris *et al.*, 2024b).

In the future, we can also tackle the problem by considering more realistic models about the mission, function and working principle of autonomous underwater vehicles.

AUTHORSHIP CONTRIBUTION STATEMENT

Ömer Melih GÜL: Conceptualization, Methodology, Validation, Formal Analysis, Resources, Writing - Original Draft, Writing-Review and Editing, Data Curation, Software, Visualization, Supervision, Project administration, Funding acquisition.

CONFLICT OF INTERESTS

The author(s) declare that for this article they have no actual, potential or perceived conflict of interests.

ETHICS COMMITTEE PERMISSION

No ethics committee permissions are required for this study.

FUNDING

No funding was received from institutions or agencies for the execution of this research.

ORCID IDs

Ömer Melih GÜL:
https://orcid.org/0000-0002-0673-7877

8. REFERENCES

Akyildiz, I.F., Pompili, D. (2005). Underwater acoustic sensor networks: Research challenges. *Ad Hoc Networks*, 3, 257–279.

Blidberg, D.R. (2001). The development of autonomous underwater vehicles (AUV); a brief summary. In Proceedings of the IEEE International Conference on Robotics and Automation (ICRA), Seoul, Republic of Korea, 21–26 May 2001, pp. 122–129.

Bonabeau, E., Dorigo, M., Theraulaz, G. (1999). *Swarm intelligence: from natural to artificial systems* (No. 1). Oxford University Press.

Eris, C., Gul, O.M., Boluk, P.S. (2023). An Energy-Harvesting Aware Cluster Head Selection Policy in Underwater Acoustic Sensor Networks. In Proceedings of the 2023 International Balkan Conference on Communications and Networking (BalkanCom), Istanbul, Turkey, 5–8 June 2023, pp. 1–5.

Eris, C., Gul, O.M., Boluk, P.S. (2024a). A Novel Reinforcement Learning Based Routing Algorithm for Energy Management in Networks. *Journal of Industrial and Management Optimization*, 20 (12): 3678- 3696.

Eriş, Ç., Gül, Ö.M., Bölük, P.S. (2024b). A Novel Medium Access Policy Based on Reinforcement Learning in Energy-Harvesting Underwater Sensor Networks. *Sensors*. 24 (17): 5791.

Cheng, F., Wang, J. (2014). Energy-efficient routing protocols in underwater wireless sensor networks: A survey. *IEEE Communications Surveys & Tutorials*, 16: 277–294.

Cheng, C., Sha, Q. (2021). Path planning and obstacle avoidance for AUV: A review. *Ocean Engineering*, 235: 109355–109368.

Davendra, D. (2010). *Travelling Salesman Problem, Theory and Applications*. InTech.

Fan, R., Jin, Z. (2023). A time-varying acoustic channel-aware topology control mechanism for cooperative underwater sonar detection network. *Ad Hoc Networks,* 149: 103228.

Felemban, E., Shaikh, F.K. (2015). Underwater sensor network applications: A comprehensive survey. *International Journal of Distributed Sensor Networks,* 11: 896832–896845.

Ghafoor, H., Noh, Y. (2019). An overview of next-generation underwater target detection and tracking: An integrated underwater architecture. *IEEE Access*, 7: 98841–98853.

Gjanci, P., Petrioli, C. (2017). Path finding for maximum value of information in multi-modal underwater wireless sensor networks. *IEEE Transactions on Mobile Computing*, 17: 404–418.

Golen, E., Mishra, F. (2010). An underwater sensor allocation scheme for a range dependent environment. *Computer Networks*, 54: 404–415.

Goldberg, D.E. (1989). *Genetic Algorithms in Search, Optimization and Machine Learning*, Addison-Wesley Longman Publishing Co., Inc.

Gül, Ö.M., Acarer, T. (2024). Deniz Taşımacılığı İzlemek için Sualtı Kablosuz Sensör Ağlarında Otonom Sualtı Aracı ile Dayanıklı ve Enerji Farkında Yol Planlama. *EMO Bilimsel Dergi*, 14(2): 71–85.

Gul, O.M. (2024). Energy-Aware 3D Path Planning by Autonomous Ground Vehicle in Wireless Sensor Networks. *World Electric Vehicle Journal*, 15(9): 383.

Gul, O.M., Erkmen, A.M. (2020). Energy-efficient cluster-based data collection by a UAV with a limited-capacity battery in robotic wireless sensor networks. *Sensors*, 20: 5865.

Gul, O.M., Erkmen, A.M., Kantarci, B. **(2022).** UAV-Driven Sustainable and Quality-Aware data collection in robotic wireless sensor networks. *IEEE Internet Things Journal*, 9(24): 25150–25164.

Gul, O.M., Erkmen, A.M. (2023). Energy-Aware UAV-Driven Data Collection with Priority in Robotic Wireless Sensor Network. *IEEE Sensors Journal*, 23 (15): 17667–17675.

Gul, O.M., Erkmen, A.M., Kantarci, B. (2024). NTN-Aided Quality and Energy-Aware Data Collection in Time-Critical Robotic Wireless Sensor Networks. *IEEE Internet Things Magazine*, 7: 114–120.

Gutin, G., Punnen, A. (2002). *The Traveling Salesman Problem and Its Variations. Combinatorial Optimization*, 12, Kluwer, Dordrecht.

Gutin, G. Yeo, A. and Zverovitch, A. (2007). Exponential Neighborhoods and Domination Analysis for the TSP, in The Traveling Salesman Problem and Its Variations, G. Gutin and A.P. Punnen (eds.), Springer.

Johnson, D.S., McGeoch, L.A. (1997). *The Traveling Salesman Problem: A Case Study, Local Search in Combinatorial Optimization*, pp. 215–310. John Wiley & Sons.

Gjanci, P., Petrioli, C. (2017). Path finding for maximum value of information in multi-modal underwater wireless sensor networks. *IEEE Transactions on Mobile Computing*, 17: 404–418.

Golen, E., Mishra, F. (2010). An underwater sensor allocation scheme for a range dependent environment. *Computer Networks*, 54: 404–415.

Kan, T., Mai, R. (2018). Design and analysis of a Three-Phase wireless charging system for lightweight autonomous underwater vehicles. *IEEE Transactions on Power Electronics*, 33: 6622–6632.

Khan, A.U., Somasundaraswaran, K. **(2018).** Wireless charging technologies for underwater sensor networks: A comprehensive review. *IEEE Communications Surveys & Tutorials*, 20: 674–709.

Khan, M.T.R., Ahmed, S.H. (2019). An energy-efficient data collection protocol with AUV path planning in the internet of underwater things. *Journal of Network and Computer Applications*, 135: 20–31.

Kumar, V., Sandeep, D. (2018). Multi-hop communication based optimal clustering in hexagon and voronoi cell structured WSNs. *AEU - International Journal of Electronics and Communications*, 93: 305–316.

Kumar, S.V., Jayaparvathy, R. (2020). Efficient path planning of AUVs for container ship oil spill detection in coastal areas. *Ocean Engineering*, 217: 107932–107945.

Lee, J., Yun, N. (2011). A focus on comparative analysis: Key findings of MAC protocols for underwater acoustic communication according to network topology. In Proceedings of the Multimedia, Computer Graphics and Broadcasting: International Conference, Jeju Island, Korea, 8–10 December 2011, pp. 29-37.

Li, Q., Du, X. (2020). Energy-efficient data compression for underwater wireless sensor networks. *IEEE Access*, 8: 73395–73406.

Liu, C.F., Zhao, Z. (2019). A distributed node deployment algorithm for underwater wireless sensor networks based on virtual forces. *Journal of Systems Architecture*, 97: 9–19.

Mirjalili, S., Lewis, M. (2014). A. grey wolf optimizer. *Advances in Engineering Software*, 69: 46–61.

Pendergast, D.R., DeMauro, E.P. (2011). A rechargeable lithium-ion battery module for underwater use. *J. Power Sources*, 196: 793–800.

Pop, P.C., Cosma, O., Sabo, C., Sitar, C.P. (2024). A comprehensive survey on the generalized traveling salesman problem. *European Journal of Operational Research*, 314(3): 819-835. doi: 10.1016/j.ejor.2023.07.022.

Qiu, T., Zhao, Z. (2020). Underwater Internet of Things in Smart Ocean: System Architecture and Open Issues. *IEEE Transactions on Industrial. Informatics*, 16: 4297–4307.

Ramos, A.G., García-Garrido, V.J. (2018). Lagrangian coherent structure assisted path planning for transoceanic autonomous underwater vehicle missions. *Scientific Reports*, 8: 4575.

Shen, G., Zhu, X. (2020). Research on phase combination and signal timing based on improved K-medoids algorithm for intersection signal control. *Wireless Communications and Mobile Computing*, 2020: 3240675.

Su, Y., Xu, Y. (2023). HCAR: A Hybrid-Coding-Aware Routing Protocol for Underwater Acoustic Sensor Networks. *IEEE Internet Things Journal*, 10: 10790–10801.

Sun, Y., Zheng, M., Han, X., Li, S., Yin, J. (2022). Adaptive clustering routing protocol for underwater sensor networks. *Ad Hoc Networks*, 136: 102953–102965.

Wei, L., Han, J. (2020). Topology Control Algorithm of Underwater Sensor Network Based on Potential-Game and Optimal Rigid Sub-Graph. *IEEE Access*, 8: 177481–177494.

Xie, R., Jia, X. (2013). Transmission-efficient clustering method for wireless sensor networks using compressive sensing. *IEEE Transactions on Parallel and Distributed Syst*ems, 25: 806–815.

Xie, L., Shi, Y. (2014). Rechargeable sensor networks with magnetic resonant coupling. Rechargeable Sensor Networks: Technology, Theory, and Application, 9, 31–68.

Yadav, S., Kumar, V. (2019). Hybrid compressive sensing enabled energy efficient transmission of multi-hop clustered UWSNs. *AEU - International Journal of Electronics and Communications*, 110: 152836–152851.

Yan, J., Yang, X. (2018). Energy-efficient data collection over AUV-assisted underwater acoustic sensor network. *IEEE Systems Journal*, 12: 3519–3530.

Yan, Z., Li, Y. (2023). Data collection optimization of ocean observation network based on AGV path planning and communication. *Ocean Engineering*, 282: 114912–114927.

Yi, Y., Yang, G.S. (2022). Energy balancing and path plan strategy for rechargeable underwater sensor network. In Proceedings of the 2022-4th International Conference on Advances in Computer Technology, Suzhou, China, 22–24 April 2022.

Zenia, N.Z., Aseeri, M. (2016). Energy-efficiency and reliability in MAC and routing protocols for underwater wireless sensor network: A survey. *Journal of Network and Computer Applications*, 71: 72–85.

Zhu, R., Boukerche, A. (2023). A trust management-based secure routing protocol with AUV-aided path repairing for Underwater Acoustic Sensor Networks. *Ad Hoc Networks*, 149: 103212–103225.

Reviewer List of Volume 10 Special Issue 1 (2024)

Duygu ÇAKIR	Bahçeşehir University	Turkey
Gizem KODAK	Girne Amerikan University	North Cyprus
Gizem KAYIŞOĞLU	İstanbul Technical University	Turkey
Gökhan MERSİN	Yıldız Technical University	Turkey
Hasan NAYIR	Yıldız Technical University	Turkey
İsmail Burak PARLAK	Galatasaray University	Turkey
Osman ARSLAN	Kocaeli University	Turkey
Suzan ÜRETEN	Bahçeşehir University	Turkey
Umut TAÇ	Piri Reis University	Turkey
Ömer ÇAYIR	Scientific and Technological Research Council of Turkey	Turkey
Üstün ATAK	Bandırma On Yedi Eylül University	Turkey

Volume: 10 Special Issue: 1 is indexed by

ULAKBİM
TRDİZİN
EBSCOhost
CABI
CiteFactor
Academic Scientific Journals
Crossref
İNFOBASE INDEX
SIS
Scientific Indexing Services
DRJI
Directory of Research Journals Indexing
INTERNET ARCHIVE
Scilit
I2OR
Academic Resource Index
ResearchBib
JOURNAL FACTOR
ScienceGate
BASE
Bielefeld Academic Search Engine
JIF
GLOBAL SOCIETY FOR SCIENTIFIC RESEARCH
JIFACTOR
IIJIF
ROOTINDEXING
JOURNAL ABSTRACTING AND INDEXING SERVICE
ASOS indeks
ASCI
Asian Science Citation Index