ISSN: 2182-2069 / E-ISSN: 2182-2077

Analyzing Security Vulnerabilities in Maritime Ad-Hoc Networks for Real-Time Navigation Data Exchange

K. Karthik[1*], and Krishnamurthy Kumar[2]

[1*]Department of Nautical Science, AMET Institute of Science and Technology, Chengalpet, Tamil Nadu, India. principal@amet-ist.in, https://orcid.org/0009-0008-2399-6249

[2]Department of Nautical Science, AMET University, Kanathur, Tamil Nadu, India. captrkkumar@ametuniv.ac.in, https://orcid.org/0009-0005-2439-0976

Received: February 17, 2025; Revised: March 27, 2025; Accepted: May 06, 2025; Published: May 30, 2025

Abstract

Maritime Ad-Hoc Networks (MANETs) have surpassed key milestones in real-time navigation data exchange during modern maritime operations, including ship-to-ship communication, autonomous navigation and smart port integration. These applications are, however, posed with a variety of security risks due to the network's centralized and dynamic attributes, which may compromise data confidentiality, integrity, accessibility, and navigational safety. This paper studies the comprehensive literature on security weaknesses and gaps in maritime MANETs, analyzing the unique security threats imposed by the maritime environment such as disconnection, lack of infrastructure, and large coverage areas. Extreme gaps in security protocols crafted by existing literature was uncovered as a result of scarce void patching on established security measures. Spoofing, denial of service, and man-in-the-middle exploits proved most prevalent using case study analysis, risk assessment techniques, and simulation-based evaluation. Key mitigative recommendations which have been proofed under maritime contexts are emergency, authentication, and access control focused tailored encryption. There is therefore an urgent need to secure maritime systems with real time communication and navigation features alongside tested blueprints which will lead the charge in developing robust architectures for maritime networks.

Keywords: Maritime Ad-Hoc Networks, Security Vulnerabilities, Real-Time Data Exchange, Navigation Systems, Cybersecurity, Wireless Communication, Maritime Operations.

1 Introduction

Digital transformation is being rapidly adopted in the maritime industry, especially in communication and information exchange (Chauhan & Bhatia, 2025). Additionally, Maritime Ad-Hoc Networks (MANETs) allow for self-contained, mobile communication between ships, buoys, ports, and other autonomous systems without fixed infrastructure controls (Clausen & Jacquet, 2003). These networks are particularly advantageous in the maritime field, where traditional communication limits face challenges due to mobility, spatial dispersion, and sporadic connectivity (Yan et al., 2013). The circulation of up-to-date information regarding a vessel’s area is one of the foundations of safety and efficiency in maritime activities (Bordbar & Bordbar, 2016) Furthermore, it enables tracking, active

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 563-577.
DOI: *10.58346/JISIS.2025.I2.039*

*Corresponding author: Department of Nautical Science, AMET Institute of Science and Technology, Chengalpet, Tamil Nadu, India.

routing, collision avoidance, and coordination with other port traffic (Stavroulaki et al., 2021). A shipping environment that is automated and increasingly reliant on data calls for prompt navigation data at various points. Any interruption or compromise in the flow of information poses catastrophic risks in the most benign scenarios—ranging from ship collisions, navigation blunders, and from ecological harm (Liu et al., 2020; Vasquez & Mendoza, 2024).

The decentralized, wireless, and open components of MANETs gives of a foul cybersecurity whiff. They can be subjected to numerous risks, including eavesdropping, spoofing, DoSing, jamming, and a myriad of other malicious attempts (Goudarzi & Pallis, 2017). In the maritime region, mobile vessels combined high bandwidth, low infrastructure availability, and low computing capabilities tend to amplify these risks even further (Atlam & Wills, 2019). A prominent spoofing attack on maritime GNSS signals in the Black Sea which misled vessel navigation systems is a powerful example of security breach ramifications (Radke, 2017). Although there is a growing need for research on securing MANETs within maritime systems, literature focusing on these frameworks is virtually non existent. Numerous studies have centered around non marinized frameworks focusing on terrestrial mobile networks which are completely different in network configuration, responsive time, and environment based restrictions (Zhang et al., 2016). Equally important is the scarce analysis concerning the vulnerabilities of maritime MANETs during real-time navigation data interchange (Pokhrel et al., 2020).

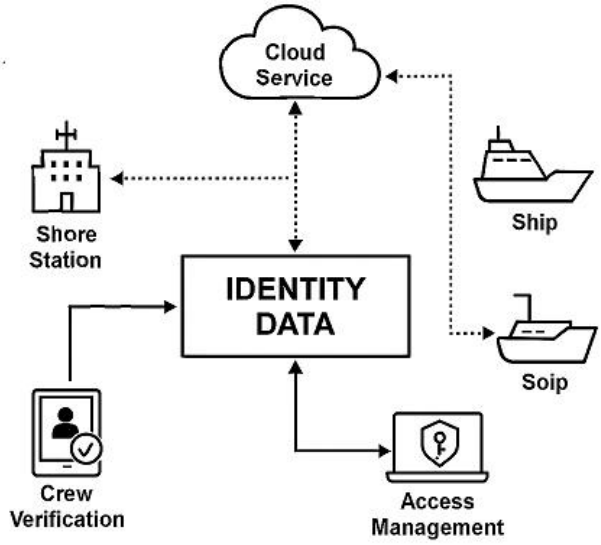

Figure 1(a): Decentralized Identity Data Flow Architecture

This diagram (Figure 1(a)) describes the non-hierarchical circulation of identity information in an maritime ad hoc network. At the core lies the Identity Data hub which communicates with a multitude of vessels, shore stations, clouds, and identity subsystems such as Crew Verification and Access Management. While these nodes do not depend on a central authority for information flow, they can achieve flexible and real-time identity verification at different spatial locations, referred to as identity validation. The cloud service in this case serves as a synchronizing layer aiding in data consistency and accessibility across all maritime elements (Park, 2023). Although this model improves efficiency, it exposes new weaknesses to potential cyber attacks (Ramprasath et al., 2020). As described, “the decentralized approach to managing identity data across various systems encapsulates both the promising opportunities and security vulnerabilities associated with the existing cyber-physical ecosystem of maritime ad-hoc networks,” stressing the importance of sufficient data safeguards within the distributed maritime network.

The diagram (Figure 1(b)) explains the basic principle of Maritime Ad-Hoc Networks (MANETs) through the wireless swap of navigation information between ships. Each ship sends and receives navigation data over the MANET without fixed infrastructure, which facilitates open sea communications. The ship's situational awareness, collision avoidance, and coordinated maneuvers are all dependent on this data flow. However, MANET architecture creates new risks like; possible interception, spoofing, or alteration of information. Therefore, this model needs to be studied in detail for adequate security risk analysis and solid protective measures design in maritime navigation systems.

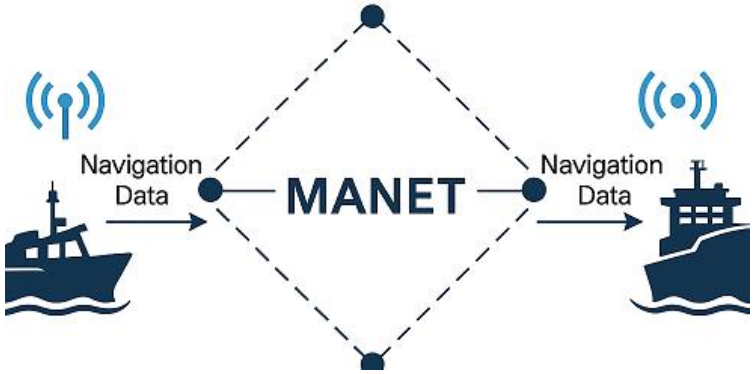

Figure 1(b): Real-Time Navigation Data Exchange in Maritime Ad-Hoc Networks (MANETs)

It is my goal in this research paper to address the shortcomings of existing literature through the analysis of the principal security vulnerabilities associated with maritime ad-hoc networks, focusing on their impact to real-time data transfer (Gajmal & Udayakumar, 2022). The goals of the research are three in number: (1) identify the main threats to maritime MANETs, (2) analyze the effects of these threats on maritime traffic and accident safety, and (3) suggest some solutions that impose reasonable security requirements without greatly affecting performance. This research works within the boundaries of maritime waters, taking into consideration the distinctive cyber technological and operational features that define its cybersecurity environment (Kumaran et al., 2023).

2 Literature Review

The transformation of the maritime industry through digitalization has led researchers to focus more on cybersecurity issues regarding MANETs (Mobile Ad-hoc Networks). The role of these networks is critical, as they facilitate megacity communication without the need for physical infrastructure; however, they present new cyber risks to maritime mobility and logistics systems. This part summarizes the literature on maritime MANET attacks, investigates security measures for real-time navigation data, and describes the primary unresolved problems in research literature.

2.1 Security Vulnerabilities Research for Maritime Ad-Hoc Networks

Haseeb et al., (2019) emphasized that maritime MANETs are not immune to the host of security problems associated with eavesdropping, spoofing, and Denial of Service (DOS) attacks. To make matters worse, the maritime environment is characterized by challenges such as limited bandwidth, sporadic connectivity, and erratic movements. Consequently, these models are highly context-dependent and cannot be applied directly to the sea environment. Zhang et al., (2021) researched marine communication challenges and concluded that decentralized dynamic topologies inhibit the implementation of uniform security policies at the vessel and infrastructure levels. On the other side, Lu et al., (2020) noted that satellite-based Automatic Identification Systems (AIS) and radar they have the

potential to spoof vessel positions and insert false navigational data, resulting in loss of situation awareness. Importantly, a case study conducted (Sultana & Aslam, 2022) had recorded incidents of spoofing attacks in port regions which brings to light the consequences such attacks have on insecure MANET communications. Such incidents resulted in inaccurate reporting of vessel locations, routing of traffic as well as temporary port shutdowns.

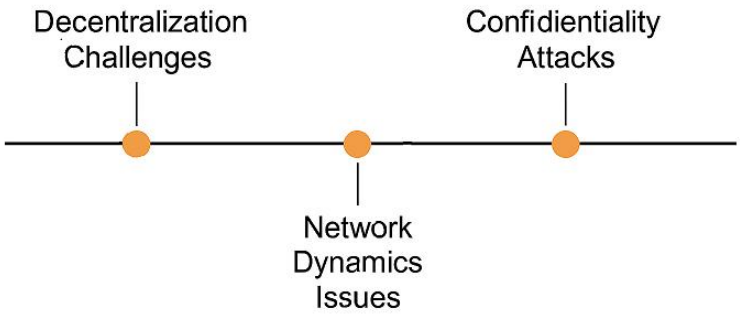

Figure 2: Timeline or Comparison of Security Vulnerabilities in MANETs (Maritime Ad-Hoc Networks)

This chart (Figure 2) gives an overview by time and magnitude of fundamental security weaknesses discovered in Maritime Ad-Hoc Networks (MANETs) as examined in latest investigations. The timeline format helps trace the emergence of threats like spoofing, jamming, denial of service (DoS) attacks, and data injections indicating when they became major issues for maritime communication systems. Furthermore, comparison highlights the frequency of references for each type of vulnerability, illustrating gaps in security protocols and areas where comprehensive counteraction frameworks are absent. The figure enables the understanding of maritime real-time data exchange regarding evolution of circumstantial adversarial forces alongside emerging counter forces hence refined efforts geared towards sustaining dynamic level of security.

2.2 Existing Solutions for Ensuring Security of Real-Time Navigation Data Exchange

In trying to address the vulnerabilities mentioned above, researchers have suggested various security frameworks compatible with the MANET paradigm. A common solution, as pointed out earlier, is encryption. For example, in the domain of maritime security, resource constrained nodes at sea are treated as computationally limited. Hossain & Islam, (2018) proposed a lightweight encryption algorithm for such nodes. Their work indicated that while encryption enhances confidentiality, it does retard the speed at which data is delivered, which is critical in real-time systems. Another important dimension of defense is authentication. A new trust-based authentication system proposed (Akbar et al., (2019) utilizes interaction history among nodes as a basis to grant authentication. Such a system is ideal for mobile networks without a central authority (Hua, 2024). On the downside, the approach resorts to chronic trust score manipulation which, if done by an attacker, can neutralize the whole system. Secure routing protocols have also been studied (Moretti & Tanaka, 2025). For instance, Li et al., (2021) developed an enhancement to the Ad hoc On-Demand Distance Vector (AODV) routing protocol that identifies and contains harmful nodes in real time. While this protocol mitigates routing attempts at black hole or wormhole attacks, scalability and energy consumption issues persist for large fleets. The need to maintain the integrity of information and non-repudiation have drawn attention towards blockchain technology. For example, Yadav & Singh, (2021) suggested a framework using blockchain for sharing navigational data between vessels and coastal authorities. Although it can improve transparency and traceability, there are issues of high processing overhead and bandwidth consumption that need to be addressed in maritime environments.

2.3 Gaps in Current Research

These works, however, do not address gaps found in the existing literature. First, most proposed solutions seem to be either theoretical or only some validated through simulations, with little real-world deployment or field testing. Maritime communication systems tend to behave quite differently from the models simulated in terrestrial environments, as noted (Rahman et al., 2022). Lacking in-depth threat modeling specific to maritime MANETs systems is a clear gap (John & Ghate, 2024). Some existing works either assess spoofing or DoS in isolation and do not examine the impact of multi-vector attacks in ever-changing maritime settings (Nguyen et al., 2021). Additionally, very few works consider the external factors of weather, electromagnetic interference, or marine obstructions, which significantly impact signals and disclosure vulnerabilities (Muller & Romano, 2024). There is also a limited availability of security frameworks or regulatory guidelines concerning maritime MANET security. Smith & Jackson, (2020) note the International Maritime Organization's (IMO) acknowledgment of cybersecurity importance, but the development of specific technical standards for secure MANETs is insufficient. Interoperability and coordination of maritime networks with shore-side systems for realtime navigation data sharing have received very little attention. Increasing integration of satellite and terrestrial communication with vessel networks pose cross-domain vulnerabilities (Chen et al., 2022).

3 Security Vulnerabilities in Maritime Ad-Hoc Networks

3.1 Risks to Data Privacy, Accuracy and Accessibility

Recently, Maritime Ad-Hoc Networks (MANETs) are being employed for real-time exchange of communication and navigation data among vessels, ports, and authorities in the marine industry, however, their wireless and decentralized design poses critical cybersecurity threats that endanger the basic tenets of data privacy, accuracy and accessibility. With regard to confidentiality, the unrestricted access to data carried by a frequency band ensures that nefarious actors can spy sensitive data without permission, this may comprise aiding defined interference such as the location of vessels, as well as their route plans, cargo information, onboard conversations, and many other items. Furthermore, the situation is made even worse by poor encryption standards and authentication failure, in particular due to legacy systems still in use by numerous maritime operators. Another principle of concern, data integrity refers to guarding that the information is not modified as it is moved from one point to the other. Maritime operations are highly dependent on accurate navigation data, and any alteration of data can pose serious risks. For example, a cyber attacker hijacking a ship's current location information may mislead navigation systems which can result in unintended route changes or collisions. Integrity threats can equally arise from the weather data or traffic advisories being modified which can be dire for vessels as they may put them in perilous navigation conditions. At the same time, availability i.e. making certain data and services are accessible at one's need is often the subject of denial-of-service (DoS) attacks or signal jamming. Such attacks are capable of paralyzing communication, situational awareness, and information flow which result in tremendous delays in making timely decisions and proactively responding that risks crew safety and mission accomplishment.

3.2 Proposed Threats Against Maritime Ad-Hoc Networks

Any number of professional maritime MANETs system pose a range of cybersecurity threats, from unskilled system breaches to sophisticated sponsored hacking groups. One example is cybercriminal activities that capture, sell, deploy ransomware, or suspend maritime system operations for profit. These actors can easily access weakly defended networks to steal ship manifests, crew lists, and even

sophisticated financial transactions. An advanced form includes state-sponsored attackers who infiltrate commercial and military vessels to gain strategic intelligence. Such entities possess the means to perform thorough concentrated assault and prolonged spy operations to retain stealth while harvesting operative intelligence or incapacitating fleet control systems. Insider threats related to cybersecurity have also become a significant issue for maritime networks in addition to external threats. Networked systems can be breached, intentionally or otherwise, by crew members or port workers who have access to the systems. A simple example is when an untrained worker uses a USB stick containing a virus and connects it to a navigation terminal, thus, literally 'booting up' malware. Organized criminal syndicates, such as pirates and smugglers, have also become more sophisticated. They take advantage of poorly protected communication lines to simulate movement where GPS signals are altered, signals are jammed, or vessels routing through safe shipping areas are stealthily rerouted to places where cargo can be snatched or detection avoided. Last but not least, bots and malware can be used to automate the exploitation of systematic weaknesses on sheer scales across fleets and ports, potentially dozens or even thousands of interlinked nodes.

3.3 How Security Breaches Affect Maritime Operations

The consequences of security breaches to maritime MANETs can be harsh and extensive. On a simple level, broken communication lines makes it impossible for vessels to receive and share important, timely information, elevating navigational errors to a new height. A ship which has lost accurate GPS positioning data could stray into dire straits, navigate into no-go-areas and collide or even get stranded in perilous zones. From the commercial perspective, these disturbances can severely impede financial returns because of extensive schedule disruptions, spoiled items, and surging insurance premiums. Where some industries may face the worst in the case of route deviation or diversion of cargo, the supply chains operating in unison can get severely crippled - all this would impact sectors that extend well outside the maritime industry. From a safety standpoint, the implications are profound. Cyberattacks which sabotage a sailor's situational awareness or disable the vessel's emergency communication systems pose a direct threat to human life. In critical scenarios, immediate contact with coastal or adjacent maritime traffic is important, and any disruption can be fatal. Furthermore, there are some environmental aspects to take into account. Data intrusion, system malfunctions, or navigation system failures can result in constructive algorithms that collude with the fundamental principles of critical infrastructure. Also, uncontrolled vessel systems could lead to severe adverse outcomes such as spilling fuel in busy shipping lanes, or running the vessel aground in regions with fragile ecosystems. In a word, for commercially intensive shipping, the strength and structural performance of maritime MANETs frameworks brings critical concern for system safety, maritime navigation efficiency, ecological concerns, and international economic stability.

4 Real-Time Navigation Data Exchange in Maritime Ad-Hoc Networks

4.1 Obstacles in Achieving the Timely and Precise Cutting of Information Data Exchange Functions

The maritime industry faces challenges such as intricate vessel movements and unpredictable weather changes requires optimal real-time integration. In tight shipping lanes with heavy vessel traffic, instantaneous navigation information exchange is particularly crucial. However, in maritime ad-hoc networks, vessels face both operational and technical difficulties with precision in timing and accuracy. One of the foremost challenges concerns the dynamic and distributed characteristic of the network.

Because vessels are mobile beyond the enduring reach of coast-based communication systems, sustained contact and commutation with consistent vessel information units is impossible. Ships are prone to frequently changing range of movement, resulting in alternations in the network topology and disruptions in the link. Advanced movement is likely to enhance delays in information transmission, reducing importance or leading to absences in range-ng information loss in presence of data packets. Furthermore, when several ships are attempting to vertically transmit data simultaneously within confined spectrum usage, bandwidth constraints become quite problematic. The existence of very high latency and jitter typically encountered in showcase, Critical Navigation information increases the unreliability of crucial data in drawing spatial references. Additionally the state of the atmosphere is likely to be relatively unstable yielding interference and increase the probability of corrupted or missing ranging information

4.2 Importance of Secure Communication for Navigation Safety

Security integration in communication within maritime ad-hoc networks is very important, especially in navigation safety. A vessel gets real time data for making decisions like speed control, heading, weather avoidance and traffic coordination. One of the major risks is bringing malicious interference to data streams; this captures, alters and delays information. As a result, the safety of the crew, the ship, and the marine setting is put in a significant hazard. Secure communication means that data shared among the vessels, satellite systems, and shore stations is received on time and it can be trusted.

This also means that messages are delivered under checks; they are genuine and have not been modified during transmission. Failure to do so would make vessels easy prey due to autonomy or misleading signals and information which increase the probability of navigational mistakes or even accidents. Additionally, the needs for secure communications are also required for international policies and marking processes which increasingly demand robust cybersecurity measures for critical infrastructure, Transport Maritime included. With the industry shifting to high digital dependence, Maritime Operations has need for supportive advanced autonomous vessels alongside dependable secured navigation intelligent system technology.

4.3 Existing Protocols and Technologies for A Data Exchange

A number of real time protocols and technologies for navigation data exchange in maritime ad hoc networks are in utilization. One of the most prominent is the Automatic Identification System, wherein vessels transmit their position, speed, and heading to other vessels and shore authorities, and enables coastal states to share information. While fundamental situational awareness, systems do not have cruise security intergrated and thus are open to a wide range of spoofing and interference. Technologies such as Global Navigation Satellite Systems (GNSS) also provide aid in essential location information, although they too are subject to disruption through jamming and spoofing attacks. The incorporation of satellite communication systems to modern vessels enhances coverage, reliability, and communications resilience in open-sea scenarios. Furthermore, throughout the undergoing research in maritime ad-hoc networks, sustained node disconnection and drift mobility are tackled through mesh networking and multi-hop routing protocols. Routinely, TCP/IP protocols are incorporated with maritime incarceration while new initiatives MDCS is projected to enhance communication standards systems interoperability based on standards. Still, there are gaps in incorporating complex encryption, authentication, and anomaly identification techniques into current frameworks for the purpose of data exchange.

5 Analyzing and Assessing Security Vulnerabilities

This study uses a combination of threat modeling, empirical risk evaluation, and case-based analysis to investigate security vulnerabilities of Maritime Ad-hoc Networks (MANETs). The analysis begins with the decomposition of the maritime communication system that contains mobile ad-hoc nodes like vessel transceivers, satellite relays, and port-side observation units. The STRIDE threat modeling framework (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege) is applied to systematically map possible threats to the network architecture constituents. Each of the mapped threats is analyzed using a DREAD-based risk analysis determining the damage, reproducibility, exploitability, number of affected users, and discoverability. This approach provides a layered understanding of the operational and technical risk exposure in real-time navigation data sharing.

Based on the amount of each type of threat recorded, Figure 3 maps the distribution of common security vulnerabilities in maritime ad-hoc networks (MANETs). Out of all the threats identified, jamming seems to be the most common, reaching a staggering 35 instances which points to its ability in neutralizing wireless links employed in the exchange of real-time navigation data. Following closely are eavesdropping and spoofing, both hovering around 30 instances each portraying the degree to which adversaries take advantage of feebly secured or inadequately encrypted communications to intercept or impersonate the data sent from the navigation systems. Data injection and denial of service (DoS) attacks appear much less often, at roughly 22 and 18 instances respectively, but still pose significant risk to the integrity and availability of services within the network. The figure reveals that there is a need for multi-layered security approaches in MANETs to protect them from diverse forms of attacks, particularly aimed at the trustworthiness and confidentiality of various navigational communications. A risk assessment matrix identifying the impact and likelihood of various security threats in maritime ad-hoc networks is shown in Figure 4. As you can see, both impact and likelihood increase sequentially across categories from “Very Low” to “Critical.” The greatest proportion of risks remains within the Critical impact zone, with likelihood surging to 25 for jamming, spoofing, and coordinated cyberattack threats. This suggests that high-impact threats—jamming, spoofing, and coordinated cyberattacks—inflict staggering potential damage, are becoming more commonplace, as observed in the figure. Strong emphasis on loss mitigation and damage control is required for strategies designed to combat threats that reside the high range to critical risk zones, which are alarming in the figure.

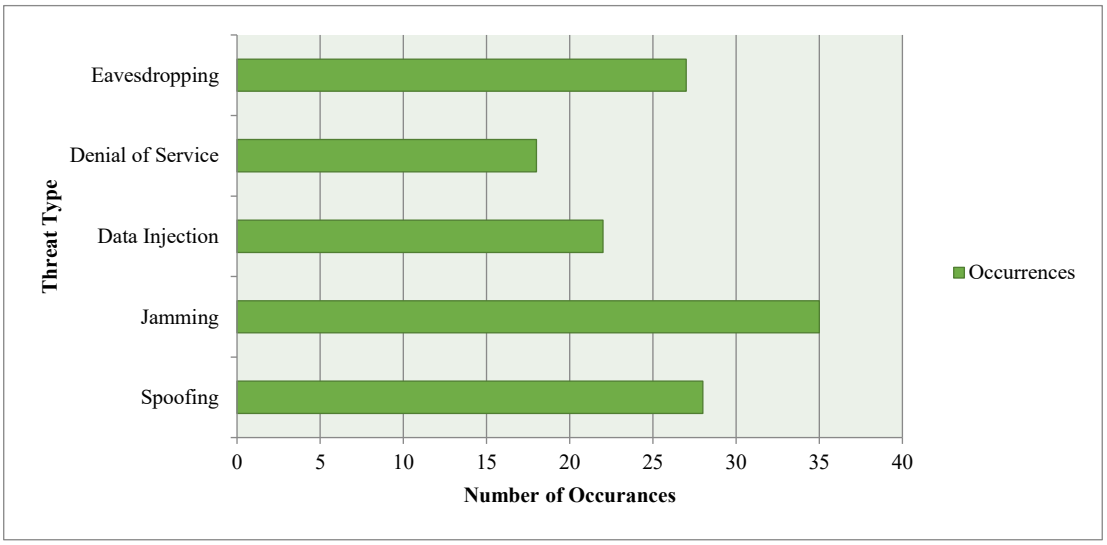

Figure 3: Distribution of Common Security Threats

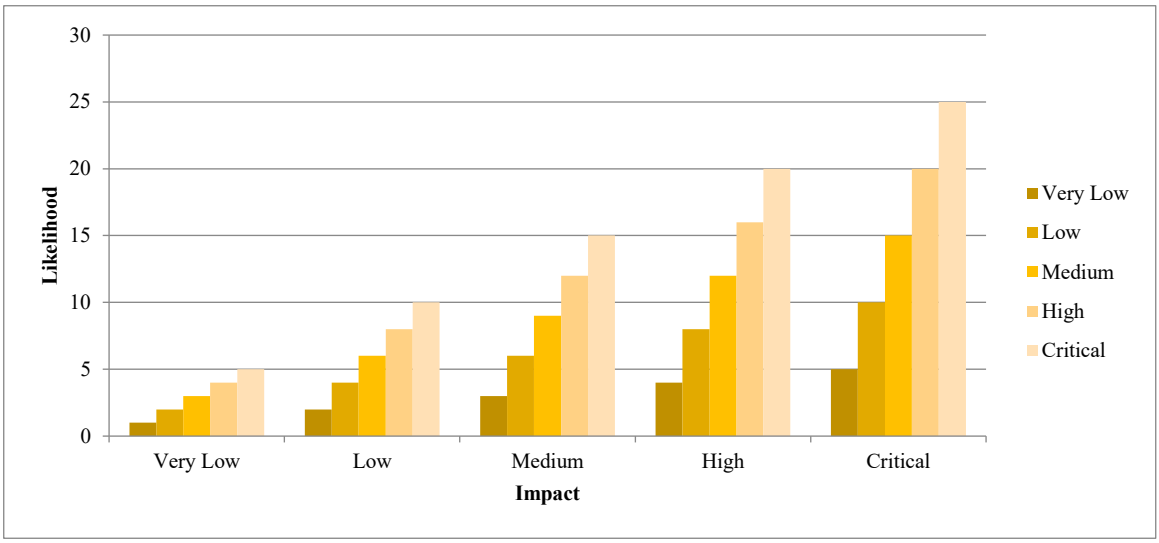

Figure 4: Risk Assessment

Figure 5 illustrates the time flow of activities following the detection of a spoofing attack in a marine ad-hoc network, measured in hours from the point of detection. The graph indicates about nine hours of managed 'system recovery' following 'port alert triggering', 'incident response' and 'logging anomalies'. 'Spoonfing Detection' comes first in the timeline, followed by 'AIS Anomaly Logging', which indicates automation protocols kicking into action. The chart captures an almost linear progression upon reaching key components of the response cycle. This image underscores the intricate nature of cyber incident response in maritime scenarios, emphasizing the need for automated alerts and swift coordinated responses designed to limit operational pauses and ensure navigational safety during seamless transitions.

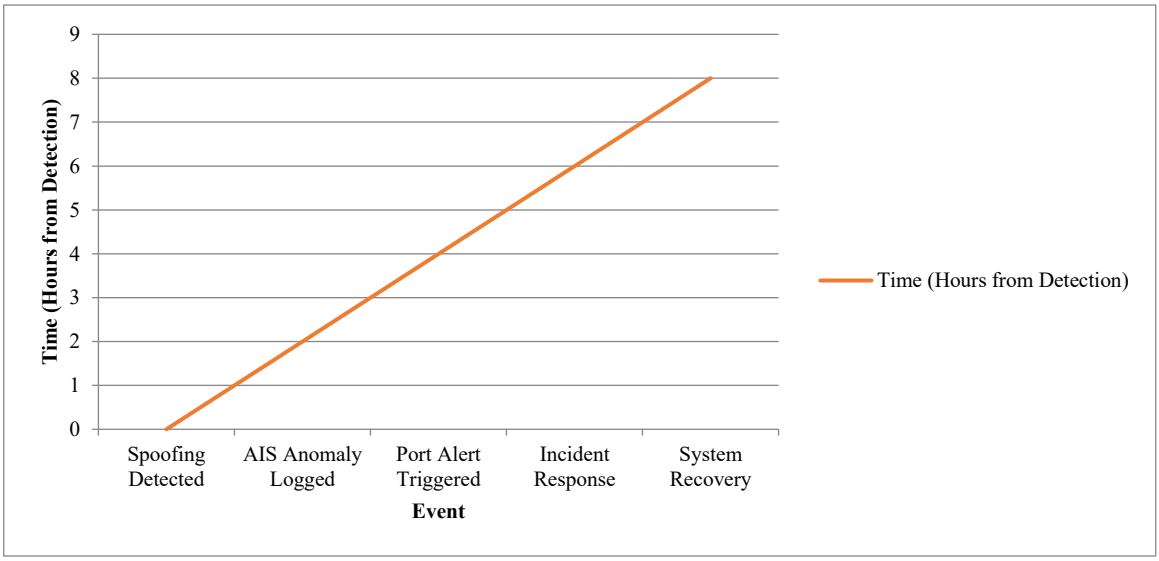

Figure 5: Incident Timeline (Hours from Detection)

Figure 6 depicts the grade of severity concerning each category of threat concerning the maritime ad-hoc networks through the lens of the STRIDE model – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS). Every threat is measured from 1-5, with Spoofing and Information Disclosure rated as the most severe (5), due to the steep risks they pose against navigational superiority

and data confidentiality. DoS and Tampering threats are also rated significantly (4), thus indicating serious damage to service availability and data integrity. Repudiation is seen as less important in this region of the world, scoring a 2. The figure depicts that considerable attention and effort need to be applied to strategically defend high-severity threats for effective secure communications in maritime endeavors. A set of tools and methods were applied to simulate network behavior, conduct vulnerability assessments, and capture various attack patterns. To simulate communication scenarios in mobile ad-hoc networks, NS-3 was utilized to simulate the injection of jamming, black hole routing, and man-in-the-middle attack interference. Wireshark was used in a packet-level traffic analysis for protocol dissection and detecting leakages of sensitive information. Penetration testing for malicious spoofing and unauthorized access was performed using tools in the Kali Linux environment.

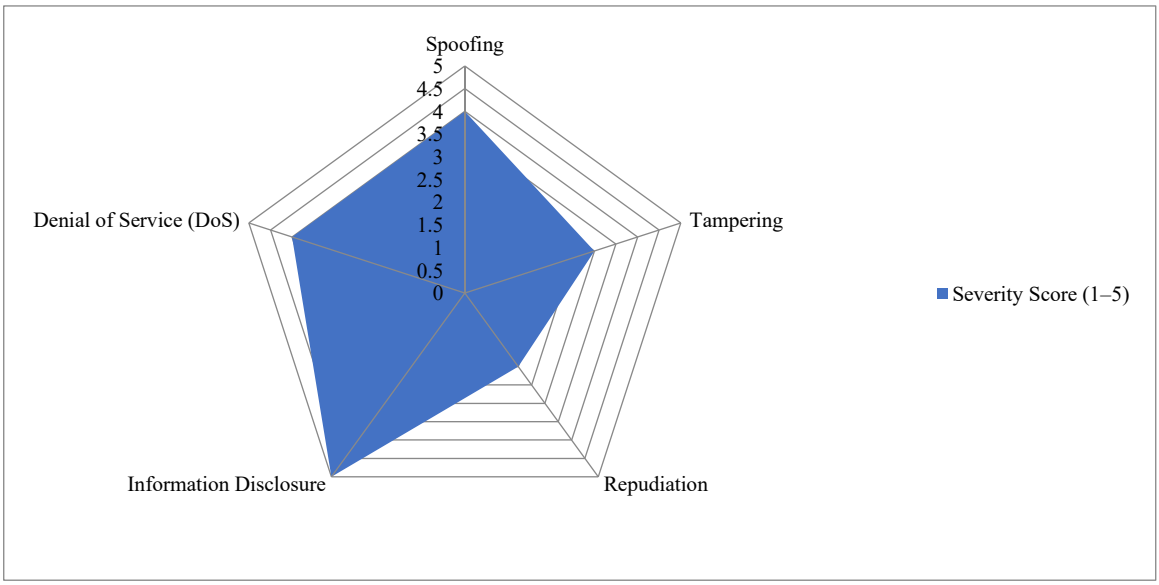

Figure 6: STRIDE Threat Model

Threat intelligence was further enhanced by the mapping of exploits to maritime technology resources from the CVE database. All these efforts facilitated a high-fidelity risk assessment revealing both immediate and latent vulnerabilities in the real-time communication flows. Besides conducting simulated analyses, the study also looks into several prominent case studies to situate the findings. An illustrative case is the 2017 Black Sea GPS spoofing incident where multiple vessels reported incorrect positioning data. Signals even purported to place certain ships on land. This ordeal demonstrated the extent to which attackers can easily target satellite navigation systems without any form of defense. Another case of concern is in the Strait of Hormuz where in 2019 fictitious vessels created using false AIS (Automatic Identification System) signals, aboard what were purportedly non-existent ships, caused chaos within maritime traffic control. The 2020 ransomware attack on a major port authority in Europe is also relevant as it attacked the port's digital infrastructure which served as a backbone for ship-to-shore communication, illuminating the relationship between maritime operational technology (OT) and information technology (IT) systems. Lastly, a jamming attack simulation through NS-3 showed that moderate jamming could incur a packet loss of more than 60%, severely undermining real-time navigation data exchange. These scenarios highlight the lack of cybersecurity in mobile ad hoc networks (MANETs) and the consequences of insufficient protective measures, making them case studies for the need of proactive and resilient cyber security strategies.

6 Mitigation Strategies

6.1 Proposed Solutions for Enhancing Security in Maritime Ad-Hoc Networks

As we have already pointed out, navigation data is of paramount importance. Likewise, the vulnerabilities of Maritime Ad Hoc Networks (MANETs) underscore the need of having solid and flexible security measures. Apart from specialized overarching restrictions, MANETs carry features of traditional mobile networks. Moreover, they function in an uncontrolled, self governing manner, which makes classical network security techniques obsolete. System security could be significantly improved in MANETs if a multi-comm layered security approach, including physical, network and application layers, were to be put in place. For instance, network layer can employ intrusion prevention, whilst application layer may use anomaly detection, thus providing holistic approach to protection. Also, civilian applications have shown growing interest in security maritime data transactions by other means of securing data by using blockchains due to their openness and unchangeableness, which makes them immune to modification of altered documents. Such measures, however, should take into account the constraints inherent to maritime contexts, like the low bandwidth, intermittent connectivity, and the need for energy conservation on the vessels.

6.2 Achieving Encryption, Authentication, and Access Control Policies

The implementation of security in MANET networks is achieved through measures such as confidentiality, integrity and authenticity through the proper application of cryptographic techniques. For instance, in real-time navigation scenarios, data protection during transmission can be assured by using light-weight end-to-end encryption algorithms like Elliptic Curve Cryptography (ECC). Another equally important measure is authentication, which certifies the identity of communicating nodes prior to information exchange. This is performed using Public Key Infrastructure (PKI) which employs digital certificates to validate vessels and shore and station counterparts. Mutual authentication can make trust associations stronger among nodes therefore reducing impersonation and man-in-the-middle attack risks. These steps are accompanied by access control mechanisms, such as Role-Based Access Control (RBAC), which restrict access to data based on designated roles and responsibilities. For instance, some port authorities may be granted wider rights compared with general cargo vessels. With these enabling mechanisms, it can be guaranteed that sensitive navigation information is used only by trusted otherwise authorized participants.

6.3 Strategies for Improvement of Cyber Resilience in Real-Time Navigation Data Exchange

To increase the real-time navigation data exchange resilience within maritime networks, adopting a proactive cybersecurity approach from the onset is essential. Primarily, communication protocols should be designed with redundancy to allow data rerouting through alternate pathways in the case of node failure or an attack. The use of alternative communication media such as VHF, subordinated to satellite and short-range mesh, ensures continuity of access even when one system is compromised. Second, automated real-time Intrusion Detection and Prevention Systems (IDPS) tailored to maritime environments should be implemented to detect anomalies and respond to threats in real time. Such systems need to be adaptive to changing topologies and usage patterns of the network. Third, establishing regular security audits, software updates, and vulnerability assessment checks should become routine policy within maritime stakeholders' vessels. International standardization of cybersecurity protocols under the International Maritime Organization (IMO) would facilitate maritime cooperation and ensure uniform practices worldwide. Lastly, addressing the human element of risk through enhanced training

and drills for maritime personnel to improve cybersecurity awareness will target a primary vulnerability in cyber defenses.

7 Future Research Directions

In the context of maritime ad-hoc networks (MANETs), much work has been done in attempting to identify and alleviate security threats, but several significant gaps continue to exist. It is necessary to develop threat models unique to maritime situations since they differ from any other terrestrial or aerial ad-hoc networks regarding their mobility characteristics, node density, and infrastructure. Research should focus on the emerging attack surfaces created by maritime-specific mechanisms, for instance, the Automatic Identification System (AIS) and the Electronic Chart Display and Information System (ECDIS) as well as satellite-based tracking systems that are unique to warfare. Furthermore, the combining of physical and cyber malfeasance known as multi-vector assaults needs to be analyzed more deeply. An example of a malfeasance of this nature is GPS spoofing coupled with denial of service (DoS) attacks that threaten the fundamental functioning of navigation. Other applicable validation could include empirical research using simulated or actual maritime traffic data to determine the operational validity of the developed security models. The automation of processes in the maritime domain, the Internet of Things (IoT), Scalable AI (SAI), and mobile ad-hoc networks pose new challenges in securing data exchange that necessitates urgent attention. For instance, regarding cyber defense, intelligent robotics could dramatically transform the autonomous vessel industry, not to mention the implementation of modern cloud technologies within ship operations. Robotics and Information Technology (IT) integration petrochemically augments the technical performance of a vessel, enhancing its operational possibilities and making it capable of situational–lead shaper operations. Advancements in providing quality control and IT integration with the emerging tech of the Industrial Internet of Things could result in the autonomous decision-making of your vessel, boosting its situational awareness and command integration. Security and Reliability of Information Systems: Supporting the security aspects of mobile ad-hoc networks should cater to the enhancement of cyber defense. Security risks increase with mobility. Everything from technical capabilities and monitoring requirements to administrative controls must be enhanced to provide needed safety. Mobile Ad-Hoc Networks: Framework Tech Architecture constituting easier managing Intelligent Robotics Systems and other onboard vessels fitted with IT requires developing liberalize approaches to make cyber defense of fleets and vessels a proactive opportunity. Besides lifting numerous limitations, autonomous vessels at the same time impose self-deployed ground rules. Autonomous vessels preserve command superiority while allowing situational potential along with self-restraint in routing behavior to effect other controlled areas.

It is evident that multifaceted approaches from different sectors and practitioners are required to solve the intricate problems of security in maritime mobile ad-hoc networks (MANETs). Maritime traffic not only involves a variety of players but also traverses various administrative boundaries. There technically exists a need to unify system remotely controlling these vessels; therefore, communication and surveillance have to be properly managed. Maritime authorities as well as cybersecurity practitioners, network architects, and even international diplomatic entities need to be included in the focus of forthcoming studies. Seamless communication and data transfer between states requires that international protocols and security measures be standardized. Constituent members of the International Shipping Association (ISA) as well as the International Telecommunication union can help maritime bordering nation in setting these controls. Moreover new maritime researchers and practitioners need to be trained in the interdisciplinary fields of maritime transport and cybersecurity, which in turn would help develop the new ideas needed to guarantee maritime security.

8 Conclusion

The current study has investigated the serious security gaps associated with Maritime Ad-Hoc Networks (MANETs), particularly their impact on real-time navigation data exchange. The investigation described various forms of spoofing, data tampering, denial-of-service (DoS) attacks, and unauthorized access that take advantage of the fluid and self-governing structure of MANETs. These vulnerabilities may severely undermine ship safety, disrupt maritime activities, and threaten significant commercial and strategic interests. The analysis of security measures available and the practices of known attacks highlights the necessity of developing in-depth, context-sensitive cybersecurity solutions for the maritime domain. The safeguarding of real-time navigation data is more than a technical obligation; it serves as an essential foundation fortifying maritime safety and vessel operational reliability. Erroneous and manipulated data in busy sea lanes during critical strategic maneuvers can culminate in catastrophic collisions, grounding incidents, and disastrous communication breakdowns. These risks can be profoundly reduced through the use of encryption, authentication, access control, perpetual monitoring with intrusion detection systems, and strong stakeholder engagement. With increasing reliance on interconnected digital systems, vessel operators and maritime regulatory authorities must prioritize the protection of navigation data. The ramifications of the investigation go beyond diagnosing contemporary issues—they indicate an approach for improving maritime cybersecurity. There are several paths which advocate the strengthening the vulnerability of maritime communications, such as the development of encryption methods, the application of artificial intelligence in detection systems, international cooperation, and standardization. In the end, defense of MANETs guarantees, in addition to safeguarding navigation data, the complete and precise information regarding safety, efficiency, and trust for international sea operations. Future research, funding, and collaboration will be crucial for addressing the evolving dangers and preserving maritime connectivity.

References

[1] Akbar, M., Ali, M., & Nazir, B. (2019). A trust-based authentication scheme for ad-hoc networks in maritime environments. *Journal of Communications and Networks, 21*(6), 567–576.

[2] Atlam, H. F., & Wills, G. B. (2019). IoT security, privacy, and ethics: Challenges and solutions. *Future Internet, 11*(3), 60.

[3] Bordbar, G., & Bordbar, M. (2016). Investigating the impact of traffic safety training on reducing risks and casualties of traffic accidents of elementary schools' pupils in villages of Salfechgan Arak axis in 2012 based on Health Belief Model (HBM). *International Academic Journal of Business Management, 3*(1), 72–82.

[4] Chauhan, P., & Bhatia, A. D. (2025). Digital Transformation in Public Sector ICT: A Case Study-Based Comparative Analysis. *International Academic Journal of Innovative Research, 12*(3), 27–32. https://doi.org/10.71086/IAJIR/V12I3/IAJIR1222

[5] Chen, T., Alshamrani, A., & Li, J. (2022). Cross-domain cybersecurity strategies for integrated maritime and terrestrial networks. *Computer Networks, 215,* 109183.

[6] Clausen, T., & Jacquet, P. (2003). *Optimized link state routing protocol (OLSR)* (No. rfc3626).

[7] Gajmal, Y. M., & Udayakumar, R. (2022). Privacy and utility-assisted data protection strategy for secure data sharing and retrieval in cloud system. *Information Security Journal: A Global Perspective, 31*(4), 451-465.

[8] Goudarzi, S., & Pallis, E. G. (2017). Security threats in wireless ad hoc networks: A survey. *Computer Networks, 123,* 47–65.

[9] Haseeb, K., Abbas, H., & Islam, N. (2019). Threat modeling and mitigation strategies for maritime ad-hoc networks. *Wireless Networks, 25*(2), 685–699.

[10] Hossain, M., & Islam, S. (2018). Lightweight encryption for secure data exchange in maritime ad-hoc networks. *IEEE Access, 6,* 32789–32799.
[11] Hua, Z. L. (2024). Elucidating the Role of Cytochrome p450 Enzymes in Drug Metabolism and Interactions. *Clinical Journal for Medicine, Health and Pharmacy, 2*(3), 1-10.
[12] John, B., & Ghate, A. D. (2024). Digital Risk Management: A Study of How Firms Mitigate Digital Risks and Threats. *Indian Journal of Information Sources and Services, 14*(4), 16–21. https://doi.org/10.51983/ijiss-2024.14.4.03
[13] Kumaran, U., Thangam, S., Prabhakar, T. V. N., Selvaganesan, J., & Vishwas, H. N. (2023). Adversarial Defense: A GAN-IF Based Cyber-security Model for Intrusion Detection in Software Piracy. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14*(4), 96-114. https://doi.org/10.58346/JOWUA.2023.I4.008
[14] Li, J., He, Z., & Qiu, M. (2021). Secure AODV-based routing protocol for maritime communication systems. *Sensors, 21*(4), 1234.
[15] Liu, L., Xu, Y., & Yu, B. (2020). Cybersecurity for maritime navigation: Threats and risk management. *Maritime Policy & Management, 47*(7), 881–899.
[16] Lu, Y., Zhang, P., & Li, F. (2020). AIS vulnerabilities in maritime communication systems. *Maritime Informatics Journal, 3*(1), 45–58.
[17] Moretti, A., & Tanaka, H. (2025). Securing Multi-Modal Medical Data Management System using Blockchain and the Internet of Medical Things. *Global Journal of Medical Terminology Research and Informatics, 2*(1), 15-21.
[18] Muller, H., & Romano, L. (2024). An Exploratory Study of the Relationship Between Population Density and Crime Rates in Urban Areas. *Progression Journal of Human Demography and Anthropology, 1*(1), 28-33.
[19] Nguyen, H. T., Pham, D. L., & Le, V. (2021). Modeling cyber threats in maritime IoT systems. *Sensors, 21*(12), 4092.
[20] Park, H.-J. (2023). Eco-friendly Computing Models for Sustainable Data Center Cloud Applications. *International Academic Journal of Science and Engineering, 10*(3), 26–29. https://doi.org/10.71086/IAJSE/V10I3/IAJSE1028
[21] Pokhrel, S. R., Basnet, M., & Kim, D. (2020). A survey of maritime cyber security and its future. *IEEE Access, 8,* 113494–113511.
[22] Radke, M. (2017, July). GNSS spoofing attack in the Black Sea. *Maritime Executive.* https://www.maritime-executive.com
[23] Rahman, M. S., Chowdhury, M. A., & Jin, Y. (2022). Experimental validation of secure maritime MANET protocols. *IEEE Internet of Things Journal, 9*(18), 17983–17994.
[24] Ramprasath, J., Ramya, P., & Rathnapriya, T. (2020). Malicious attack detection in software defined networking using machine learning approach. *International Journal of Advances in Engineering and Emerging Technology*, *11*(1), 22-27.
[25] Smith, L., & Jackson, T. (2020). The policy gap in maritime cybersecurity. *Journal of Maritime Affairs, 19*(4), 521–538.
[26] Stavroulaki, A. V., Kalogeras, A. P., & Trakadas, P. (2021). Survey on maritime navigation systems: Challenges and future trends. *Sensors, 21*(9), 3086.
[27] Sultana, T., & Aslam, N. (2022). Real-time detection of spoofing attacks in smart port MANETs. *Ad Hoc Networks, 127,* 102743.
[28] Vasquez, E., & Mendoza, R. (2024). Membrane-Based Separation Methods for Effective Contaminant Removal in Wastewater and Water Systems. *Engineering Perspectives in Filtration and Separation, 1*(1), 21-27.
[29] Yadav, V., & Singh, R. (2021). Blockchain for secure navigation data sharing in maritime networks. *Ocean Engineering, 234,* 109259.
[30] Yan, H., Lin, Z., & Song, X. (2013). An overview of maritime communication networks. *IEEE Wireless Communications, 20*(5), 146-152.

[31] Zhang, P., Wang, F., & Guo, M. (2016). Secure routing in mobile ad hoc networks: A review. *Security and Communication Networks, 9*(12), 1416–1429.
[32] Zhang, W., Wang, Y., & Kim, H. (2021). A survey on maritime ad-hoc networks and their security challenges. *IEEE Systems Journal, 15*(3), 4330–4341.

Authors Biography

Capt. K. Karthik graduated with a Bachelor's degree in Physics and is a Master Mariner with 16 years of sea-going experience on various dry and liquid cargo vessels, including crude oil, product, and chemical tankers, general cargo, and bulk carriers. He began his academic career with AMET University in 2007 and has since held several key positions, including Professor, Director – Centre for International Relations, Dean – Post Sea and Simulator Training, and currently serves as the Dean and Head of the Department of Nautical Science. His professional interests span maritime education, simulator-based training, youth development. He holds a post-graduation in Shipping and logistics and yoga for human excellence. He is currently the principal of AMET Institute of science and technology, Maersk Centre of Excellence campus.

Capt. Krishnamurthy Kumar (more fondly known as Capt R K Kumar) was a state-level merit scholarship holder in his High-School Board examinations. He passed out from Training Ship "Rajendra" in First Class in 1974 and cleared his MASTER (FG) Competency Examinations in 1983 in first attempt. After serving at sea for 20 years in various ascending ranks, he came ashore as Principal Surveyor with M/s J.B. Boda Surveyors where he was involved in investigating several Casualty incidents such as Groundings, Collisions, major fires, Mega cargo claims and GA surveys. He had also done several consultancy assignments for Project Cargo shipments and turn-key projects. After 12 years as a surveyor, he joined the CCTL Container terminal serving 4 years as Operations Head under P&O ports. He, along with his two-member team, won the second prize amongst all the 21 global container terminals of P&O Ports for "innovative OHSE measures".

Capt. RKK is currently serving as Associate Professor in AMET University for past 20 years having joined as a Marine faculty in 2004. His tenure includes 3 years as Dean of Nautical Science and chairperson of Maritime Studies.

He is a member of the prestigious CMMI, India and an Ex- Fellow of the Institute of Chartered Shipbrokers, UK. He won the South-India topper's Prize in the Institute's Examination in Shipping Practice in 1996. He is also currently the Indian Ambassador for CHIRP MARITIME, United Kingdom aimed at promoting awareness of confidential Reporting of Maritime Incidents amongst Seafarers.