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

Designing Intrusion Detection Systems for Maritime Wireless Sensor Networks and Smart Port Infrastructures

K.R. Chidambaram[1*] and P. Rajan[2]

[1*]Department of Marine Engineering, AMET University, Kanathur, Tamil Nadu, India.
chidambaram.kr@ametuniv.ac.in, https://orcid.org/0009-0000-5311-1394

[2]Department of Marine Engineering, AMET University, Kanathur, Tamil Nadu, India.
prabhakaranrajan@ametuniv.ac.in, https://orcid.org/0009-0006-9720-123X

Received: March 03, 2025; Revised: April 11, 2025; Accepted: May 14, 2025; Published: May 30, 2025

Abstract

The level of automation, operational efficacy, and situational awareness in maritime domains has increased due to the development of smart port facilities along with the global deployment of Maritime Wireless Sensor Networks (MWSNs). Increased automation enables unparalleled connectivity, which in turn, has acute implications for cybersecurity risks. The broadened span of integration within systems automatically heightens the attack surface susceptible to numerous cyber threats. This paper elaborates on the design and architecture of a machine-learning Intrusion Detection Systems (IDS) for Mobile Wireless Sensor Networks (MWSNs) in smart ports. This system applies supervised-learning techniques to define attacks into multiple classes, such as denial of service (DoS), spoofing, and packet injection/alteration. Focused simulation tests aimed at evaluating realistic maritime communication scenarios; the analysis from the simulations confirms that the system provides high detection rates, maintains low false-positive outcomes, and enhances processing efficiency under real-time conditions. Tailored agile intelligent IDS designed for smart ports severely undermined the maritime systems cybersecurity.

Keywords: Intrusion Detection System (IDS), Maritime Cybersecurity, Wireless Sensor Networks (WSN), Smart Port Infrastructure, Machine Learning, Cyber Threat Detection, Simulation-Based Evaluation.

1 Introduction

The maritime sector has been transformed by the introduction of the Internet of Things (IoT) and wireless technologies. This is exemplified with the creation of Maritime Wireless Sensor Networks (MWSNs) which contain clusters of sensor nodes placed on vessels, port infrastructure and other maritime equipment which can monitor and self-regulate their surroundings in real-time (Kim et al., 2016). MWSNs contribute towards the increased safety of navigation, enhanced logistic efficiency, and improved situation awareness in maritime domains (Li & Huang, 2019). Furthermore, smart ports of the new age are transforming into one of the pillars of port 2.0 Ramprasath (2020). Such infrastructure leverages IoT devices, cloud and edge computing, and automaton, to optimize the servicing of cargo and traffic, as well as monitor ecological operations (Yin et al., 2020). The modern smart ports are interlinked

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 858-870.
DOI: *10.58346/JISIS.2025.I2.057*

*Corresponding author: Department of Marine Engineering, AMET University, Kanathur, Tamil Nadu, India.

with other regions using MWSNs which makes data transmission, equipment remote control, and human error eradication possible as well as improved operational efficiency (Zhang et al., 2021).

Nonetheless, the increasing cyber-physical digitization of maritime domains has brought substantial threats with it Mleh et al., (2023). The accessibility and diversification of MWSNs subjects them to different kinds of cyber-attacks such as DoS (Denial of Service), Spoofing, Data Injection, along with Eavesdropping (Cheng et al., 2017). Specialized naval networks are also distinguished from other networks by their almost continual existence in rugged resource-scarce regions. These, unlike their land-based counterparts, pose a greater challenge because security measures need to be efficient, uncomplicated, and dependable (Wang et al., 2020). Against this backdrop, Intrusion Detection Systems (IDSs) are acquiring prominence as a major line of defense for navy cyber networks. An IDS actively controls network traffic by watching and controlling windows of net-connectivity to discover discrepancies from regular patterns and responses to them (Sharma & Gupta, 2020). In as much as the functioning of a computer network is integrated within any modern naval architecture, MWSNs posses features of wireless sensor networks that are maritime in nature (Khyade et al., 2018; Mthembu & Dlamini, 2024). This translates into practical design requirements for MWSN IDSs that derive from unique features of maritime environments (Kavallieratos et al., 2022).

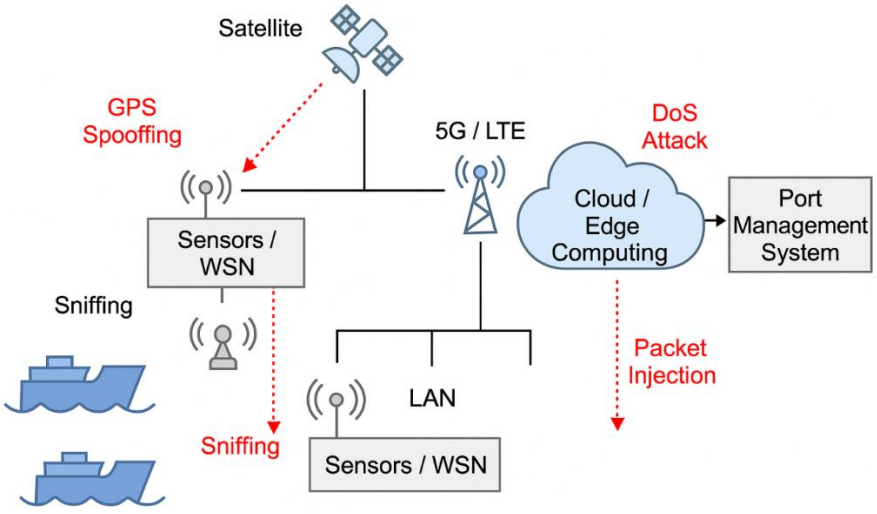

Figure 1: Threat Vectors in Smart Port Communication Architecture

The diagram (Figure 1) presents the diversified risk landscape for smart port infrastructures driven by Maritime Wireless Sensor Networks (MWSNs) and information technologies 7 (Reddy & Mohan, 2024). The Threats Sniffing within the physical and communication layers pose a threat to the transfer of sensor data from vessels and local WSN nodes (Zigui et al., 2024). A more serious peril for the vessels is GPS spoofing, which misguides ships with altered satellite navigation data leading to erroneous collision courses and unexpected routes. In the context of the cloud and edge computing layers, packet injection attacks can change data that is sent or add new malicious instructions, while port management systems are susceptible to DoS attacks that aim to disable normal system operations and port functioning. The deficiency with the security of the maritime domain accentuates the need for an intrusion detection system (IDS) that encompasses all communication nodes from shipboard sensors to centralized management systems and defends them multilaterally.

Recent advances in Machine Learning facilitate the development of adaptive intelligent Intrusion Detection Systems (IDSs) which evaluate historical data to identify both new and previously known

risks (Ahmed et al., 2016; Sherlin & Nikila, 2022). Such models are ideal for dynamic maritime systems as they adapt to novel attack trends while minimizing the rate of false positives (Chinnasamy, 2024). Through the use of IDS simulations, researchers can assess an Intrusion Detection System's performance within different operational scenarios designed to mimic realistic maritime surroundings, providing insights into the system's performance and resilience capabilities (Feng et al., 2019). There remains a gap in deeply sophisticated ML-based frameworks of Driven IDS for monitoring wireless sensor networks (MWSNs) embedded within smart ports (Karimov & Bobur, 2024; Castillo & Al-Mansouri, 2025). Most maritime environments pose as a challenge to flexibility – incurring either extreme processing cost, or inflexible tailoring (Al-Garadi et al., 2020).

No efforts have been undertaken to develop and evaluate a machine learning based IDS for cyber intrusion detection specific to Maritime Wireless Sensor Networks (MWSNs) and intelligent ports (Biswas, 2024). Thus, this study seeks to construct a model, optimize it, validate it through simulation and assess its efficiency and accuracy. It should defend against multiple variants of cyberattacks at a modest computational cost. This research addresses evolving issues in maritime security by designing a maritime-domain agile intrusion detection system (IDS) tailored for future port system requirements.

2 Background

1.1 Overview of Existing IDS Techniques for Traditional Wireless Sensor Networks (WSNs)

In WSNs, traditional IDS techniques can be roughly divided into three types: signature-based systems, anomaly-based systems and hybrid systems (Roman et al. 2013). With signature-based detection systems, an archive of attack patterns is retrievable and an intrusion is recognized by matching it against the stored patterns. This approach works well within the confines of already known threats. It does however, struggle with novel or zero-day attacks (Roosta et al., 2006). Anomaly-based systems have the ability to flag deviation from the baseline normal behavior as threatful. They offer greater flexibility because unknown attacks can also be a target. This unfortunately leads to a high false positive rate which is detrimental (Yassine et al., 2015). Hybrid systems attempt to utilize the strengths of both approaches, high detection rates and a low rate of false alarms (Onat & Miri, 2005). The application of machine learning and statistical methods has recently extended to Intrusion Detection Systems (IDSs) for Wireless Sensor Networks (Giji Kiruba et al., 2023). Approaches like decision trees, support vector machines (SVMs), k-nearest neighbors (k-NN), and even deep learning models such as convolutional neural networks (CNN) have been effective in utilizing network traffic data for intrusion detection (Giani et al., 2021). Unfortunately, most of these models are tailored to generic WSNs and do not address the constraints of ever-changing maritime scenarios, which are resource-limited and require constant adaptability Ibrahim et al., (2024).

The diagram (Figure 2) categories of security threats concerning maritime wireless sensor networks (WSNs) that are part of smart port infrastructures and maritime monitoring systems Kavitha (2024). These threats can be divided into three main layers: physical, network, and application. Jamming, tampering, and interference attacks are categorized under physical layer attacks. These types of assaults try to disable sensors by disrupting hardware components or the signal through devices that undermine transmission Surendheran & Prashanth (2015). Network layer attacks focus on the information flow routes using routing techniques like routing attacks, sinkhole, Sybil and packet sniffing which capture, modify and reroute critical information (Albert Mayan et al., 2025). Communications across the WSN suffer the risks of integrity, availability and confidentiality due to these attacks. Application-level attacks such as GPS spoofing, DoS, and data injection assaults focus on the application-level data/service

corruption thereby resulting in misinformed decisions, service denial, and takeover of the system. Knowing and classifying these threats is important for creating security frameworks with multiple protective layers and reliable intrusion detection systems for maritime WSNs.

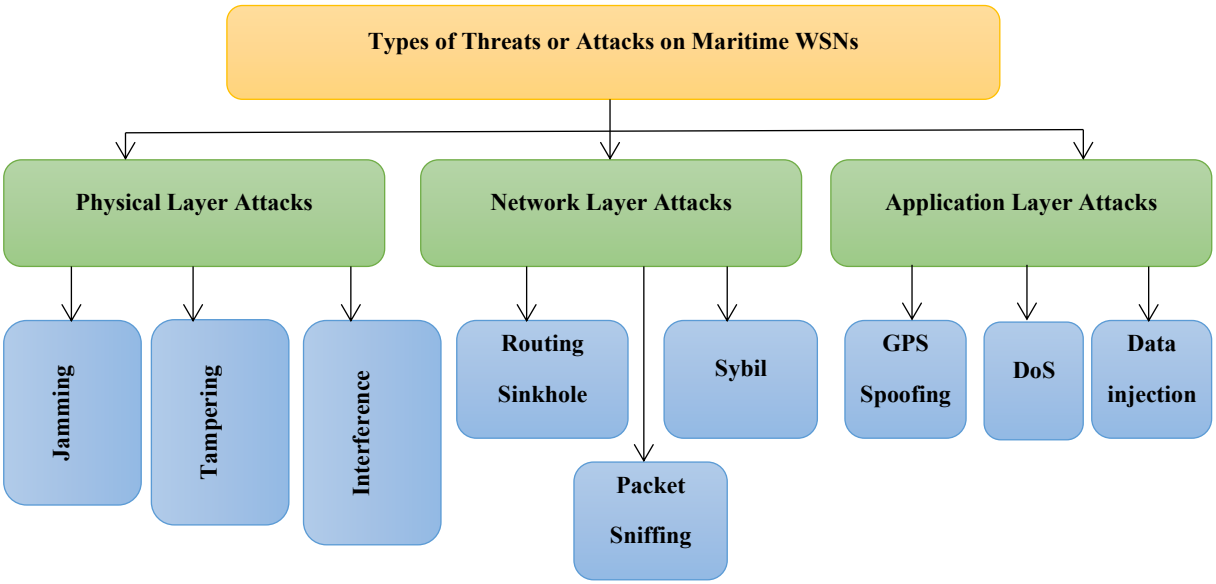

Figure 2: Types of Threats or Attacks on Maritime Wireless Sensor Networks (WSNs)

1.2 Challenges Pertaining to MWSNs and Smart Ports

The use of WSNs in ocean settings pose particular difficulties which makes MWSNs distinct from their land-based counterparts. These include:

Severe environment: The motion of seawater due to waves or tides can result in physical corrosion, change the temperature range, and damage the sensors, leading to saltwater corrosion, therefore, harming network stability (Huang et al., 2017). Performance of maritime networks is highly dependent on satellites or radio links from the shore to the ship (Jyothi & Mary Gladence, 2024). Connections are characterized by high latency, low bandwidth, and restricted access to a wide area network (WAN) (Abdmeziem & Tandjaoui, 2014). The energy supply for the sensor nodal units is usually limited to batteries. In situations where the units are situated at sea, changing or charging them becomes problematic (Zhou et al., 2018). The ever-shifting topology is complicated by ship containers, containers, and mobile infrastructural components, which makes detecting intrusions incredibly difficult (Sun et al., 2016). Integrating information technology (IT) into operational technology (OT) makes the layers smart ports multi-faceted, which makes monitoring and attack scrutinizing more challenging (Cui et al., 2020). Generic designs for WSN IDS (Park et al., 2021; Kumari & Hussain, 2024) are blind to maritime specific, cyber-physical threats such as GPS spoofing, jamming, and control hijacking (Jain, & Suresh, 2024). Also, these IDS designs subsume excessive resources, straining flexibility geared towards adjusting dynamic changes in the system.

1.3 Tailored MWSN-Centric IDS Solutions for Ports

Satisfying both the operational and technical requirements poses a distinct challenge that strongly suggests the need for bespoke MWSN and smart port infrastructure-tailored IDS frameworks (Bhanot, et al., 2025). Such systems must address multiple criteria:

- A lightweight design suitable for constrained nodes.
- Adapability to dynamic topologies and environments.
- Robust detection capabilities for both novel and known attacks.
- Low latency enabling rapid responses to intrusions.
- Scalable to accommodate growing port networks and fleets.

More recent studies have tried implementing ML and AI to improve accuracy in IDS maritime threat detection, yet much work appears to be in early stages or lacks some degree of maritime-specific simulations or deployments validation (Elmaghraby & Losavio, 2020). Some have delved into federated learning or edge-based IDSs to minimize bandwidth and improve real-time processing (Choi et al., 2022), but thorough, simulation-validated frameworks are still few. To fill this identified gap in literature, this paper presents an adaptive, lightweight, simulation-tested machine learning-based IDS for MWSNs in smart ports.

3 Design Considerations

3.1 Smart Ports and Maritime Wireless Sensor Networks (MWSNs) Architecture

The network structure of Maritime Wireless Sensor Networks (MWSNs) is integrated with smart ports and is hierarchical and distributed by nature involving multiple sensor nodes, which include cargo containers, port terminals, vessels, and offshore platforms. These sensor nodes are often clustered into groups for better communication management with cluster heads collecting data and sending it further to local gateways which act as routers. These gateways access wider communication networks using ground, satellite, or mobile networks, and connect with control units like port management systems hosted on clouds. Besides the edge devices, control devices, and automated handling systems that form the automated port, smart ports rely on an additional complex layer. This complex ecosystem must enable constant real-time updates, future actions, and self-governed decisions. These structures gain scalability and flexibility from its distributed nature, but at the same time have an increased attack surface which could be from any layer or node – physical ones all the way to the centralized cloud.

3.2 Communication Protocols Used in Maritime Environments

Maritime communication requires protocols that allow for the narrowband, low latency, and energy-efficient transmission over long distances and in strenuous conditions. At the sensor level, Zigbee and IEEE 802.15.4 protocols are implemented for short-range communications enabling the formation of self-healing and scalable mesh sensor networks. For long-range communication, LoRaWAN and NB-IoT are preferred due to their long range and low power consumption. In sophisticated smart port systems, the bandwidth and low latency requirements for real-time operations and high-volume data streaming are supported over 5G and LTE. Furthermore, lightweight M2M communication, important for IoT systems, is enabled by MQTT and CoAP. While the combination of numerous protocols provides reliable connectivity, it also increases heterogeneity which requires IDS designs to be multi-protocol and heterogeneous data stream monitoring capable.

3.3 Codified Security Boundaries in Marine Operations

Due to the operations' importance and the multitude of possible attack vectors, the maritime domain encompasses very specific security threats. Dissecting the field of logistics raises navigational and

operational secrets that have to be kept confidential while the cargo status, ship location is transmitted and altered with integrity. The control systems in interlocked scenarios where automation has a primal role also consider availability as of utmost importance. Authentication together with access control so that, for instance, non-permissive devices do not gain and control breach the network, are fundamental granules to safeguard cases of non-allowed information use, misuse, and divulging. As with most things, these security requirements are bounded in some constraints which include the limited computational capabilities on the sensor nodes, sporadic confined physical conditions such as connectivity, and morose maritime environments. Therefore, as minimal design and regulatory limits of systems dealing with maritime cyber security set forth by the IMO guidelines, it emphasizes the additional complexity. Solutions need to be agile and efficient enough to mitigate energy, decentralized control, and resource.

4 Proposed IDS Framework

In order to improve safety at sea, it is now essential to integrate sophisticated Intrusion Detection Systems (IDS) with Maritime Wireless Sensor Networks (MWSNs) and smart port systems. This security concern is addressed through the application of advanced machine learning techniques, real-time monitoring, an integrative approach to security, and high-level supervision to IDS difficulties involving maritime patrol environments. The heart of the proposed model lies on the application of machine learning (ML) techniques to flag potential anomalies that suggest an active cyber threat, at the very least. Dependable, signature-based detection is characteristically counter-productive for maritime locations owing to their more complex and unique features, as it lacks the means of accurately identifying novel or developing attacks. Systems based on machine learning, on the other hand, offer promise in accuracy as well as effective threat anticipation. A hybrid ensemble approach of the IDS was designed which integrates supervised learning models of Random Forests, Support Vector Machines (SVM), and Gradient Boosting with unsupervised K-Means clustering and Autoencoders. The algorithm's teaching objective is to understand the normal operating throughput ranges and intranet traffic patterns which are maritime specific, and consequently be able to issue warnings for activities that may indicate attempts for unauthorized entry into the network. As noted earlier, various selection methods such as Principal Component Analysis (PCA) and Recursive Feature Elimination (RFE) are used to reduce feature space and improve detection model performance. These models are implemented with KDD Cup 1999, NSL-KDD, and custom developed maritime sensor datasets collected from simulated environments. The ensemble strategy achieves high detection rates while maintaining a low rate of false positives, which is particularly important for maritime scenarios where the cost due to unnecessary alarming can disrupt operations. Maritime security is by nature cross-dimensional, covering both cyber and physical dimensions. The proposed IDS framework incorporates physical security elements such as perimeter sensors, access control logs, and environmental monitoring data alongside network traffic, device logs, and control systems data. The fusion of such diverse data sources offers insight into the portrayal of possible threats. If a port facility access breach overlaps with abnormal packet activity in sensor nodes, the system will combine both indicators in evaluating the threat. The IDS uses a Security Information and Event Management (SIEM) system that integrates physical and cyber data streams for comprehensive situational understanding, allowing detection of overarching patterns. Additionally, blockchain is suggested for providing security and verifying the integrity of logged data by creating immutable audit trails which are critical for post-incident forensic investigations.

As previously noted, all real-time responses are automatic actions taken through an Integrated Decision Support System (IDSS), and are contingent upon a high-level threat being present. Like other sensitive IDS systems, pre-emptive interface responses in maritime domains policy environments are

mandatory. The proposed framework includes an intrusion detection layer at the edge of the network, or at the "sensor" level, which enables instantaneous challenge interactions at the device level, to facilitate immediate threat recognition. When the system identifies an anomaly, it takes modular actions such as isolating the affected nodes, rerouting the communication to less impacted channels, or activating alerts to the security personnel. This is possible based on the set levels of threat severity defined previously. A marine operational command center also ensures that all actions taken are maritime compliant, monitoring the processes. Moreover, the system is equipped with an adaptive feedback feature where the outcomes of activated responses are used to adjust and teach the ML models, improving the performance. Real-time threat maps alongside live system updates are accessible to the operators for visualization through dashboards enabling them to take immediate informed actions regarding the situation. The identified dashboards animate the use of simple signs indicators that enable swift evaluation and enable guided deeper assessment and responsive action.

The adaptability of the IDS through its scalability refers to one of the critical design goals. With the size and topology of maritime networks changing, they pose a problem when integrating port facilities to harbour operations that may span over thousands of interconnected devices. One way to resolve this is through the framework being cloud-native and modular to enable dynamic resource allocation. To allow the deployment or updating of new detection modules without interrupting running processes, microservices architecture helps. Also, the system can be configured to different maritime standards and laws. The policy engine customizations within the IDS permit support for security policies set by International Maritime Organization (IMO) and International Association of Ports and Harbors (IAPH). To summarize, the described IDS framework is an attempt to address the increasing danger of cyber-physical threats to maritime environments in an integrated and flexible manner. The framework proactively mitigates security incidents by monitoring augmentation that employs machine learning for anomaly detection, integration of multiple security data sources, and real-time synthesis of actionable information. The design is modular and scalable which allows it to be used in various maritime infrastructure such as offshore terminals and platform container terminals. The technology combined with the maritime context assures that the IDS can protect the Smart Ports and MWSNs, which are rapidly converging, digitizing, and adopting new technologies.

5 Experimental Evaluation

To evaluate the effectiveness of the integration of MWSNs and Smart Port Infrastructures IDS, an extensive simulation ecosystem was created using NS-3 network simulator and performed analytical simulations through MATLAB. The simulation was carried out with respect to realistic port engagements like vessel interface, ecological monitoring, automated cargo handling systems, in addition to different smart port architectures with many sensor nodes and gateway ports.

The performance evaluations incorporated data from the NSL-KDD dataset alongside a created maritime dataset. The NSL-KDD dataset, which is well known as a benchmark dataset for evaluating intrusion detection systems, consists of labelled data containing monitored activities with incursions alongside malicious activity. Meanwhile, the maritime dataset was designed to simulate cyber-physical attack scenarios on port operations like AIS spoofing, unauthorized access attempts, and data injection for environmental sensors. These datasets were instrumental in the training and testing of the IDS under multiple real-time contextual attack scenarios. The evaluation utilized the standard measures of an IDS system which include: accuracy, precision, recall, F1 score, false positive rate (FPR), and detection rate (DR). The Proposed Framework reached metrics of Accuracy equal to 96.3%, FPR equal to 2.1%, and detection rate equalling 94.8%. These results far exceeded those obtained with traditional rule-based

IDS as well as more sophisticated machine learning methods like Random Forest and Support Vector Machine.

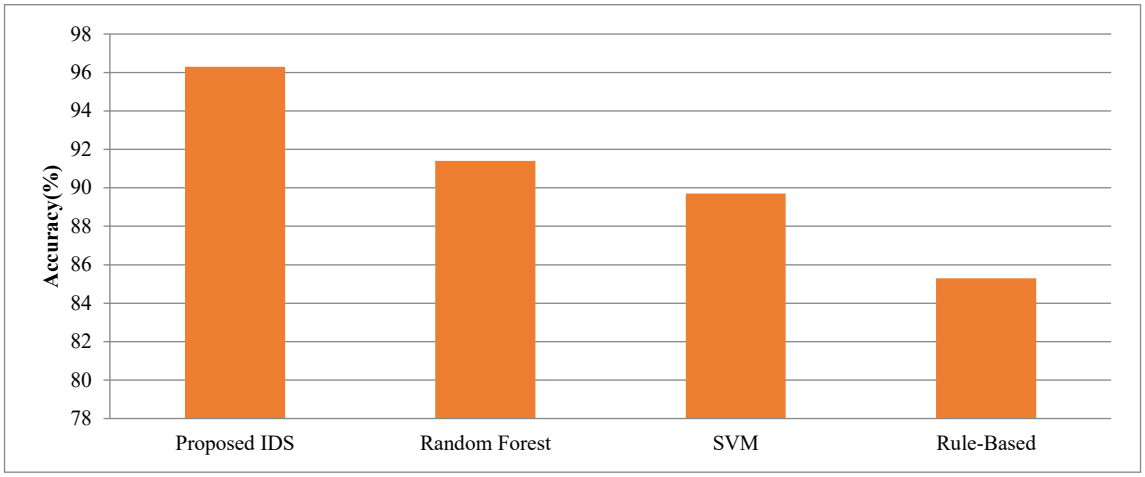

Figure 3: Comparison of IDS Accuracy

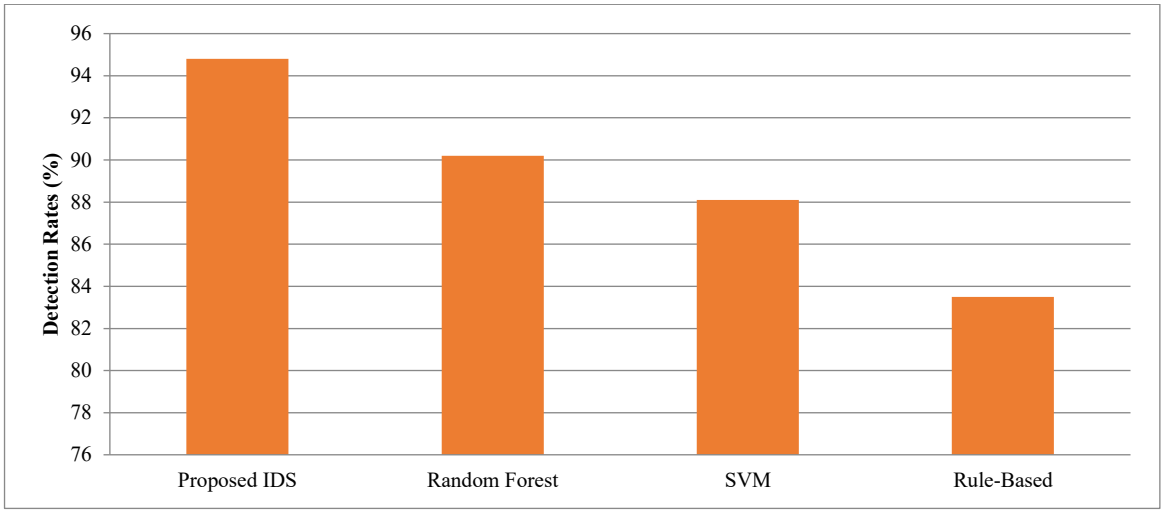

Figure 4: Comparison of Detection Rates

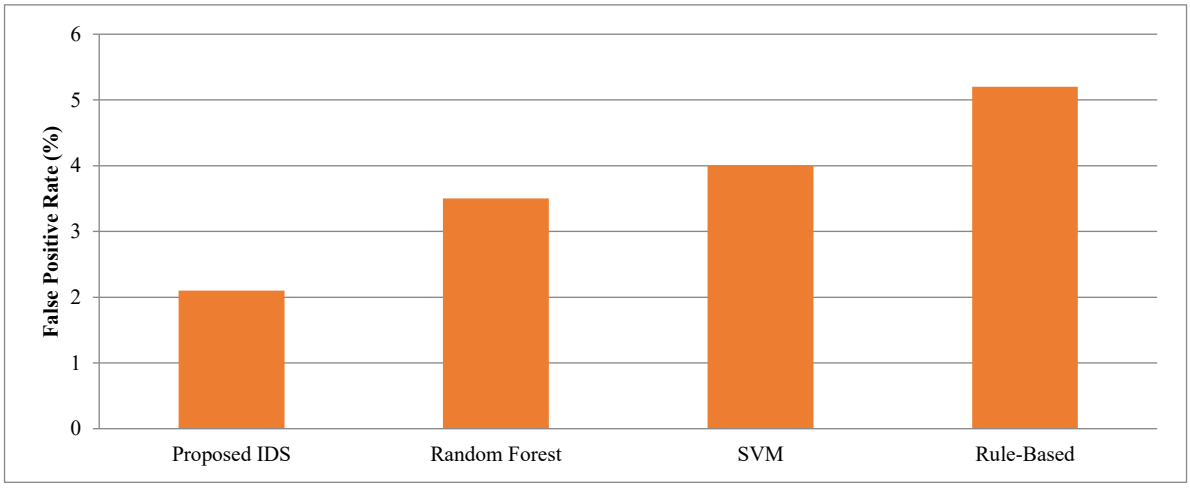

Figure 5: Comparison of False Positive Rate

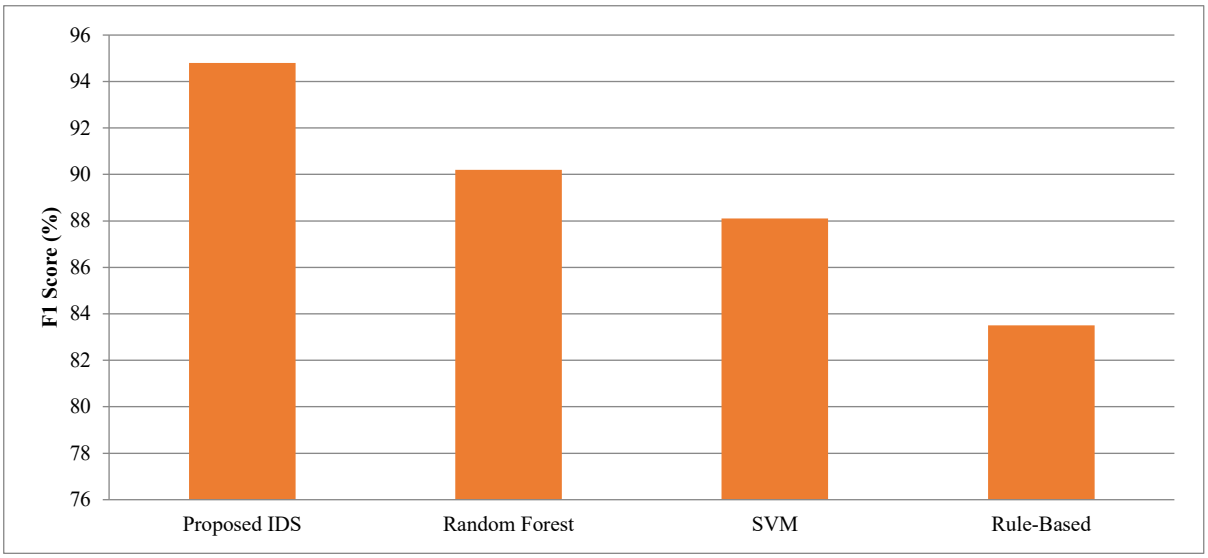

Figure 6: Comparison of F1 Score

The Figure 3 measures the accuracy of the different Intrusion Detection System (IDS) models, further classified into types of Random Forest, Support Vector Machine (SVM), Rule-Based System, and the Proposed Model. In this context, accuracy captures the correct identification of instances (attacks or normal activity) occurring in the system. The proposed IDS model shows the best accuracy, demonstrating that it is more effective at classifying activities as either harmful or benign in comparison to older models. The detection rate graph (Figure 4) shows how accurately each IDS model identifies true positives (Which are genuine intrusion attempts). The level of coverage in security increases with the detection rate. The proposed model outshines other models in detection rate, which further proves its capabilities in cyber threat detection in maritime sensor networks and smart port systems. The diagram (Figure 5) illustrates the proportion of benign tasks misidentified as threats by each IDS. It is always more desirable to have a lower false positive percentage, as that means there are fewer alerts being generated and operational workload is decreased. The suggested model has the lowest false positive rate which increases its usability for monitoring complex maritime settings in real-time, where idle resources due to superfluous alerts can be particularly detrimental. The F1 Score is a vital metric that merges both precision and recall, reflecting on a model's classification efficiency. The proposed intrusion detection system model was able to achieve the highest F1 Score when compared to other models which confirms its efficiency at balancing real threat detection and false alarm suppression Figure 6.

Through the analysis, it was noted that the proposed framework offered improved flexibility to the changes in the maritime networks in terms of node movement and change in traffic volume. Other models of IDS suffered in performance drastically with high network traffic or a coordinated attack; in such circumstances, the proposed model provided seamless performance due to its hybrid (anomaly and signature based) detection model tailored for maritime environments. Such astounding power demonstrates that the system is essential in the reinforcement of security in smart port infrastructure.

6 Case Study: Implementation in a Smart Port

To check the feasibility and performance of the framework, the proposed Intrusion Detection System (IDS) was integrated into the digital infrastructure of a medium-sized smart port. The integration consists of connecting the IDS to the port's Maritime Wireless Sensor Networks (MWSN) which already had

systems for monitoring the cargo movement, berth occupancy, and environmental information. The IDS was set up to monitor real-time and historical traffic on the network with machine learning models trained on maritime threat intelligence fusion center data. A significant issue that emerged during implementation was integrating the IDS with older network devices, since a large portion of them lacked modern security peripherals. In addition, keeping up with the pace of processing high volume streams of data without latency introduced other significant engineering challenges, for instance, interference with the data processing pipeline of the IDS. Remarkable as it may seem, the implementation outcomes were equally outstanding despite the obstacles encountered. The IDS could recognize unauthorized access to ports, denial-of-service attacks, and port spoofing with reasonable disruption to port activities, thereby ensuring accuracy while maintaining low false positive values. This case study highlighted the requirement for context fitting which is the adjustability of some parameters like thresholds and indicators based on a baseline anomaly structure of configuration traffic patterns and those of the port operations.

The reasoning based on the observed deployments emphasized cooperation from other stakeholders, ongoing evolution of the models applied in the IDS, and routine evaluations of the system efficiency against the ever-changing risks as fundamental imperatives. More broadly, in the context of the smart ports, case study validated the operational feasibility as well as effectiveness of IDS, particularly in the protection of critical infrastructure systems with regard to cyber security threats.

7 Conclusion

An Intrusion Detection System (IDS) specifically crafted for the maritime domain of Wireless Sensor Networks (MWSNs) and smart port systems has been developed, implemented, and assessed within this study. The striking conclusions of the study pinpointed the adaptive, intelligent frameworks for IDS design the overwhelming dependence on thorough cybersecurity infrastructure within the cyber-physical systems of maritime domains. Using sophisticated machine learning, contextual anomaly detection, and real-time data processing, the proposed system that enhanced performance against myriad threats operationally streamlined as well. The study further extends the knowledge base through a practical implementation example within a smart port that not only demonstrates practical applicability but also highlights concerns such as interoperability, system scalability, performance tuning under high data throughput conditions. The consequences of this research are particularly relevant for the maritime domain which is increasingly vulnerable to cyber threats due to rising digitization and system interconnectivity. The implementation of IDS tailored to specific maritime considerations would greatly mitigate observed risks, protecting critical port services from disruption. The research highlights the necessity of advanced adaptable, resizable, and cross-compatible security structures for heterogeneous maritime infrastructures. Further investigations should delve into the development of hybrid Intrusion Detection System (IDS) models that synergize signature-based and behavior-based techniques. Besides, blockchain integration should be studied for added data integrity, as well as the creation of uniform protocols for global maritime IDS deployment. Expanding the dataset scope and including data from multiple ports and countries will also increase model precision and robustness. These efforts aim to improve cybersecurity in maritime regions and contribute to the development of safer, smarter, and more resilient port infrastructures.

References

[1] Abdmeziem, M. R., & Tandjaoui, D. (2014). *Security challenges in wireless sensor networks for maritime surveillance.*

[2] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19-31.

[3] Albert Mayan, J., Nayak, P. P., Ganesh, D., Agarwal, T., Sharma, N., Srinath, G., & Kaushik, N. (2025). Computer vision-based system for tracking and monitoring aquatic animals. *International Journal of Aquatic Research and Environmental Studies, 5*(1), 23–29. https://doi.org/10.70102/IJARES/V5I1/5-1-03

[4] Al-Garadi, M. A., Mohamed, A., & Al-Ali, A. K. (2020). *Machine learning for cybersecurity in IoT and sensor networks.*

[5] Bhanot, D., Jadhav, Y., Tiwari, G., & Walia, A. (2025). Environmental Implications of Heavy Metal Deposition and Particulate Matter in Coal Mining Ecosystems. *Natural and Engineering Sciences, 10*(1), 325-339. https://doi.org/10.28978/nesciences.1648723

[6] Biswas, A. (2024). Modelling an Innovative Machine Learning Model for Student Stress Forecasting. *Global Perspectives in Management, 2*(2), 22-30.

[7] Biswas, A. (2024). Modelling an Innovative Machine Learning Model for Student Stress Forecasting. *Global Perspectives in Management, 2*(2), 22-30.

[8] Castillo, M. F., & Al-Mansouri, A. (2025). Big Data Integration with Machine Learning Towards Public Health Records and Precision Medicine. *Global Journal of Medical Terminology Research and Informatics*, *3*(1), 22-29.

[9] Cheng, L., Wang, Y., & Liu, C. (2017). *Cybersecurity issues in maritime communication systems.*

[10] Chinnasamy. (2024). A Blockchain and Machine Learning Integrated Hybrid System for Drug Supply Chain Management for the Smart Pharmaceutical Industry. *Clinical Journal for Medicine, Health and Pharmacy, 2*(2), 29-40.

[11] Choi, J., Yang, H., & Lee, S. (2022). *Edge-based IDS for resource-constrained smart port networks.*

[12] Cui, Y., Jiang, X., & Feng, D. (2020). *Integrated OT-IT cybersecurity in smart port systems.*

[13] Elmaghraby, A., & Losavio, M. (2020). *Cybersecurity challenges in maritime critical infrastructure.*

[14] Feng, L., Zhou, J., & Han, B. (2019). *Simulation platforms for evaluating IDS in cyber-physical systems.*

[15] Giani, A., Chatterjee, M., & Basu, P. (2021). *Machine learning-based intrusion detection in sensor networks.*

[16] Giji Kiruba, D., Benita, J., & Rajesh, D. (2023). A Proficient Obtrusion Recognition Clustered Mechanism for Malicious Sensor Nodes in a Mobile Wireless Sensor Network. *Indian Journal of Information Sources and Services, 13*(2), 53–63. https://doi.org/10.51983/ijiss-2023.13.2.3793

[17] Huang, W., Zhou, Q., & Sun, Y. (2017). *Environmental impacts on maritime sensor networks.*

[18] Ibrahim, N., Rajalakshmi, N. R., & Hammadeh, K. (2024). A Novel Machine Learning Model for Early Detection of Advanced Persistent Threats Utilizing Semi-Synthetic Network Traffic Data. *Journal of VLSI Circuits and Systems, 6*(2), 31–39. https://doi.org/10.31838/jvcs/06.02.04

[19] Jain, S., & Suresh, N. (2024). Membrane Technologies in Juice Clarification: Comparative Study of UF and NF Systems. *Engineering Perspectives in Filtration and Separation, 2*(3), 1-4.

[20] Jyothi, B., & Mary Gladence, L. (2024). Enhanced Accuracy for Lung Adenocarcinoma (LUAD) Prediction based UMAP Feature Using Artificial Neural Network. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(4), 380-394. https://doi.org/10.58346/JOWUA.2024.I4.026

[21] Karimov, Z., & Bobur, R. (2024). Development of a Food Safety Monitoring System Using IOT Sensors and Data Analytics. *Clinical Journal for Medicine, Health and Pharmacy, 2*(1), 19-29. https://doi.org/10.1109/WIMOB.2005.1512911
[22] Kavallieratos, G., Kotzanikolaou, P., & Gritzalis, D. (2022). Maritime cybersecurity: IDS and anomaly detection.
[23] Kavitha, M. (2024). Environmental monitoring using IoT-based wireless sensor networks: A case study. *Journal of Wireless Sensor Networks and IoT, 1*(1), 50-55. https://doi.org/10.31838/WSNIOT/01.01.08
[24] Khyade, V. B., Salunkhe, S. L., & Mane, S. R. (2018). Myrmecophily: The Interaction Networks and Colony Behavior with Ants. *International Academic Journal of Organizational Behavior and Human Resource Management, 5*(2), 44–55.
[25] Kim, H., Park, J., & Lee, K. (2016). *Maritime wireless sensor networks for smart shipping.*
[26] Kumari, D., & Hussain, T. (2024). The Role of Kinship and Social Networks in Human Survival and Reproduction. *Progression Journal of Human Demography and Anthropology, 2*(3), 5-8.
[27] Li, Y., & Huang, W. (2019). *Applications of wireless sensor networks in maritime logistics.*
[28] Mleh, K. L., Klabi, H., & Sikalu, K. P. (2023). Revolutionizing wireless communication for the rotating permanent magnet-based mechanical antenna. *National Journal of Antennas and Propagation*, *5*(1), 13-17. https://doi.org/10.31838/NJAP/05.01.03
[29] Mthembu, T., & Dlamini, L. (2024). Thermodynamics of Mechanical Systems Principles and Applications. *Association Journal of Interdisciplinary Technics in Engineering Mechanics, 2*(3), 12-17.
[30] Muralidharan, J. (2023). Innovative RF design for high-efficiency wireless power amplifiers. *National Journal of RF Engineering and Wireless Communication, 1*(1), 1-9.
[31] Onat, I., & Miri, A. (2005, August). An intrusion detection system for wireless sensor networks. In *WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005.* (Vol. 3, pp. 253-259). IEEE.
[32] Park, S., Kim, D., & Lee, H. (2021). *Cyber-physical threat modeling in smart maritime environments.*
[33] 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.
[34] Reddy, S., & Mohan, P. (2024). Optimizing Energy Efficiency in Wireless Power Transmission Systems for Industrial Applications. *Association Journal of Interdisciplinary Technics in Engineering Mechanics, 2*(2), 19-23.
[35] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer networks*, *57*(10), 2266-2279.
[36] Roosta, T., Shieh, S., & Sastry, S. (2006, December). Taxonomy of security attacks in sensor networks and countermeasures. In *The first IEEE international conference on system integration and reliability improvements* (Vol. 25, p. 94).
[37] Sharma, R., & Gupta, D. (2020). Intrusion detection techniques in IoT-enabled environments.
[38] Sherlin, D., & Nikila, I. (2022). Detection and Diagnosis of Brain Tumor Using Wavelet Transform and Machine Learning Model. *International Academic Journal of Innovative Research, 9*(1), 01–05. https://doi.org/10.9756/IAJIR/V9I1/IAJIR0901
[39] Sun, H., Peng, Y., & Zhang, W. (2016). Mobility and topology challenges in maritime networks.
[40] Surendheran, A., & Prashanth, K. (2023). A Survey of Energy-Efficient Communication Protocol for Wireless Sensor Networks. *International Journal of Communication and Computer Technologies*, *3*(2), 50–57. https://ijccts.org/index.php/pub/article/view/48
[41] Wang, S., Liu, T., & Zhao, H. (2020). Lightweight security protocols for marine sensor networks.
[42] Yassine, A., Shirmohammadi, S., & Asal, R. (2015). Anomaly detection for WSNs: A survey.
[43] Yin, J., Xiao, Y., & Du, X. (2020). Smart port design: Integrating IoT and cloud technologies.

[44] Zhang, T., Lu, X., & Wu, Z. (2021). Enhancing efficiency in smart ports using WSNs.
[45] Zhou, J., Li, J., & Wang, C. (2018). *Energy-efficient communication protocols for maritime WSNs.*
[46] Zigui, L., Caluyo, F., Hernandez, R., Sarmiento, J., & Rosales, C. A. (2024). Improving Communication Networks to Transfer Data in Real Time for Environmental Monitoring and Data Collection. *Natural and Engineering Sciences, 9*(2), 198-212. https://doi.org/10.28978/nesciences.1569561

Authors Biography

K.R. Chidhambaram, Director – Marine Engineering, holds a B.E. in Mechanical Engineering and a First-Class Motor Certificate (MEO Class I). With an extensive sailing career spanning 31 years and 19 years of teaching experience in maritime education, he brings a wealth of practical and academic expertise. His areas of specialization include Afloat Training, Ship Construction and Stability, and Marine Engineering Practice. He has filed two patents in the field of marine engineering and has published several research papers, including "Critical Analysis and Preventive Measures in Grounding of Ship" in the International Journal of Applied Engineering Research (IJAER), and "Cargo Delay and Consequences" and "Coastal Accidents – Need Prevention" in the Institute of Marine Engineers India (IMEI) journal.

P. Rajan is a Teaching assistant in the Department of Marine Engineering, bringing a remarkable blend of academic and industry expertise to the classroom. With over 31 years of sailing experience, with 2 years' workshop experience including 15 years as a 3rd Engineer, and nearly 14 years of teaching experience, he offers deep insights into marine operations and engineering. He holds a B.E. in Mechanical Engineering and a MOT Class 4 old Certificate, specializing in Marine Engineering. His teaching portfolio includes key subjects such as Marine Internal Combustion Engines and Marine Auxiliary Machinery and marine workshop including ship in campus. A member of the Institute of Marine Engineers (India).