International Journal of Computational Intelligence Systems (2024) 17:147
https://doi.org/10.1007/s44196-024-00539-z

RESEARCH ARTICLE

Application of Artificial Intelligence Technology in Vulnerability Analysis of Intelligent Ship Network

Dan Lan[1,2] · Peilong Xu[2] · Jia Nong[1] · Junkang Song[3] · Jie Zhao[4]

Received: 11 March 2024 / Accepted: 23 May 2024

Abstract

The improvement in transportation efficiency, security, safety, and environmental effects may be possible due to the impending advent of autonomous ships. Automatic situational awareness, risk detection, and intelligent decision-making are the key features of the intelligent ship network, differentiating it from conventional ships. There is an immediate need to implement a system for marine information management and network security due to the growing importance of this field, which poses a risk to national and societal stability due to factors, such as the diversity and complexity of marine information types, the challenges associated with data collection, and other similar factors. By recognizing different vulnerabilities and through research cases of the ship systems and Artificial Intelligence (AI) technologies, this paper presents Adaptive Fuzzy Logic-assisted Vulnerability Analysis of Intelligent Ship Networks (AFL-VA-ISN) in various cyberattack scenarios for autonomous ship intrusion detection and information management. Fuzzy logic has been combined with AI, providing a framework for handling uncertainty and imprecision in intelligent ship networks and effective decision-making. This work presents a method for detecting anomalies in risk data based on the collaborative control structure of the Ship Information System. Maintaining the network security of intelligent ships is the primary focus of this research, which mainly employed multi-sensor nodes to evaluate data containing information about malicious attacks and placed self-execution protection organize generating nodes into place to intercept and protect against attacks. The experimental outcomes demonstrate that the suggested AFL-VA-ISN model increases the data transmission rate by 99.2%, attack detection rate by 98.5%, risk assessment rate by 97.5%, and access control rate of 96.3%, and reduces the network latency rate of 11.4% compared to other existing models.

Keywords Artificial intelligence · Vulnerability analysis · Intelligent ship network · Fuzzy logic · Data security · Information management system · Navigational operations

Abbreviations

AI	Artificial inteligence
ISN	Intelligent ship network
ICT	Information and communication technology
CPS	Cyber-physical system
AIS	Automatic identification system
ANS	Autonomous navigation system
GPS	Global positioning system
SCC	Shore control centre
GMDSS	Global maritime distress and safety system
SART	Search and rescue transponders
EPIRB	Emergency position indication radio beacons
SA	Situational awareness
SOC	Security operations centers

✉ Dan Lan
landan014@163.com

Peilong Xu
xpl@qdu.edu.cn

Jia Nong
Jerry30902442@Outlook.com

Junkang Song
songjunkang@gxnun.edu.cn

Jie Zhao
zhaojie52985@163.com

[1] College of Automotive and Information Engineering, Guangxi Eco-Engineering Vocational and Technical College, Liuzhou 545004, Guangxi, China

[2] Computer Engineering Department, Pukyong National University, Busan 48513, Korea

[3] College of Mathematics, Physics and Electronic Information Engineering, Guangxi Normal University for Nationalities, Chongzuo 532200, Guangxi, China

[4] College of Information Engineering, Liuzhou City Vocational College, Liuzhou 545036, Guangxi, China

Published online: 13 June 2024

GNSS	Global navigation satellite systems
RADAR	Radio detection and ranging
CRC	Cyclic redundancy check
FCS	Frame check sequence
LiDAR	Light detection and ranging
IRA	Intrusion ring alert

1 Introduction

Maritime transportation is essential for expanding global economies and maintaining commerce between transoceanic nations and the seas [1]. With the development of Information and Communication Technology (ICT), it has become common for ships to be linked to the Internet, and the communication between ships and shores has increased rapidly [2]. Yet, cyber-attacks like malware infection and illegal access to internal networks have become more common due to ships' persistent Internet connectivity [3]. Reducing the risk of cyber-attacks to zero is difficult, so it is important to consider countermeasures, assuming everyone is vulnerable [4]. The primary components of an intrusion detection system (IDS) are security and information exchange devices that check the accuracy of the instructions transmitted from the decision-making system to the designated response system. [5].

Autonomous navigation systems leverage artificial intelligence (AI) technology to process vast amounts of high-dimensional data like human cognition, learning, and knowledge-based reasoning [6]. There is an increasing demand for reliable navigational data to support the deployment of AI-controlled, Internet-connected, integrated ships that operate without human operators [7]. Numerous research studies on ship systems and vulnerabilities in AI technology, such as Fuzzy Logic and deep learning methods, are being conducted to solve cybersecurity issues [8]. Measuring uncertain occurrences generated by subjective and objective elements is possible using fuzzy set theory and probabilistic risk assessment technologies [9]. The ship control system's information security risk assessment demonstrates that the process may increase the reliability and stability of evaluation findings by successfully reducing uncertainty caused by subjective and objective elements [10].

The paper's novelty is to design an Adaptive Fuzzy Logic-assisted Vulnerability Analysis of Intelligent Ship Network (AFL-VA-ISN) model for intrusion detection in autonomous ships and information management. Combining AI with fuzzy logic provides a framework for intelligent ship networks to effectively handle uncertainty and imprecision in decision-making. Using the Ship Information System's collaborative control framework, this study demonstrates a way to spot irregularities in risk data. This research mainly used multi-sensor nodes to assess data containing data on malicious attacks and placed self-execution security organize-producing nodes to intercept and protect against attacks; the primary focus was on maintaining the network security of intelligent ships.

The main contribution of the paper is

- Designing the Adaptive Fuzzy Logic-assisted Vulnerability Analysis of Intelligent Ship Network (AFL-VA-ISN) model for intrusion detection in autonomous ships and information management.
- Evaluating the mathematical model of the fuzzy logic system for cyber attack risk assessment in an intelligent ship network environment.
- The simulation findings have been established, and the suggested AFL-VA-ISN model increases the data transmission rate, risk assessment rate, access control rate, and attack detection rate, and reduces the network latency rate compared to other existing models.

2 Related Work

Su et al. [11] suggested the Edge Services and Computing Capability (ES-CC) for Intelligent Maritime Networking (MN). Zhou et al. [12] proposed the System-Theoretic Process Analysis (STPA) for autonomous ships' safety and security co-analysis. Bolbot et al. [13] recommended the novel cyber-risk assessment method (NCRAM) for ship systems. Liu et al. [14] presented the Deep Learning-Powered Vessel Trajectory Prediction (DLPTP) for Improving Smart Traffic Services in the Maritime Internet of Things (IoT). Chen et al. [15] introduced the Video-based Detection Infrastructure Enhancement (VDIE) for Automatic Ship Recognition and Behavior Analysis. The author suggested a you only look once (YOLO) paradigm to analyze ship behaviour. Kavallieratos and Katsikas [16] discussed the Managing Cyber Security Risks of the Cyber-Enabled Ship. In this paper, the author uses the STRIDE and DREAD methodologies to evaluate the cyber-risk of Cyber-Physical System on digitalized ships, both now and in the future. Jiang et al. [17] offered the Bayesian network approach (BNA) for risk analysis of maritime accidents along the main route of the Maritime Silk Road (MSR).

Göksu et al. [18] deliberated the Fuzzy-Bayesian networks (FBN) to assess the Ship steering gear failure risk. This research uses Fuzzy-Bayesian Networks to assess potential risks and investigate the reasons behind on-board steering gear failures. Xin et al. [19] suggested graph-based ship traffic partitioning for intelligent maritime surveillance. A technique of probabilistic conflict detection is used first to construct a composite similarity measure, and then, maritime knowledge mining is used to train a newly constructed network for maritime traffic routes. Enoch et al. [20]

proposed the Novel Security Models, Metrics, and Security Assessment for Maritime Vessel Networks. Ameeq et al. [21] discussed the group-acceptance sampling plan following an alpha power transformation-inverted perks distribution. When determining the test termination and consumer risk, design criteria like the acceptance number and minimum group size are reached using the median as a quality indicator.

Imran et al. [22] introduced the Kumaraswamy Bell exponential (KwBE). The author provides a GASP for the shortened life test based on the KwBE model, where median life is used as a quality measure. In addition, the length of the test and the customer risk are defined to obtain the critical design parameters. They looked at GASP using an ordinary sampling strategy (OSP). Hussain et al. [23] presented the acceptance sampling plan for the odd exponential-logarithmic (OEL) Fréchet distribution. The suggested model is based on the difficulties encountered by objects with varying densities (right-skewed, j-shaped, reversed, and nearly symmetric) and varying danger rates. Kanwal et al. [24] proposed the weighted Weibull detection model for line transect sampling. The author used Bayesian and maximum-likelihood estimation techniques to ensure that the parameter estimates were spot on. To evaluate this model's efficacy, the author compared its population size estimations to those of other popular parametric estimating approaches. Ameeq et al. [25] recommended the Marshall–Olkin Lomax (NMOL) distribution. The density shapes shown by the NMOL distribution were diverse and included symmetry, right-skewness, reversed-J shape, upside-down bathtub curves, and scenarios with varied trends (increasing, decreasing, or no trend at all). The NMOL model was used to evaluate the insurance and failure data practically. On top of that, the NMOL distribution was used to create a GASP, where the median was used as a quality metric.

Begum and Venkataramani [26] suggested the New Compression Scheme for Secure Transmission. This article suggests a new algorithm, encryption and compression (CEC), for data security and compression. The data are compressed to make it shorter using this approach. Using a novel encryption technology, the compressed data are compressed without sacrificing information security or compression performance. Venkataramani and Begum [27] proposed the Efficient Text Compression for Massive Volume of Data. This proposal aims to provide a novel approach to ASCII text compression that works well across a range of document sizes. This algorithm is split into two parts. In the first step, the input strings are transformed into dictionary-based compression. Begum and Venkataramani [28] recommended the novel multi-dictionary-based text compression. The system as a whole is quick and almost perfect on the test files. The authors of this paper provide Multidictionary with burrows wheeler transforms (MBRH), an innovative, fast dictionary-based text compression method, to achieve better performance across a range of document sizes.

3 Adaptive Fuzzy Logic-Assisted Vulnerability Analysis of Intelligent Ship Network (AFL-VA-ISN)

Smart ships, equipped with enhanced monitoring, communication, and connection capabilities, are now expected by leading ship manufacturers and operators. These ships will allow for remote ship management from any location using land-based services. As a cyber-physical system (CPS) that incorporates resources, data analysis, and processing, an intelligent ship network incorporates the benefits of sensors, intelligent control, big data, communication technology, and other inclusive technologies. With its help, ships can automatically interpret data about their equipment, the maritime environment, port logistics, and more, allowing for real-time control and decision-making. As intelligent ship CPS is included in the system, its complexity increases. When cybercriminals target weak points in a ship's network, they may compromise its data and control systems, leading to disastrous accidents. Data security is of utmost importance in the real-time data exchange of intelligent ships. The data in a network carry the information. Ensuring secure data allows ships to get accurate environmental information and instructions faster. On the one hand, it protects ships' navigational integrity; on the other, it shields ship operators' assets against privacy and data breaches. The shore-based platform must continuously gather status information from intelligent ships throughout navigation. This information is used for auxiliary decision-making, real-time remote control, and status monitoring. The exposure of communication systems, location sensors, and vehicle control systems to high-risk circumstances, such as terrorism, should be avoided. Due to the little data change shown by the intelligent ship meteorological data, CPS's engine room data, and ocean current information, the messages' contents quickly become identical. In addition, the symmetric encryption technique is vulnerable to ciphertext and selective attacks, yet it is less sensitive to the plaintext version of the same data. Regarding remote intelligent ships, the control centre on land takes over all aspects of the operation, including situation analysis, direct control, and indirect control. Hence, this study presents Adaptive Fuzzy Logic-assisted Vulnerability Analysis of Intelligent Ship Networks (AFL-VA-ISN) in various cyberattack scenarios for autonomous ship intrusion detection and information management.

Figure 1 shows the proposed AFL-VA-ISN model. The data are taken from the Cyber Threat Data for New Malware Attack Kaggle Dataset [29]. This study designed a hybrid architecture comprising satellite and terrestrial elements and

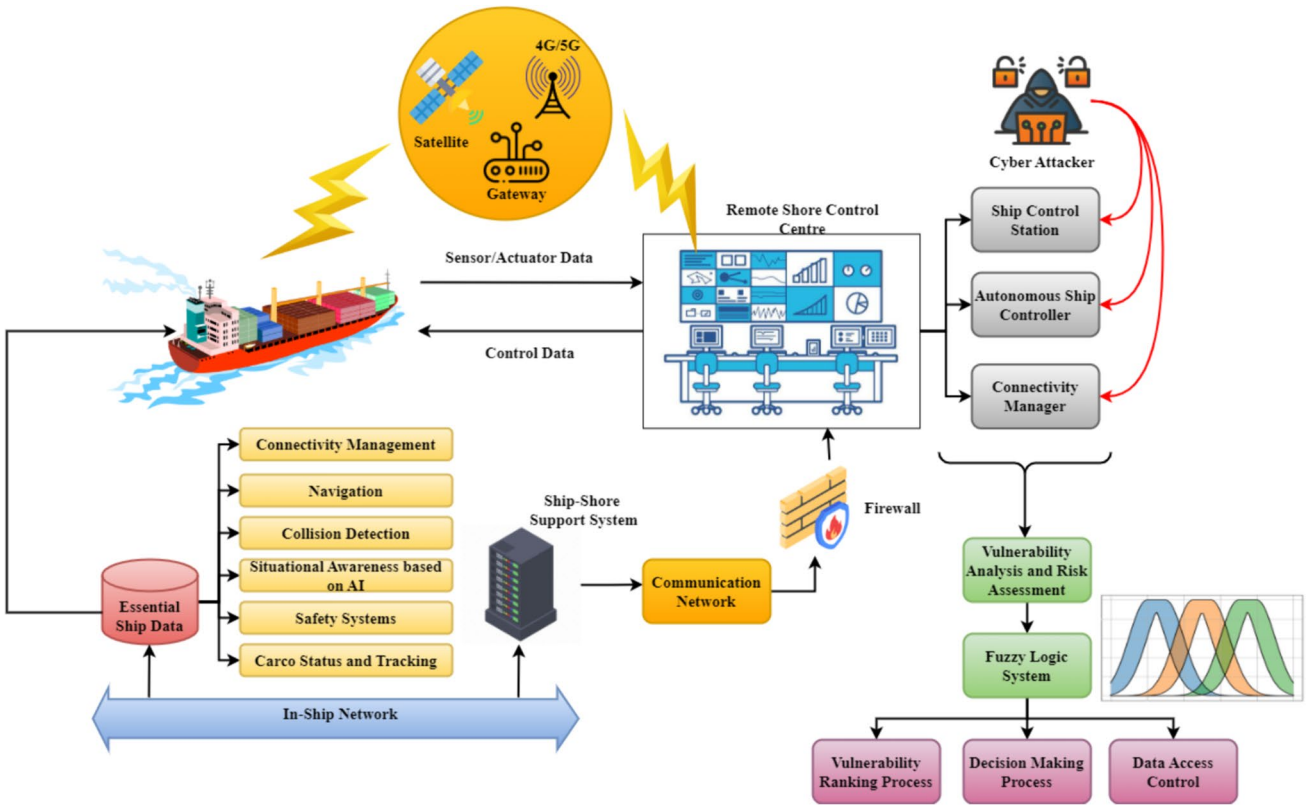

Fig. 1 Proposed AFL-VA-ISN model

probable high-altitude platform elements. The ship is linked to remote shore control centres with numerous redundant systems to guarantee resilient operations.

3.1 Essential Ship Data

Essential ship data databases collect data required for autonomous and remote-controlled operations. Various sensors and systems, including radars, temperature, infrared cameras, wind detectors, etc., contribute to the data utilized for collision detection and situational awareness. This information is used with navigational data from the Global Positioning System (GPS) and the Automatic Identification System (AIS) to determine the safest way to sail in any weather. Data from remote-sensing satellites, such as ice coverage and storm statistics, may be included to enable proactive route adjustment far in advance of any issues. Satellites or the shore control centre (SCC) may be the source of remote-sensing data. The ship's autopilot and autonomous navigation system (ANS) utilize all these data to navigate safely, regardless of the surroundings. In addition to devices for preventing collisions, the ship has fire extinguishers, optical sensors for monitoring the ship's state, and fire alarms and doors. Safety equipment mandatory by the Global Maritime Distress and Safety System (GMDSS) includes search and rescue transponders (SART) detectable by X-band radars or emergency position indication radio beacons (EPIRBs) that allow satellites to pinpoint the ship's location. When ships are having difficulty, both are crucial for finding them. The data about machinery and automation include actuators and sensors, which are utilized to control and monitor mechanical components. For instance, it is necessary to convey data to distant operators while monitoring the propulsion system, engines, cargo, and ballast tank condition. For example, reducing cargo ships' waiting times and increasing fuel economy are two areas where logistics chain development and cooperative optimization with ports may be very beneficial. Digitalization and automation of ships will enhance people's work experience by allowing them to focus on other tasks, such as automated routing, collision avoidance, and the possibility of unmanned bridges a portion of the time.

3.2 Connectivity Management and Sensor Fusion

Multiple high-resolution sensors rapidly increase the overall quantity of situational awareness (SA) data. Sensor fusion reduces the volume, and just the required portion of the data is delivered to human operators. The performance of various sensors varies. Though inexpensive and delivering great spatial resolutions with colour data, the image quality of

optical cameras is quite sensitive to environmental factors like lighting and weather. The fusion of sensors improves the system's stability and dependability and expands its sensing capabilities. Efficient sensor fusion is crucial for autonomous ships and other on-board reasoning and decision-making systems. Sensor fusion requires secure semantic interoperability of actuator and sensor information for autonomous and remote-controlled ships. Connectivity management selects the most appropriate radio access techniques and routes to the data, guaranteeing end-to-end resource management. A gateway that allows various networks and devices to communicate with one another is essential for effective connection management. The gateway utilizes protocol transformation to link network components and technologies, linking the ship's sensors and actuator to the decision-making and the external ecosphere. Transmission range, throughput, and latency are some of the quality-of-service characteristics used in decision-making processes related to various access modes. In other words, the connection manager chooses the access technology based on the applications' quality-of-service needs. Important selection criteria include the cost and security of the access technology. Therefore, to balance the interests of many entities in the system, the connection decision is made using numerous criteria concurrently. To guarantee end-to-end service, the integrated satellite-terrestrial architecture may leverage 5G capabilities, including quality-of-service control, prioritization, and network slicing. Prioritizing vital data ensures its prompt delivery, even in times of crisis, whereas non-critical data might be delayed. A virtual or physical network segment might be devoted to the vital data related to autonomous ships.

3.3 AI in Cyber Attack Scenario

Additionally, regarding the cybersecurity of the ship's systems, the cybersecurity of AI technology must also be measured to guarantee the safety of automatic ships. This paper shows potential cyberattack scenarios on autonomous ships' AI systems by determining numerous vulnerabilities and using research instances of the ship's systems and AI technologies. Datasets, neural networks housed in ship control stations, protocols, and data about autonomous ship control and sensors are vulnerable to cyber-attacks. Unsecured AI models, neural networks, sensors, and protocols are potential entry points for attackers targeting autonomous ships in any attack scenario.

3.4 Vulnerability Analysis and Risk Assessment Using Fuzzy Logic Systems

The autonomous navigation systems of automated ships may be classified depending on how failures affect the system, the sensors and controllers used, and the on-board usage and application of computer-based systems. There is a suggested design for a potential fuzzy logic system that can identify cyber-attacks. It enables the operational staff of the security operations centres (SOC) to make reasonable and speedy selections for their detection. The technologies used include machine learning, data mining, artificial intelligence, and big data processing. Results shown dispersedly are not sufficiently obvious to demonstrate the difference between the assessments, making it impossible to evaluate the vulnerability levels. Therefore, to make the ranking process easier, this study provides a crisp value linked to each expression in the language. One last step is to rate the vulnerability of various straits and canals by utilizing the predicted utility values to prioritize the findings. Vulnerability analysis involves identifying weaknesses or susceptibilities within a system that could be exploited by potential threats or attackers in the ship information network. Fuzzy logic systems can model and quantify the vulnerability linked with different system elements or aspects, considering various factors such as accessibility, complexity, and criticality.

Any place where information monitoring interacts with other monitoring equipment, whether on land or in space, and the region that supports the information transmission and communication network are all part of the physical domain of navigational monitoring. Intelligent ship navigational information systems generate, analyze, and share data, and the area where these activities occur is known as the information domain of navigation monitoring. Tasks are assigned and carried out by the navigational information monitoring command centre in the cognitive domain of navigation monitoring. To ensure the smart ship navigational information system operates effectively, it is crucial to maintain the validity of the information. The monitoring progression handles these data, the primary carrier of interaction behaviours traversing all three domains. Our smart ship navigational information system efficacy assessment indicators are built to correctly depict the many underlying subsystems based on information integrity, accuracy, and timeliness. This study selects key indications for the information's timeliness, accuracy, and integrity. The following is a complete metric that may be used to determine how successful an intelligent ship navigational information system is

$$E = f\left(E^1_{Integrity}, E^2_{accuracy}, E^3_{timeliness}, \varphi_1, \varphi_2, \varphi_3\right). \tag{1}$$

As shown in Eq. (1), where f denotes an aggregation function that represents smart ship navigational information system efficacy, $E^1_{Integrity}$ signifies the integrity of monitoring data, $E^2_{accuracy}$ denotes the accuracy of monitored data, $E^3_{timeliness}$ symbolizes the timeliness of monitoring data, and

φ_1, φ_2, and φ_3 specify the relative significance of the three indicators.

Adjacency matrics B signifies the links relating every pair of nodes in an intelligent ship network. The component b_{ji} of the adjacent matrics, B equals 1 if there is a link from nodes j to i or 0 if there is no link. If networks are directed, meaning that the edge points in one direction from one node to another node, then nodes have two dissimilar degree, the in-degree $l_{in}(j)$, which count the numbers of its received edge and out-degrees $l_{out}(j)$, which is the overall number of its transmitting edge for cyber attack detection

$$l_{in}(j) = \sum_{i \neq j} b_{ij}, l_{out}(j) = \sum_{i \neq j} b_{ji}, l_{all}(j) = \sum_{i \neq j} b_{ij} \quad or \quad b_{ji}. \tag{2}$$

Since the shipping route is directed, links in networks must be directed. From the asymmetric adjacent matrics B, three types of degrees (i.e., out-degree, in-degree, and all-degree) can be computed.

Connectivity via navigation systems like Global Navigation Satellite Systems (GNSS), AIS, and Radio Detection and Ranging (RADAR) negatively influence the security level of intelligent ship network infrastructures. The Automated Identification System (AIS) signal processing steps provide the framework to examine vulnerabilities and capture the hacker's behaviour. The research presents the Cyclic Redundancy Check (CRC) polynomial equation and calculates the Frame Check Sequence (FCS) to identify the data. A hacker may launch a successful spoofing attack, which might lead to a collision between ships, by transmitting a message on the AIS receiver's correct radio channel using an FCS identical to the computed FCS of the target AIS decoder. The hacker can perform the following changes in the localization: longitude p, latitude $\omega(t, J)$, and altitude $m(t)$, inject false messages. The model of the data transmitted on-ship AIS signals $W_{AIS}(t)$ is given by the subsequent

$$W_{AIS}(t) = expj\omega(t, J) \tag{3}$$

$$\omega(t, J) = \pi \sum_{l=0}^{m} J_l p(t - lT). \tag{4}$$

At satellite receivers, the AIS signal is given by the subsequent

$$r_{AIS} = AS_{AIS}(t - \tau)\exp j\left(2\pi f_D t + \theta\right) + m(t). \tag{5}$$

As inferred from Eqs. (3–5), where AS represents the access to the ship network, r_{AIS} denotes the satellite receiver of the AIS signal, and $t - \tau$ indicates the time variation.

Cybercriminals have been able to use GNSS's lack of authentication and encryption to launch attacks. The most alarming example is using fake location information, greatly increasing the likelihood of accidents. The GPS technique for determining location is shown in Eq. (6). The first stage of a GNSS spoofing attack is signal synchronization with the satellite, and the second is signal power increases. The position (x, y, z) of GPS receiver is the intersection of c_0, c_1, c_2 and c_3 with the following:

$$c_j = \sqrt{(x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2} - (x_0 - x)^2 + (y_0 - y)^2 + (z_0 - z)^2, \quad \text{with } j \in [0, 3] \tag{6}$$

The local period is provided by the following:

$$t_k = t_m + \frac{\sqrt{(x_m - x)^2 + (y_m - y)^2 + (z_m - z)^2}}{d}. \tag{7}$$

As discussed in Eqs. (6) and (7) with t_m is the transmitted period with latency, x_m,y_m and z_m are the position of the satellites m, and d is the speediness of light.

Figure 2 shows the Situational Awareness of the Ship Network using AI Sensor Fusion. A vision system, including radar, CCTV, Light Detection and Ranging (LiDAR), and automatic identification system (AIS), is used in situational recognition and detection technologies. This system can effectively distinguish weather conditions and other objects at sea. To effectively manage a fleet of autonomous boats, the utmost precautions must be taken to protect location data. Consequently, substantial research has been dedicated to detecting GNSS spoofing attacks. Spatial processing techniques are utilized to identify the signal's origins. The Intrusion Ring Alert (IRA) data sent by the satellite formed the basis of a GNSS detection approach. Both the complexity of the receiver and the availability of satellite signals are kept within acceptable limits by the suggested strategy. RADAR plays a crucial role in preventing collisions during navigation and managing the ever-increasing volumes of marine traffic. To get the most precise distance readings between the ship and any other objects they detect, marine radars use two frequency bands, 3 GHz and 10 GHz. Identifying the situation and spotting outliers is possible by combining data from sensors, camera images, audio signals, and a global navigation satellite system (GNSS). The easiest way to determine whether situational recognition works as it should is if the classified and detected results match the AIS message information. Following this, to identify nearby objects and determine the likelihood of collisions based on the intended route. Autonomous ships can already sail, arrive and depart, and moor themselves due to judgment technology, which uses data acquired and forecasted by vision systems. It can anticipate problems, establish a safe and economical navigation path automatically based on weather and sea conditions, and take corrective action before they happen. Through artificial intelligence and

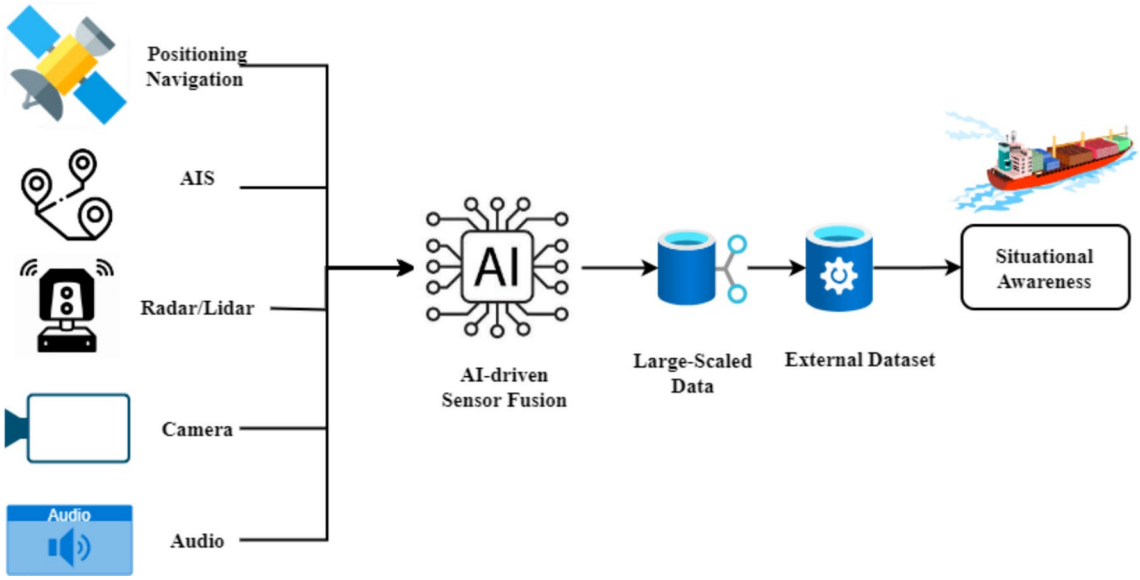

Fig. 2 Situational awareness of ship network using AI sensor fusion

its judgment technology, the ship's location, speed, and engine are controlled by the control and action technology. This technology enables the coastal control centre to operate the ship remotely in an emergency. Laws, standards, and institutions comprise the infrastructure technology, which aligns with port automation technology and can operate autonomous ships. While technologies are classified according to their roles, autonomous ships' systems identify, detect, judge, and control one another depending on data from other systems; hence, they cannot be identified as distinct systems.

As an alternative to using hard figures to represent the likelihood of an occurrence, risk evaluation professionals often use the terms "very possible," "impossible", "possible," and to describe the likelihood of an event. It is more appropriate to utilize triangular fuzzy numbers to indicate the likelihood of an occurrence, since expert knowledge somewhat expresses the event's uncertainty. Triangular fuzzy numbers are vector groups (q_k, q_n, q_g) containing three vectors ranging from 0 to 1, where q_k is the least likelihood of occurrences of the event, q_n is the likelihood of the occurrence of the events, and q_g symbolizes the high likelihood of the occurrence of events. Four tuples can represent triangular fuzzy numbers for risk assessment

The expression respective to the typical triangular fuzzy numbers membership function picture is shown in Eq. (9)

$$\mu_q(q_e) = \begin{cases} \frac{q_e - q_k}{q_n - q_k} \; q_k \le q_e \le q_n \\ \frac{q_g - q_e}{q_g - q_n} \; q_n \le q_e \le q_g \\ 0 otherwise \end{cases}. \tag{9}$$

This attack's sensor node events are evaluated according to expert knowledge, with five likelihood categories (low, potential, moderate, high, and extremely high) describing the elements that influence their occurrence.

Information security risk analysis for intelligent ship network systems mainly includes threat, asset, and vulnerability detection. Determining the link among the three components of risk analysis allows for an accurate assessment of the likelihood of security events. Equation (10) is a statistical expression for the loss produced by the incidence of security events

$$R(A, T, U) = R\big(Q(T, U), F\big(K_a, U_a\big)\big). \tag{10}$$

As shown in Eq. (10), where Q denotes the likelihood of security event caused by system vulnerability; T denotes the likelihood of incidence of basic security event; U denotes the

$$\widetilde{Q}(\beta) = \{\beta_j, q_k, q_n, q_g\} j = 1, 2, \ldots m, k = 1, 2, \ldots m, g = 1, 2, \ldots m, n = 1, 2, \ldots m. \tag{8}$$

vulnerabilities. $F(K_a, U_a)$ represents the loss of asset values instigated by the security events; K_a signifies the loss of the asset values; U_a indicates the level of vulnerabilities. From this, risk value computation formulas can be described. In Eq. (11), K_U denotes the asset values loss caused by obtaining the attack targets and Q_H indicates the likelihood of occurrence of the target node events

$$R = K_U \times Q_H. \tag{11}$$

Combining AI with fuzzy logic systems allows for a more detailed analysis of possible security breaches by offering a framework to deal with ambiguity and imprecision in threat detection. AI-powered systems can monitor autonomous ships' cybersecurity posture in real time and adjust protection measures to counter new threats as they emerge.

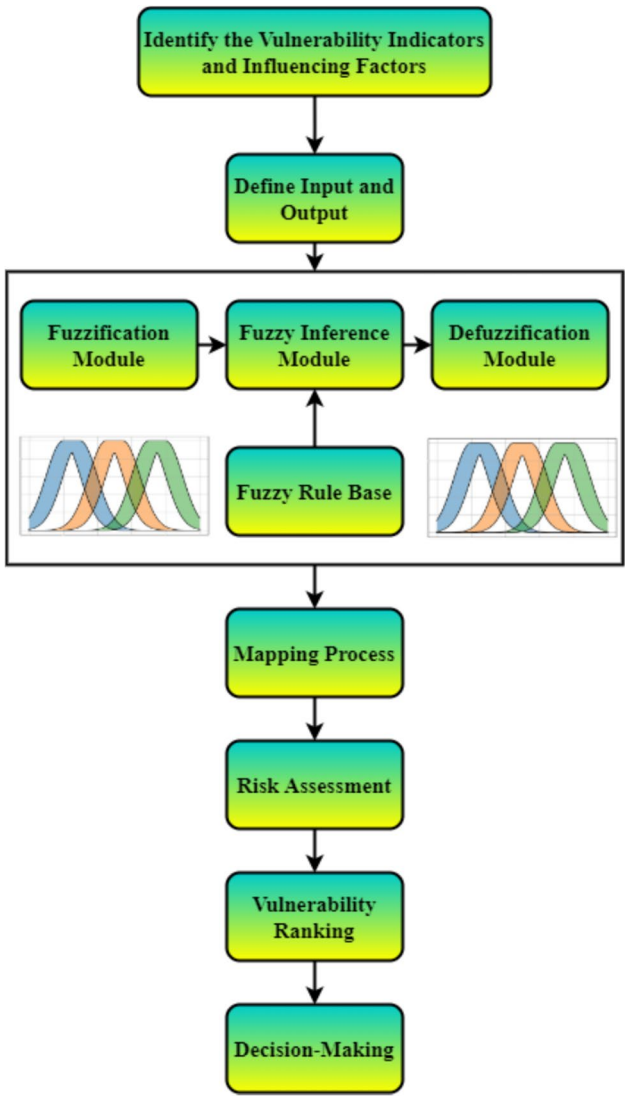

Fig. 3 Flowchart of fuzzy logic system in vulnerability analysis of intelligent ship network

Autonomous ships can adapt to evolving threat environments using fuzzy logic systems, which provide linguistic variables and flexible rules to evaluate the probability and severity of attacks.

Figure 3 shows the flowchart of fuzzy logic system in the vulnerability analysis of an intelligent ship network. Fuzzy theory deals with fuzziness or uncertainties that follow all trust characteristics. The fuzzification module uses term sets and linguistic variables to express the quantitative and qualitative values of the researched factors. Using the proposed model for cyber attack detection, this study considered incomplete data or uncertainties about the network's behaviour. The knowledge base's new fuzzy production rules were generated using an extra rules generation module. This module intersected sets of existing fuzzy rules with the most important language variables determined by experts for every class of cyber-attacks. The foundation of this body of knowledge is an expert-built fuzzy production rule. The fuzzy inference module aims to call on the network's status by establishing a connection between the data input and expert judgments utilizing fuzzy logic. The defuzzification module transformed the fuzzy inference values into crisp ones. All qualities have equal weights, since their significance was considered throughout the mapping process. A navigational risk evaluation for inland waterway transportation systems may be carried out using this innovative method. Node vulnerability indicators might aid a multiple-attribute decision-making analysis to ease the decision-making method. Multicriterion techniques are unique, because they provide a more methodical approach to evaluating the influence of multidimensionality, incommensurability, and uncertainty on decision-making. Remote-controlled and autonomous ships of the future can function without connectivity. The ship's extensive network of actuators, sensors, and radio technologies necessitates gateway device and connection management to optimize resource utilization and guarantee the security and reliability of operations. Using ship simulators and fuzzy logic systems, this article outlines the necessary techniques and discusses how to improve connection research. An efficient way to assess cyber attack detection models and methodologies grounded on fuzzy inference and fuzzy sets was shown by deploying the created simulation models of fuzzy cyber attack detection systems. By comparing the newly established methodological and scientific apparatus with existing ones, this study observes that it has the potential to guarantee the accurate detection of polymorphic cyber-attacks and increase the efficacy of information systems' cyber protection. Compared to other popular methodologies, the suggested AFL-VA-ISN model increases the data transmission, risk assessment, attack detection, access control, and network latency ratio.

Table 1 Simulation variables

Parameter	Value
Virus detection frequency	500 Hz
Calculation channel	85 bit/s
Number of virus attack per unit data channels	10–120 dB
Attack type	Multi-channel 4 direction
Simulation tool	NetLogo V4.1RC5
Self-organizing communication range	3 patches
Network transmission bandwidth	15 bit/dB
Time	54 ticks
DATA packet size	154
Topology	Fixed/random

4 Results and Discussion

This study presents Adaptive Fuzzy Logic-assisted Vulnerability Analysis of Intelligent Ship Networks (AFL-VA-ISN) in various cyberattack scenarios for intrusion detection and information management of autonomous ships. The data are taken from the Cyber Threat Data for New Malware Attack Kaggle Dataset. The performance of the AFL-VA-ISN model has been analyzed based on metrics such as data transmission, risk assessment, attack detection, access control, and network latency ratio. Table 1 shows the simulation variables and their value.

4.1 Data Transmission Rate

The navigational information monitoring system may accomplish transmission of data for the defined distance via a wired or wireless connection. There has to be a certain amount of success with the data transfer. Depending on the activity, the response and command transmission time needed to show instructions after receiving target data must be sufficient. An attack on the ship's communication network or a software flaw in the control system might result in a network attack. The assailant can be a member of the ship's group. They engage in aggressive password cracking to get control of the system and launch attacks by connecting external devices to slave stations. Intentional remote attackers may accomplish their goals by attacking communication networks at the management layer. By deciphering encryption techniques, they can steal several crucial parameters of the ship's control systems. Attackers may utilize replay attacks to deceive systems into sending incorrect data or instructions, increase data transmission delays, and drain network capacity. Furthermore, attackers launching denial-of-service attacks on inside networks might impact devices' availability. Based on Eqs. (3) and (4), the data transmission

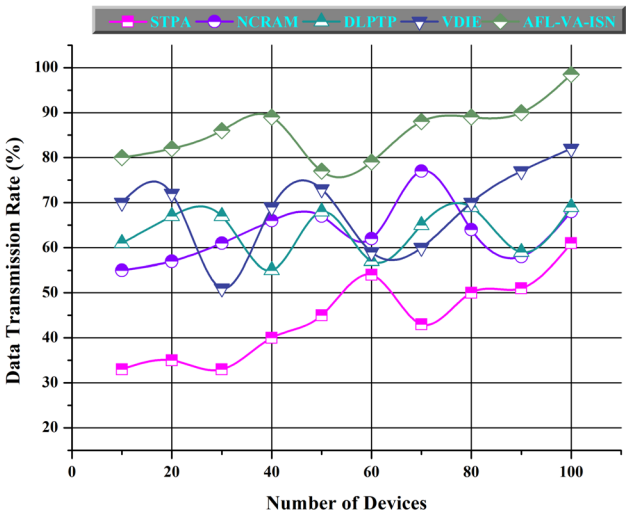

Fig. 4 Data transmission rate

in an intelligent ship network has been analyzed. Figure 4 shows the data transmission rate.

4.2 Risk Assessment Ratio

Innovation in navigational risk assessment via the use of an evidentiary reasoning algorithm and a fuzzy rule-based strategy. The vessel's collision alarm system was programmed to use spatial mapping and timing analysis algorithms to determine the best course of action based on navigational safety data, including AIS information and harbour weather forecasts. With expertise, seasoned navigators often determine the safety range and measure a clearance (such as two nautical miles) to preserve between their ship and any

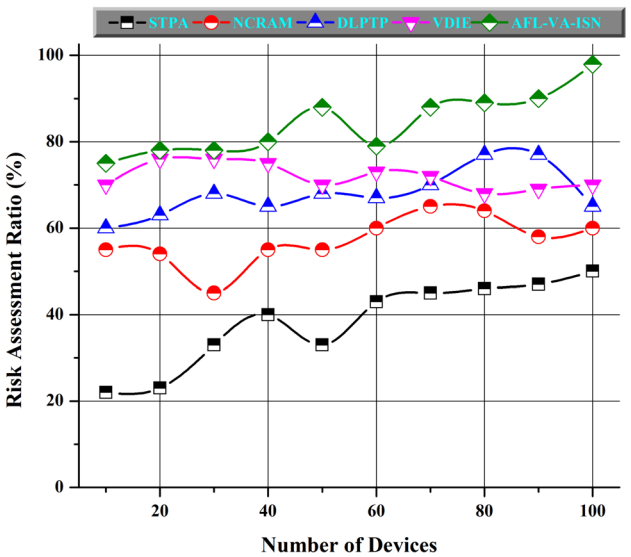

Fig. 5 Risk assessment ratio

other target ships. Ship movement, speed, and traffic circumstances imprecise the clearance. The difference between nodes and disturbances like pirate attacks, maritime accidents, or terrorist strikes may be interpreted as exposure. Based on Eq. (8), the risk assessment rate has been calculated. Figure 5 demonstrates the risk assessment ratio.

4.3 Attack Detection Ratio

To do vulnerability assessments, this research used network modelling to compare the relative importance of nations and their shipping connections before and after the attack. Considering the severity of pirate and terrorist attacks on certain straits and canals, this research incorporates security risk elements. Massive cargo ships are now a part of freight transport, thanks to advancements in marine transportation. This has led to considering the elements linked to accidents in the organizational structure. Most unusual patterns originate from harmful, illegal operations that masquerade as large-scale interactions in traffic flows. These include cyber intrusions, botnet assaults, worm propagation, malicious port scanning, and brute-force attacks. When dealing with faulty or unclear data, fuzzy anomaly detection frameworks may help improve cyberattack detection accuracy by incorporating multiple fuzzy algorithms into distinct operational processes. Based on Eq. (2), attack detection has been determined. Figure 6 illustrates the attack detection ratio.

4.4 Access Control Rate

Attacks against the ship's control station or the shore control centre to gain privileged access might pose the greatest threat to the vessel's safety and attract the attention of terrorists. Accident avoidance and situational awareness systems are particularly vulnerable to malware infections, which may compromise their safety. Onshore corporate information systems make access to the systems on-board linked unmanned ships possible. Remote monitoring, coordination, and ship administration are increasingly crucial tasks for shore-based operations systems, especially as marine vessels grow more unmanned and autonomous. Those in which the perpetrators choose to get physical access to the ship or its systems from a close distance or in which the perpetrators can remotely exploit security holes. A model for access control is being developed for use in intelligent ship networks; this model will dynamically assess the security risks of access request using contextual sensor data. Based on Eq. (5), the access control rate has been predicted. Figure 7 denotes the access control rate.

4.5 Network Latency Rate

The shown satellite-terrestrial systems rely on spectrum resources. There are two simple ways to improve the restricted bandwidth. The first is the need for a specific spectrum resource, preferably in a higher frequency range, to support marine connection. Second, more resources may be obtained via spectrum sharing. Including this fuzzy logic-based approach in the entire design is possible, as shown in Sect. 3. Important data with low latency might benefit greatly from the shared band. The most crucial functionality in manifold radio access networks is interface assortment. A connection manager's primary responsibilities include determining data priorities, assigning information to accessible communication channel and route, and guaranteeing sufficient capacity for data transmission. Collaboration with neighbouring ships guarantees that all parties get the

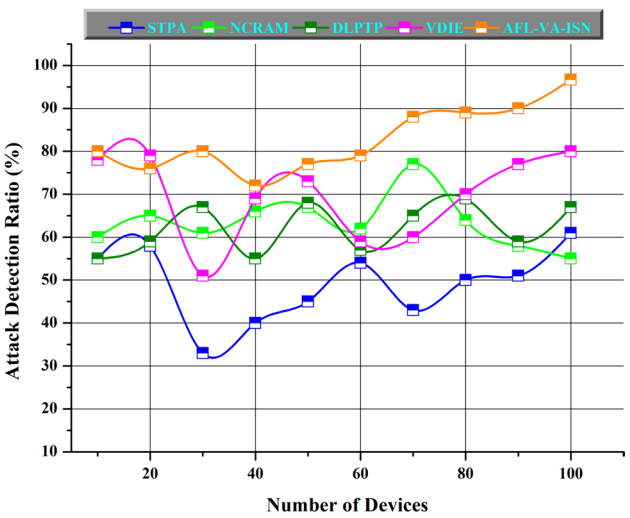

Fig. 6 Attack detection ratio

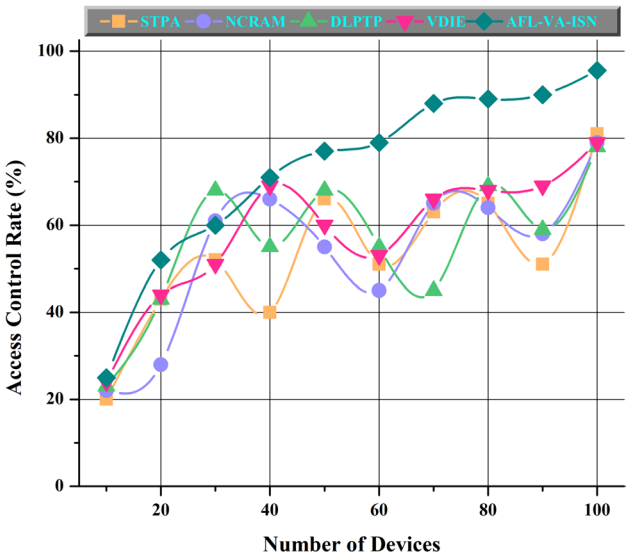

Fig. 7 Access control rate

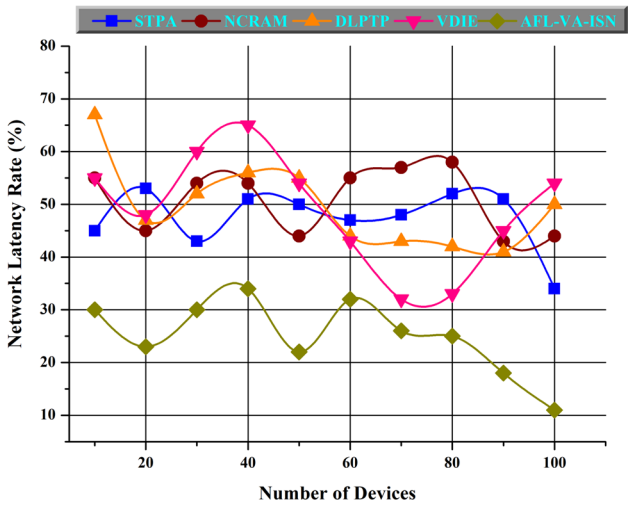

Fig. 8 Network latency rate

necessary service, which is crucial for data integrity and rapid transmission. The shown integrated satellite-terrestrial architecture may take advantage of several 5G technologies, such as network slicing, quality-of-service management, and prioritization, to guarantee end-to-end service and a strong association, for instance, amid the ships and the distant operator. During a disaster, it is essential to prioritize the delivery of key data above less important data, so that the former may wait. Based on Eq. (7), network latency has been detected. Figure 8 signifies the network latency rate.

5 Conclusion

This study presents AFL-VA-ISN in various cyberattack scenarios for intrusion detection and Cybersecurity Measures for Information Management on Autonomous Ships. This research presents an AI-based monitoring and defence technology approach to guarantee smart ship network security. Developing effective security measures designed to reduce identified threats is based on thorough risk assessments conducted within the framework of erecting defences. Security experts may apply controls and safeguards logically, addressing the most serious risks, provided that they thoroughly grasp the organization's unique vulnerabilities and threats. The organization's risk tolerance and commercial goals are considered in this focused defence approach, which guarantees the effective allocation of resources. The two main goals of risk assessment are finding out what threats the system faces and ensuring that protections are in place to deal with them. The uncertainty surrounding the occurrence of attacks can be more accurately represented by interval probabilities derived from fuzzy mathematics and risk probability methods. The foundation of our approach lies in an innovative risk analysis model that integrates a multifaceted array of risk factors, such as the asset's attractiveness, the effectiveness of existing controls, historical risk incidents, and the potential financial and reputational repercussions resulting from threat realization. Unlike the traditional risk model, which primarily focuses on assessing the likelihood and impact of individual events, our approach considers a broader range of factors that better capture the complexity of the system environment. For instance, while the traditional model may solely evaluate the probability of a data breach occurring and its potential financial impact, our innovative model takes into account additional variables such as the organization's susceptibility to social engineering attacks, the resilience of its cybersecurity infrastructure, and the potential cascading effects of a breach on customer trust and market reputation. The fuzzy inference systems employ a set of rules and linguistic variables to assess the likelihood of attacks on the system being realized. By considering various input parameters, such as historical attack data, system vulnerabilities, and threat intelligence, the fuzzy inference systems analyze the uncertainty and imprecision inherent in these factors to generate a probabilistic assessment of the likelihood of potential attacks. After defuzzification, which converts fuzzy linguistic variables into crisp values, the likelihood of a point estimate becomes more consistent, trustworthy, and representative. This transformation ensures that the fuzzy inference results are translated into precise numerical values, providing a clearer and more actionable understanding of the estimated likelihood. By reducing the uncertainty inherent in fuzzy logic-based assessments, defuzzification enhances the reliability and utility of the likelihood estimate for decision-making purposes. Future work will analyze the static evaluation approach, which typically entails analyzing attack scenarios, techniques, and patterns based on predefined criteria and known attack vectors.

Acknowledgements Not applicable.

Author Contributions Dan Lan: writing—original draft, writing—review and editing, conceptualization, methodology, software, and formal analysis. Peilong Xu: writing—original draft, writing—review and editing, conceptualization, methodology, and software. Jia Nong: writing—original draft, validation, formal analysis, visualization, and supervision. Junkang Song: writing—review and editing, validation, visualization, and supervision. Jie Zhao: Writing—review & editing, validation, visualization, and supervision.

Funding This work was supported by Guangxi vocational education teaching reform research project, China. Exploration and Practice of the chain Teaching system of "six in One" in Higher Vocational Colleges under the perspective of "entrepreneurship and Innovation", Project number: GXGZJG2021B096.

Availability of Data and Materials Data will be made available on reasonable request. The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declarations

Conflict of interest There are no potential competing interests in our paper. And all authors have seen the manuscript and approved to submit to your journal. We confirm that the content of the manuscript has not been published or submitted for publication elsewhere.

References

1. Yoo, J.W., Jo, Y.H., Cha, Y.K.: Artificial intelligence for autonomous ship: potential cyber threats and security. J. Korea Inst. Inf. Secur. Cryptol. **32**(2), 447–463 (2022)
2. Dogancay, K., Tu, Z., Ibal, G.: Research into vessel behaviour pattern recognition in the maritime domain: past, present and future. Digit. Signal Process. **119**, 103191 (2021)
3. Illiashenko, O., Kharchenko, V., Babeshko, I., Fesenko, H., Di Giandomenico, F.: Security-informed safety analysis of autonomous transport systems considering AI-powered cyberattacks and protection. Entropy **25**(8), 1123 (2023)
4. Martelli, M., Virdis, A., Gotta, A., Cassarà, P., Di Summa, M.: An outlook on the future marine traffic management system for autonomous ships. IEEE Access **9**, 157316–157328 (2021)
5. Zhang, Y., Zhang, D., Jiang, H.: A review of artificial intelligence-based optimization applications in traditional active maritime collision avoidance. Sustainability **15**(18), 13384 (2023)
6. Karaca, İ, Saraçoğlu, R., Söner, Ö.: Meteorological risk assessment based on fuzzy logic systems for maritime. J. ETA Marit. Sci. **10**(2), 97–107 (2022)
7. Poornikoo, M., Øvergård, K.I.: Levels of automation in maritime autonomous surface ships (MASS): a fuzzy logic approach. Marit. Econ. Logist. **24**(2), 278–301 (2022)
8. Hu, Y., Park, G.K.: Collision risk assessment based on the vulnerability of marine accidents using fuzzy logic. Int. J. Naval Archit. Ocean Eng. **12**, 541–551 (2020)
9. Jiang, M., Wang, B., Hao, Y., Chen, S., Lu, J.: Vulnerability assessment of strait/canals in maritime transportation using fuzzy evidential reasoning approach. Risk Anal. **43**(9), 1795–1810 (2023)
10. Shi, Z., Zhen, R., Liu, J.: Fuzzy logic-based modeling method for regional multi-ship collision risk assessment considering impacts of ship crossing angle and navigational environment. Ocean Eng. **259**, 111847 (2022)
11. Su, X., Meng, L., Huang, J.: Intelligent maritime networking with edge services and computing capability. IEEE Trans. Veh. Technol. **69**(11), 13606–13620 (2020)
12. Zhou, X.Y., Liu, Z.J., Wang, F.W., Wu, Z.L.: A system-theoretic approach to safety and security co-analysis of autonomous ships. Ocean Eng. **222**, 108569 (2021)
13. Bolbot, V., Theotokatos, G., Boulougouris, E., Vassalos, D.: A novel cyber-risk assessment method for ship systems. Saf. Sci. **131**, 104908 (2020)
14. Liu, R.W., Liang, M., Nie, J., Lim, W.Y.B., Zhang, Y., Guizani, M.: Deep learning-powered vessel trajectory prediction for improving smart traffic services in maritime internet of things. IEEE Trans. Netw. Sci. Eng. **9**(5), 3080–3094 (2022)
15. Chen, X.Q., Wang, M., Ling, J., Wu, H., Wu, B., Li, C.: Ship imaging trajectory extraction via an aggregated you only look once (YOLO) model. Eng. Appl. Artif. Intell. **130**, 107742 (2024)
16. Kavallieratos, G., Katsikas, S.: Managing cyber security risks of the cyber-enabled ship. J. Mar. Sci. Eng. **8**(10), 768 (2020)
17. Jiang, M., Lu, J., Yang, Z., Li, J.: Risk analysis of maritime accidents along the main route of the maritime silk road: a Bayesian network approach. Marit. Policy Manag. **47**(6), 815–832 (2020)
18. Göksu, B., Yüksel, O., Şakar, C.: Risk assessment of the Ship steering gear failures using fuzzy-Bayesian networks. Ocean Eng. **274**, 114064 (2023)
19. Xin, X., Liu, K., Loughney, S., Wang, J., Li, H., Yang, Z.: Graph-based ship traffic partitioning for intelligent maritime surveillance in complex port waters. Expert Syst. Appl. **231**, 120825 (2023)
20. Enoch, S.Y., Lee, J.S., Kim, D.S.: Novel security models, metrics and security assessment for maritime vessel networks. Comput. Netw. **189**, 107934 (2021)
21. Ameeq, M., Tahir, M.H., Hassan, M.M., Jamal, F., Shafiq, S., Mendy, J.T.: A group acceptance sampling plan truncated life test for alpha power transformation inverted perks distribution based on quality control reliability. Cogent Eng. **10**(1), 2224137 (2023)
22. Imran, M., Bakouch, H.S., Tahir, M.H., Ameeq, M., Jamal, F., Mendy, J.T.: A new Bell-exponential model: properties and applications. Cogent Eng. **10**(2), 2281062 (2023)
23. Hussain, N., Tahir, M.H., Jamal, F., Ameeq, M., Shafiq, S., Mendy, J.T.: An acceptance sampling plan for the odd exponential-logarithmic Fréchet distribution: applications to quality control data. Cogent Eng. **11**(1), 2304497 (2024)
24. Kanwal, S., Tahir, M.H., Jamal, F., Ameeq, M., Mendy, J.T.: A weighted Weibull detection model for line transect sampling: application on wooden stake perpendicular distance data. Cogent Eng. **11**(1), 2303237 (2024)
25. Ameeq, M., Naz, S., Tahir, M., Muneeb Hassan, M., Jamal, F., Fatima, L., Shahzadi, R.: A new Marshall-Olkin lomax distribution with application using failure and insurance data. Statistics **58**, 450–472 (2024)
26. Begum, M.B., Venkataramani, Y.: A new compression scheme for secure transmission. Int. J. Autom. Comput. **10**, 578–586 (2013)
27. Begum, M.B., Venkataramani, Y.: A Novel Multidictionary Based Text Compression. J. Comput. Sci. **8**(12), 1940 (2012)
28. Begum, M.B., Venkataramani, Y.: An efficient text compression for massive volume of data. Int. J. Comput. Appl. **975**, 8887 (2011)
29. https://www.kaggle.com/datasets/zunxhisamniea/cyber-threat-data-for-new-malware-attacks