Journal of *Marine Science and Engineering*

MDPI

Article

Risk Analysis of Pirate Attacks on Southeast Asian Ships Based on Bayesian Networks

Qiong Chen [1], Jinsheng Zhang [1], Jiaqi Gao [1,*], Yui-Yip Lau [2], Jieming Liu [1], Mark Ching-Pong Poo [3] and Pengfei Zhang [1]

[1] Navigation College, Jimei University, Xiamen 361021, China; qchen@jmu.edu.cn (Q.C.); zjsfchihn@163.com (J.Z.); liujieming0714@163.com (J.L.); shippinglaw@163.com (P.Z.)
[2] Division of Business and Hospitality Management, College of Professional and Continuing Education, The Hong Kong Polytechnic University, Hong Kong, China; yuiyip.lau@cpce-polyu.edu.hk
[3] Liverpool Hope Business School, Liverpool Hope University, Liverpool L16 9JD, UK; pooc@hope.ac.uk
* Correspondence: 15698480612@163.com

Abstract: As a bridge for international trade, maritime transportation security is crucial to the global economy. Southeast Asian waters have become a high-incidence area of global piracy attacks due to geographic location and complex security situations, posing a great threat to the development of the Maritime Silk Road. In this study, the factors affecting the risk of pirate attacks are analyzed in depth by using the Global Ship Piracy Attacks Report from the IMO Global Integrated Shipping Information System (GISIS) database (i.e., 2013–2022) in conjunction with a Bayesian Network (BN) model, and the Expectation Maximization algorithm is used to train the model parameters. The results show that piracy behaviors and the ship's risk are the key factors affecting the risk of pirate attacks, and suggestions are made to reduce the risk of pirate attacks. This study develops a theoretical basis for preventing and controlling the risk of pirate attacks on ships, which helps maintain the safety of ship operations.

Keywords: piracy behaviors; Bayesian network; expectation maximization algorithm; risk analysis; global integrated shipping information system; ship safety

Citation: Chen, Q.; Zhang, J.; Gao, J.; Lau, Y.-Y.; Liu, J.; Poo, M.C.-P.; Zhang, P. Risk Analysis of Pirate Attacks on Southeast Asian Ships Based on Bayesian Networks. *J. Mar. Sci. Eng.* **2024**, *12*, 1088. https://doi.org/10.3390/jmse12071088

Academic Editor: Lúcia Moreira

Received: 9 June 2024
Revised: 25 June 2024
Accepted: 25 June 2024
Published: 27 June 2024

1. Introduction

Maritime transportation is an essential link in international trade. Currently, 90 per cent of world trade is realized through maritime transport, and more than 90 per cent of China's foreign trade is also carried out. With the development of economic globalization, domestic and foreign reliance on maritime transport is increasing. However, in maritime transportation, piracy and hijacking can pose a major threat to international trade and seriously impact the safety and stability of maritime transportation routes.

The Bayesian Network (BN) is a probabilistic graphical model that expresses conditional dependencies between variables in the form of directed acyclic graphs (DAGs) and is used for probabilistic reasoning and decision making [1]. BNs can be used to model and infer the interactions between various factors and their effects on pirate attacks in the analysis of pirate attacks. By constructing a BN model, it is possible to comprehensively consider the determining factors of piracy attacks, such as geographic location, time, pirates' motivation and ability, ships' defense measures, and the deployment of maritime security forces [2]. In BNs, nodes represent random variables, and edges represent probabilistic dependencies between variables. Through prior and conditional probabilities, BNs can dynamically assess the risk of pirate attacks by continuously updating and retesting the probabilities based on new pirate attacks [3]. For example, through BN analysis, it is possible to identify the key causal factors and related influences on the risk of pirate attacks [4], assess the effectiveness of different anti-piracy measures [5], and develop contingency plans [6].

The research of this paper aims to examine the risk factors of ship piracy attacks by combining the Global Ship Piracy Attacks Report (2013–2022) in the database of the International Maritime Organization's Global Integrated Shipping Information System (IMO GISIS) with the relevant studies of domestic and international scholars. A BN model is applied to explain the basis of this study relevant to the risk of ship piracy attacks, identify the BN nodes, determine the final BN structure, and train the model parameters through the Expectation Maximization (EM) algorithm to study the main reasons for the occurrence of the risk of piracy attacks on ships in Southeast Asia and the associated influencing factors.

The main contributions of this paper are as follows: (1) Analyzing the determining factors contributing to the piracy phenomenon in Southeast Asia from the IMO GISIS database. (2) Constructing a risk prediction model for piracy attacks using the BN model. (3) Using the EM algorithm to train the model parameters.

2. Literature Review

Domestic and international research on piracy attacks mainly focuses on analyzing, managing, and controlling piracy attacks. Psarros et al. [7] and Pristrom et al. [8] conducted a regression analysis of cases in the database of the International Maritime Organization (IMO) to find out the main factors affecting piracy attacks. Li et al. [9] used Fractional Adaptive Direct Twiddling (FADTW) to analyze the impact of piracy factors in pirate attacks. Vanek et al. [10] created the Agent-Based model to simulate the individual behavior of ships, which provides a basis for effectively implementing anti-piracy measures by maritime stakeholders. He et al. [11] employed the LDA modeling method to conduct risk analysis of pirate attacks.

The BN is commonly used in various fields, including behavioral analysis, sensitivity analysis, and decision management. Amal et al. [12] used the BN model to examine the impacts of piracy factors in pirate attacks. Hu et al. [13] and Fan et al. [14] established a model based on the BN model for analyzing the three main factors for piracy attacks: environmental settings, physical characteristics of piracy events, and logical features of piracy events on maritime routes. Liu et al. [15] combined the cloud model to propose a BN risk analysis and probabilistic prediction model. Pristrom et al. [16] proposed a BN-framed analytical model to predict the likelihood of the recurrence of pirate attacks.

The above literature review can be categorized into two main types: One is for analyzing and predicting the combined factors of piracy attacks using the BN model. The other is for estimating the main characteristics of piracy attacks using the double-layer planning model and Agent-Based model. The research factors and methods of these two categories are organized in Table 1. In this paper, a BN model is built to add the piracy factor to the attack event based on other comprehensive factors, and the EM algorithm is employed to train the model parameters to examine the risk of piracy attacks in depth.

Table 1. Pirate attacks, important literature collation.

Research Articles	Research Factors	Research Model
Li et al. [9]	Pirate factors	Double-layer planning model
Vanek et al. [10]	Ship factors	Agent-Based model
Hu et al. [13]	Ship, pirate factors	BN model
Pristrom et al. [16]	Ship, environment, protection factors	BN model
This study	Ship, environment, protection, piracy factors	BN model

3. Analysis of Factors Affecting Piracy Attacks on Ships

Currently, global piracy attacks are still occurring on a global scale [17]. To examine the risk impact factors of ship piracy attacks, it is necessary to use ship piracy attack information to support them. Therefore, this study selected 1126 pirate data from the IMO GISIS database for the past ten years, from 2013 to 2022, as the research object for data

analysis, and the results are shown in Table 2. The table shows that the piracy attacks in Southeast Asia occupy a relatively large proportion of global piracy incidents. From 2013 to 2015, the proportion was more than 50%, indicating that Southeast Asia is the main region of global piracy activities. Starting from 2016, the Southeast Asian region's share of global piracy attacks began to decline but then increased again in 2021 and 2022, to 49% and 58%, respectively. In recent years, the incidents of pirate attacks in the South China Sea have been decreasing annually due to the increased efforts in anti-piracy measures by China. Conversely, the overall trend in pirate attacks in the Strait of Malacca has been on the rise. This has led to a situation where, despite a general decline in pirate attacks across Southeast Asia, the proportion of incidents in the Strait of Malacca has been increasing year by year. Consequently, pirate attacks in Southeast Asia have consistently accounted for a significant proportion of global pirate attacks.

Table 2. Piracy in Southeast Asia (2013–2022).

Year	South China Sea	The Strait of Malacca	The Sum of South China Sea and The Strait of Malacca	The Sum of Global	Proportion
2013	142	22	164	307	53%
2014	92	82	174	291	60%
2015	83	135	218	306	71%
2016	68	21	89	221	40%
2017	62	26	88	206	43%
2018	60	8	68	224	30%
2019	34	45	79	193	41%
2020	37	48	85	228	37%
2021	15	70	85	172	49%
2022	4	72	76	131	58%

Under this setting, this paper comprehensively analyzes the risk factors for pirate attacks on ships from four key dimensions: the ship's characteristics, the surrounding environmental conditions, the protective measures taken, and the piracy factor.

3.1. Vessel's Risk Factors

Two main factors influence the risk of the ship itself: ship type and ship condition. The impact of ship type on the risk of pirate attacks is mainly reflected in the type of goods carried and the height of the dry side [18]. Ships carrying high-value cargo are more likely to be the target of pirates, and the corresponding risk of pirate attacks will increase. Ships with lower dry docks increase the risk of pirate attacks due to the lack of sufficient physical barriers that allow pirates to carry out boarding operations quickly and relatively easily. The design features of ships with type A dry-docks, such as oil tankers, include open decks with a high degree of integrity; fewer openings on the deck, thus providing better containment; and small dry-docking requirements with a correspondingly large draught. By contrast, B-type dry-side ships, such as bulk carriers and container ships, whose open decks do not have the same integrity as tankers and have more openings on the deck, such as hatches for the loading and unloading of cargoes, require a higher dry-side to accommodate the higher number of openings on their decks and loading and unloading needs, and have higher dry-side requirements. Thus, this paper adopts a broad classification method to distinguish ship types based on their drywall height. The relatively low dry deck of tankers, liquefied petroleum gas (LPG) vessels, liquefied natural gas (LNG) vessels, barges, fishing vessels, tugs, and yachts are categorized as low-dry-deck vessels; cargo ships are defined as medium-dry-deck vessels; and container ships and ro-ro vessels are classified as high-dry-deck vessels.

The state of the waters in which the ship is located is also an essential factor. According to data released by the IMO, as shown in Figure 1, piracy incidents occurring in ports and territorial waters account for 72% of global piracy incidents from 2013 to 2022. This

indicates that ships located in ports or territorial sea areas are at a relatively high risk of experiencing pirate attacks. In the port berth, the crew of the pirates will be laxer, vigilance may be reduced, and the port personnel is relatively complex, greatly increasing the risk of pirate attacks. Ships located in the territorial sea area have relatively slow speeds, and pirates usually use fast and simple means of transportation, making chases and attacks more likely to occur.

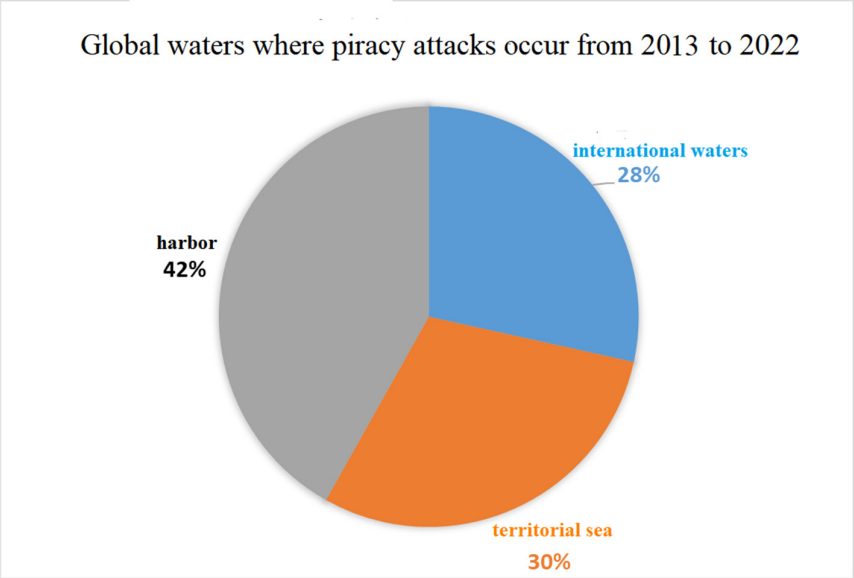


Figure 1. Global waters of piracy attacks, 2013–2022.

Therefore, this paper uses ship type and state as the parent nodes of the ship's risk factors.

3.2. External Environmental Factor

The external environment also significantly impacts the risk of pirate attacks. The external environmental factors affecting the risk of pirate attacks are the time and monsoon factors. From the time factor, this paper defines the local time between 6:00 and 18:00 as daytime and the rest of the time as nighttime, and after processing the data as in Figure 2, it can be found that the vast majority of pirate attacks in Southeast Asia occur in the darkness of the night, accounting for 75% of all pirate incidents. Pirates in Southeast Asia usually approach ships in high-speed vessels with the help of darkness, control the crew, and damage communication equipment after boarding, aiming to steal high-value goods from the ship [19]. In a dark environment, the lack of natural light leads to reduced visibility at sea, significantly affecting the crew's vision. The restricted range of vision weakens the effectiveness of the lookout, making it difficult for the crew to accurately monitor abnormalities in the surrounding environment in a timely manner. Under such circumstances, it becomes complicated to detect the movements of pirates and take corresponding countermeasures promptly, thus increasing the risk of ships encountering pirate attacks at night.

On the other hand, if the ship is in the monsoon region and is affected by the monsoon, the strong winds and waves brought by the monsoon will make the sea conditions extremely poor, which poses a challenge to the stability of the ship, leading to difficulties in maneuvering the ship, seriously affecting its maneuverability. While most of the transportation used by pirates are simple wooden boats or speedboats [20], the pirate attack operations will also be limited; the operational risk of these vessels increases, thus reducing the frequency of pirate attacks and, to a certain extent, reducing the probability of the occurrence of pirate attacks. In summer, Southeast Asia is susceptible to the southwest monsoon. So, this paper analyzes the monsoon period by noting June to August as the monsoon period and the rest of the dates as the non-monsoon period.

Therefore, this paper takes time and monsoon period as the parent nodes of external environmental factors.

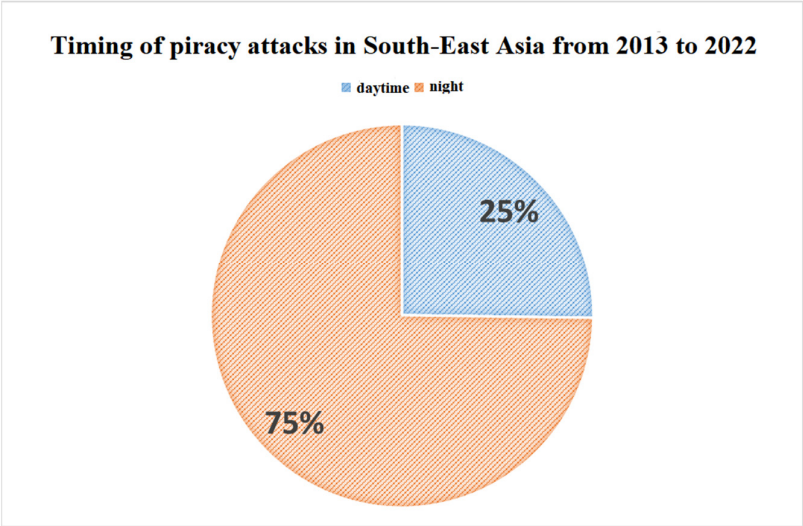


Figure 2. Timing of piracy attacks in Southeast Asia, 2013–2022.

3.3. Protection Factors

Protection factors are quite important. The ship cannot control the behavior of pirates but can enhance self-protection measures to effectively reduce the possibility of pirates successfully carrying out attacks. Implementing preventive security strategies can significantly improve the ability of ships to resist pirate attacks. Adopting appropriate protective measures can effectively reduce the impact of pirate attacks, and the crew can find pirates promptly and convey information promptly. The captain can also quickly take countermeasures to effectively reduce the risk of pirate attacks and protect the crew, cargo, and the purpose of the ship itself.

In addition, the sending of emergency alerts in a timely manner to the relevant agencies of coastal states or relevant international organizations is also crucial to reduce the risk of pirate attacks on ships, and effective reporting can lead to rescue by the relevant agencies in a timely manner, minimize the probability of a successful pirate attack, and help to reduce the possible losses due to attacks. Through cooperation and information sharing with these organizations, ships can receive assistance in strengthening their safety and security networks, thereby effectively reducing the risk of pirate attacks. In addition, such active communication can also promote synergistic defense between regions and build a stronger security line.

Therefore, in this paper, protective measures and hazard reporting are treated as parent nodes of protective factors.

3.4. Piracy Factor

The risk of piracy on ships is mainly reflected in the impact of protective measures on ships. When the number of pirates is large, even if the ship has taken protective measures, it will arrange protective measures against pirates. The increase in the number of pirates means that the strength and scale of the attack will increase, which will lead to the ship's defense system being difficult to effectively respond to or enhance the possibility of successful attacks by pirates, thus increasing the risk of pirate attacks.

The advanced degree of the pirates' weaponry will also make the ship's protective measures more difficult. With the increase in the number of ways for pirates to obtain higher-end weapons, their attack capability has also been strengthened, making it more difficult for the ship's protective measures to resist the pirates' attack and raising the risk of the ship suffering from pirate attacks.

To this end, this paper takes the number of pirates and pirate weapons as the parent node of the ship's risk factors.

4. Modeling of Pirate Attacks

4.1. BN Models

In contrast to other risk assessment models, the BN allows a fundamental analysis of the relationship between different risk factors. Due to its structural flexibility and the engine for projecting probabilities, the network can also handle adding new nodes within the network [21].

The ground rules of a BN can be expressed as

$$P(A,B) = P(A) \times P(B|A) \tag{1}$$

where **P(A,B)** is denoted as the probability of event **A** and event **B** occurring at the same time, **P(A)** is denoted as the probability of event **A** occurring, and **P(B | A)** is denoted as the probability of event **B** occurring based on event **A** occurring. According to the symmetry law transformation, formula (1) can be rewritten as

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{2}$$

The meaning of **P(A | B)** is then the posterior probability of **A** if the probability of **B** occurring is certain. The BN model is a one-quadratic group (S, Θ) defined on the set of variables $\mathbf{A} = \{X_1, X_2, \ldots\ldots, X_n\}$, where S represents the directed acyclic graph of probabilistic dependencies between variables, and Θ represents the table of conditional probability distributions of nodes in the network. If a BN has **n** nodes $X_1, X_2, \ldots\ldots, X_n$ and each node is randomly independent, its joint probability distribution can be expressed as

$$P(X_1, \ldots\ldots, X_n) = \prod_{i=1}^{n} P(X_i|X_1, \ldots\ldots, X_n)P(X_n) \tag{3}$$

Simplifying the equation further, it can be expressed as

$$P(X_1, \ldots\ldots, X_n) = \prod_{i=1}^{n} P(X_i|X_{i+1}, X_{i+2}, \ldots\ldots, X_n) = \prod_{i=1}^{n} P\left(X_i \middle| X_{P(a_i)}\right) \tag{4}$$

where $X_{P(a_i)}$ is the parent node of X_i. Based on these formulas, a BN model can be built. The construction process of this model mainly includes data processing, variable identification, initial structure learning, network parameter learning, sensitivity analysis, and model validation [22].

4.2. Data Processing

By collecting and organizing the data on pirate attacks on ships in Southeast Asian waters from the IMO GISIS database from 2013 to 2022, the statistical chart shown in Figure 3 was obtained. Analyzing Figure 3, the Southeast Asian Sea area was the hardest hit by pirate attacks in 2015, with a proportion of 71%. Although the proportion declined in the following years, from 2020, the pirate attacks in Southeast Asian seas again showed an upward trend, and the proportion of pirate attacks that occurred in the last two years was more than half of the global. Therefore, this paper selected the piracy attacks in Southeast Asian waters as the research object to study the key factors affecting the piracy attacks in the region. After cleaning, filtering, and sorting the relevant data in the IMO GISIS database, a Southeast Asian piracy attack dataset containing 1126 incidents was constructed for training and analyzing the BN model in the subsequent sections.

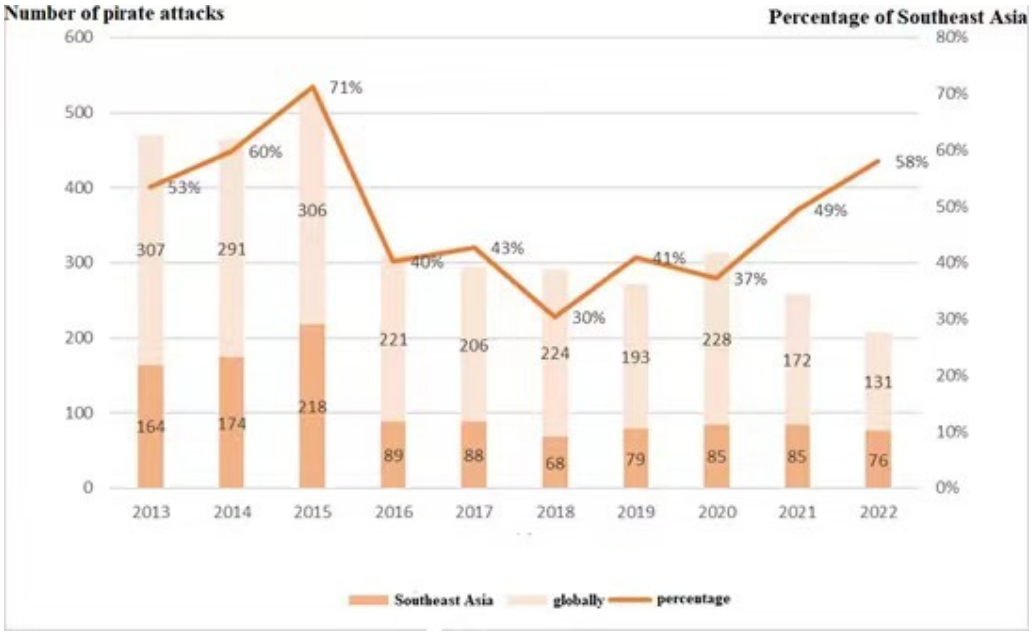


Figure 3. Statistics on piracy attacks in Southeast Asia, 2013–2022.

4.3. Variable Identification

Before constructing the model, the variables and influencing factors of the model need to be identified. Based on the above study, 13 essential factors were identified as contributing to pirate attacks. The different states of these variables can be categorized based on rational division. The model parameter training algorithm must deal with discrete values in the identification process, so the sample data should be discretized. The state description of each node data point and the value of discretization are shown in Table 3:

Table 3. State description and discretization of the data for each node.

Variable	State	Variable	State	Variable	State
Ship type (A1)	Status 1: high freeboard ship Status 2: medium freeboard ship Status 3: low freeboard ship	Ship status (A2)	Status 1: International waters State 2: Territorial sea State 3: Port	Time (A3)	State 1: During the day State 2: Night
Monsoon period (A4)	State 1: Yes State 2: No	Protective measures (A5)	State 1: Have State 2: No	Report (A6)	State 1: Yes State 2: No
Number of pirates (A7)	Status of 1: <5 persons Status of 2: 5 people	Pirate armament (A8)	State 1: Gun State 2: Other	Ship's own risk (B1)	State 1: Good State 2: Bad
External environment (B2)	State 1: Good State 2: Bad	Protection (B3)	State 1: Good State 2: Bad	Pirate factor (B4)	Status 1: High-risk Status 2: Low-risk
Ship being hijacked (C)	Status 1: Occurrence Status 2: Non-occurrence				

The ship piracy attack risk node represents the probability of a ship being successfully targeted by pirates. This risk encompasses potential property or personnel losses. Additionally, it includes the possibility of crew and ship hijacking, as well as the theft or robbery of the ship's property. All these scenarios are part of the overall risk of a piracy attack occurring. Therefore, this paper categorizes ship hijacking into two states: "occurrence" and "non-occurrence". "Occurrence" indicates that the ship has been successfully attacked

by pirates and has caused damage to the ship. "Non-occurrence" means that the pirate attack was unsuccessful and did not cause damage to the ship.

4.4. Initial Structure Learning

The risk factors of pirate attacks on ships were analyzed in detail through four aspects: the ship itself, the external environment, protective measures, and pirate actions. The influencing factors in Section 3 were converted into BN nodes. The BN nodes of the ship piracy attack risk were determined as 8 root nodes, 4 intermediate nodes, and 1 target node. The BN topology was constructed based on the network nodes identified above, as shown in Figure 4. In this network, the 8 root nodes representing the original causes were ship type, ship status, time, monsoon zone, protective measures, reporting, number of pirates, and pirate weaponry. The target node representing the result was the risk of a pirate attack. The four intermediate nodes connecting the root and target nodes were the ship's risk, external environmental conditions, protection, and pirate factors.

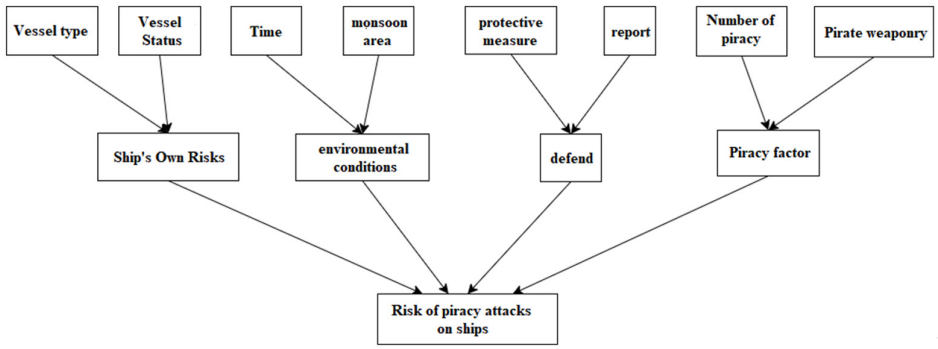


Figure 4. Constructing the BN topology.

4.5. Learning of Network Parameters

After determining the BN structure of the risk of ship piracy attacks, it is also necessary to clarify the interrelationship between each node and determine the BN node conditional probability. This paper uses the learning sample data method to obtain each node's conditional probability distribution due to the problem of missing data in the IMO GISIS database for reporting pirate attacks. EM algorithms are used in many fields, including machine learning, pattern recognition, information retrieval, and financial risk assessment. In constructing BNs, the EM algorithm is commonly used for parameter learning, especially when missing values are in the data. Thus, the EM algorithm is used for parameter training.

The EM algorithm, an iterative parameter estimation method, is used in statistics for the great likelihood estimation of the parameters of probabilistic models containing hidden variables. The EM algorithm is particularly suitable for datasets in the presence of unobserved data or hidden variables and maximizes the likelihood function of the data through an iterative process. It consists of two main steps: the expectation E step and the maximization M step. These two steps alternate until convergence as follows:

Step 1:

Expectation Step E: This step does not involve updating the parameters but rather calculating the posterior probability distribution of the hidden variables given the current parameters. Given the observed data $\boldsymbol{X}$ and the current parameters, the expectation of the log-likelihood function for the complete data $\boldsymbol{Z} = (\boldsymbol{X}, \boldsymbol{Y})$ is calculated. The formula can be expressed as

$$\boldsymbol{Q}\left(\boldsymbol{\theta}, \boldsymbol{\theta}^{\boldsymbol{i-1}}\right) = \boldsymbol{E}\left[\log \boldsymbol{p}(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{\theta}) \middle| \boldsymbol{X}, \boldsymbol{\theta}^{\boldsymbol{i-1}}\right] \tag{5}$$

where $\boldsymbol{Q}\left(\boldsymbol{\theta}, \boldsymbol{\theta}^{\boldsymbol{i-1}}\right)$ is the expected posterior function in the EM algorithm, $\boldsymbol{\theta}^{\boldsymbol{i-1}}$ is a known estimate of the current parameter, $\boldsymbol{E}$ is the expectation operator, and $\log \boldsymbol{p}(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{\theta})$ is the log-likelihood function, which represents the logarithm of the joint probability of the observed

data $\boldsymbol{X}$ and the latent data $\boldsymbol{Y}$ under the condition of the parameter $\boldsymbol{\theta}$. $\boldsymbol{\theta}$ represents the model parameters

Step 2:

Maximization M step: Using the information obtained in the E step, the model parameters are adjusted to maximize the likelihood function of the observed data. This step usually involves optimizing the likelihood function to find the best parameter values. Maximizing the expectation $\boldsymbol{Q\left(\theta, \theta^{i-1}\right)}$ requires choosing a parameter to satisfy the condition:

$$\boldsymbol{\theta^{i}} \textbf{arg}\ \underset{\boldsymbol{\theta}}{\boldsymbol{max}}\ \boldsymbol{Q\left(\theta, \theta^{i-1}\right)} \tag{6}$$

where $\textbf{arg}\ \underset{\boldsymbol{\theta}}{\textbf{max}}\ \boldsymbol{Q\left(\theta, \theta^{i-1}\right)}$ is part of the M-step and represents the finding of the parameter $\boldsymbol{\theta}$ that maximizes the desired posterior function $\boldsymbol{Q\left(\theta, \theta^{i-1}\right)}$.

The iterative process of the EM algorithm is as follows:

- ✓ Start with a set of random parameter values.
- ✓ Perform step E to compute the expectation of the hidden variables.
- ✓ Perform step M to update the parameters to maximize the likelihood.
- ✓ Repeat the E-step and M-step until the amount of change in the parameters exceeds some predetermined threshold, indicating that the algorithm has converged.

5. Results Analysis

5.1. Results of Model Training

Netica software, Version 7.01, was applied to train the EM algorithm using Equations (5) and (6). The training results are shown in Figure 5. The significance of variables A1 through A8 and B1 through B4 can be ascertained from Table 3, with the conditions of each factor detailed therein. The probabilities associated with B1 through B4 are calculated based on the joint probabilities of the root nodes A1 with A2, A3 with A4, A5 with A6, and A7 with A8. The variable C, indicative of the likelihood of a ship hijacking, is derived from the prior probabilities of the root nodes B1 through B4. The probability of the ship being hijacked is 70.1%. When the prior probability of the network node variables changes, the likelihood of a successful attack changes accordingly.

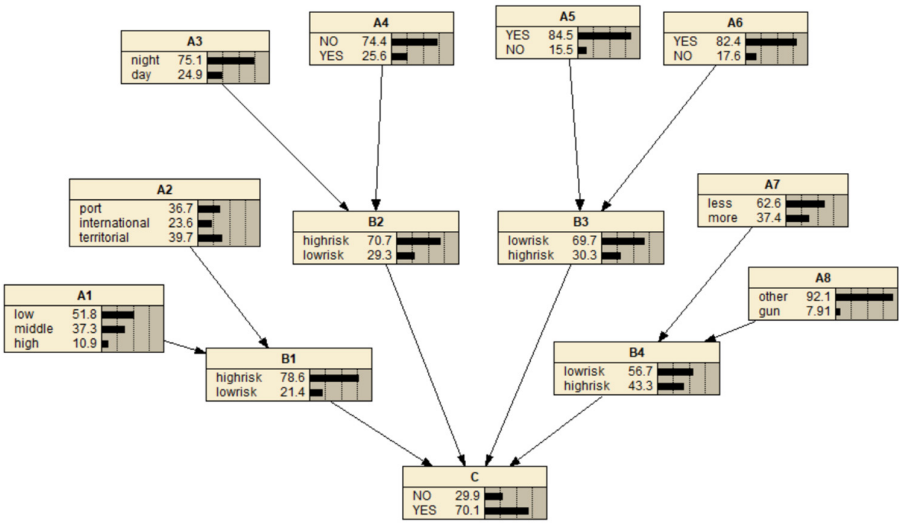


Figure 5. Model training results.

Diagnostic reasoning is a systematic approach to problem solving and decision making. In this paper, we utilized it to ascertain the primary factors influencing the risk of pirate attacks on maritime vessels in Southeast Asian waters. It involves the application of structured analysis to hypothesize potential risk factors, followed by rigorous testing and evaluation to confirm their effectiveness and correlation with the risk of maritime piracy. In

the BN constructed above for ship piracy attacks in Southeast Asian waters, the probability of the "occurrence" state of the piracy attacking risk node is set to 100%. The posterior probability of each root node is calculated according to the results of model training, as shown in Figure 6, and organized into tabular form, as shown in Table 4. The data are sorted as follows: Time = "Night" > Vessel dry side = "Low" > Number of pirates = "More than 5" > Vessel status = "Port".

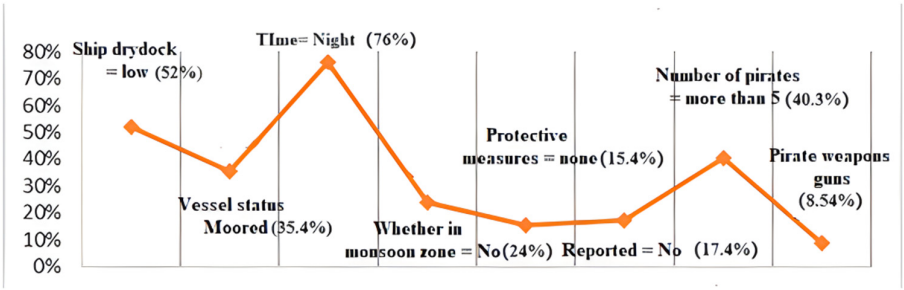


Figure 6. Posterior probability of each root node.

Table 4. Posterior probability of each root node.

Root Node	Posterior Probability
Ship drydock = low	52%
Vessel status = Moored	35.4%
Time = Night	76%
Whether in monsoon zone = No	24%
Protective measures = none	15.4%
Reported = No	17.4%
Number of pirates = more than 5	40.3%
Pirate weapons = guns	8.54%

When the risk of pirate attacks occurs, the most significant influencing factors are the time of day being in the dark, the ship's low dry-dock, the number of pirates being greater than five, and the status of the port being in a harbor. Ships sailing at night are more likely to be the target of pirates, which may be due to the low visibility at night, and the ship's alertness and defense ability are relatively weakened, providing pirates with better concealment and attack opportunities. An unprofitable external environment and high-risk ships can increase the likelihood of successful pirate attacks. Low-dry-docked ships are more vulnerable to pirate attacks because they may lack effective defense measures, such as anti-climbing devices, making it easier for pirates to board. The threat to ships increases significantly when the number of pirates exceeds five. This may be because when pirate groups are more prominent, they can control the ship and crew more effectively, increasing the attack's success. Ships anchored in ports are more vulnerable to pirates because they are slower, and their crews may let their guard down. An unfavorable external environment, such as rough sea conditions, may limit pirate movement and thus reduce the success of attacks.

The success rate of piracy attacks is most dependent on the external environment. Reporting in a relatively timely manner and failure to take protective measures have little impact on the occurrence of the risk of piracy attacks. Reporting in a timely manner and protective measures have a limited effect on reducing the risk of piracy attacks. This may be because, by the time a piracy attack occurs, these measures may no longer stop the attack. It is also possible to judge from this scenario that a low dry-docked ship traveling at night in a port area in Southeast Asian waters is more likely to experience the risk of a pirate attack when it encounters a pirate attack with more than five pirates. The International Maritime Organization reports that piracy in Southeast Asia is typically characterized by small-scale thefts from anchored vessels in territorial waters and port areas at night, which is consistent with the results of this paper.

5.2. Sensitivity Analysis and Model Validation

In BNs, sensitivity analysis refers to analyzing the impact of multiple causes on the outcome and the degree of influence. Sensitivity analysis is used to validate the constructed model by assessing the probability of the risk of ship piracy attacks in Southeast Asia. It can identify the relevant factors that significantly influence the risk of ship piracy attacks. This paper uses pushing up from the bottom to the top to carry out the sensitivity analysis; i.e., starting from the child node, the probability of occurrence of the child node is set to 100% and the change value of the probability of each parent node from the initial state is calculated. The larger the change value, the stronger the sensitivity of the node, and the greater its role in promoting the occurrence of the child node [23]. In the BN of the risk of ship piracy attacks in Southeast Asian waters, the target node of the ship piracy attacks risk node "occurrence" state is set to 100%, its change is observed, and it is sorted. The results are shown in Table 5.

Table 5. State sensitivity of the root nodes.

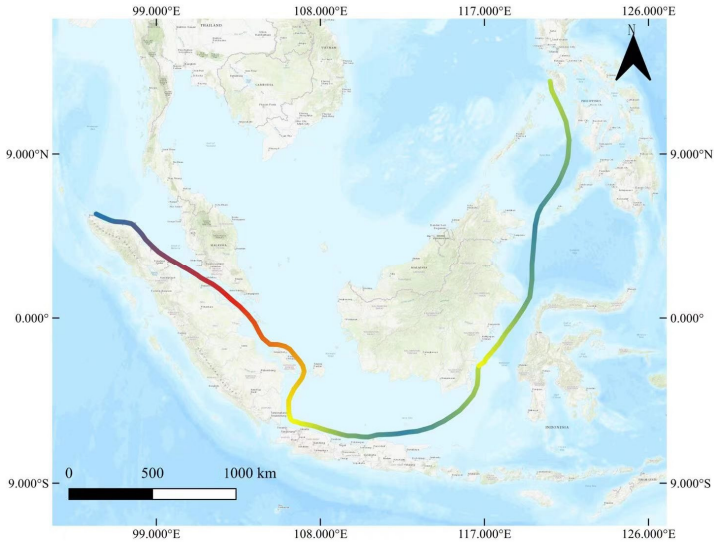
Node Settings	Difference in Sensitivity	Sensitivity Ranking
Starfboard of the ship = "low"	0.2%	6
Ship status = "Port"	1.3%	3
Time = "dark night"	0.9%	4
Is in monsoon = No	1.6%	2
Protection = "None"	0.1%	8
Reported = No	0.2%	6
Pirnumber = "greater than 5"	2.9%	1
Pirate weapon = "gun."	0.6%	5

According to Table 5, it can be found that the most influential factors in the occurrence of the risk of piracy attacks are the number of pirates greater than five, not being in the monsoon period, the time being in the dark, and the ship being in the harbor state. The high sensitivity difference of these factors indicates that they have a solid contribution to the occurrence of the risk of pirate attacks. The factors of the pirate use of force as a weapon, low dry-docking vessels, failure to report, and protective measures have lower sensitivity differences and are all in the bottom half of the rankings, suggesting that these factors have less of an impact on the risk of pirate attacks relative to the other factors. The four most significant influencing factors are analyzed below.

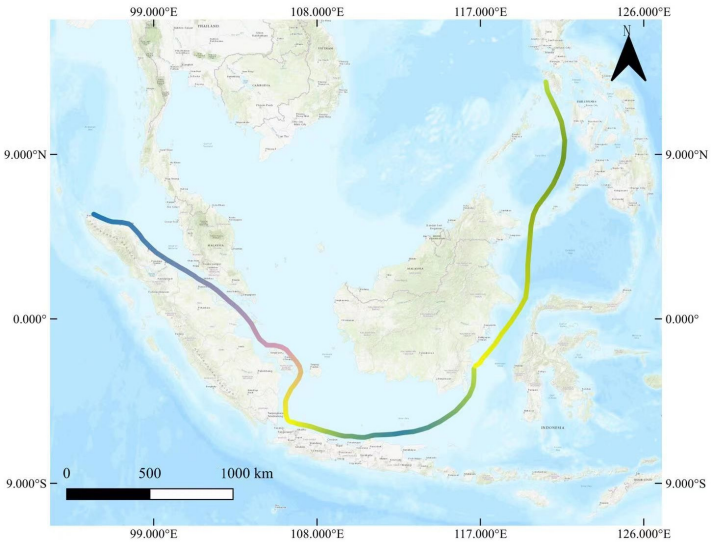
6. Discussion

To further investigate the influencing factors of pirate attacks, a specific analysis will be conducted on the circumstances of pirate attacks in 2023. Figure 7a,b depict the distribution of pirate attacks in Southeast Asia for the months of January to March and June to August 2023, respectively. The route is roughly divided into three stages. The line segment in the figure shows the departure from Singapore, crossing the Strait of Malacca as the first stage, arriving at Indonesia from the Strait of Malacca as the second stage, and finally arriving at the Philippines as the third stage, which is roughly divided into three stages, where the red line segment indicates the highest number of pirate attacks in the region, which is more than five; the yellow line segment is the next largest, which represents 4–5 times; the blue represents 2–3 times; and the green represents 0–1 times. Figure 7 illustrates that from January to March, within the region stretching from Singapore to the Malacca Strait, the frequency of pirate attacks intensifies as the maritime routes approach the strait, reaching its zenith at the strait, which is the epicenter of pirate attacks in Southeast Asia. After the strait, as one navigates towards the Philippines, the high seas remain devoid of pirate incidents; however, the coastal regions occasionally witness pirate encounters, though with a comparatively infrequent occurrence. Transitioning to the period between June and August, there is a significant decline in the occurrences of pirate attacks in contrast to the

preceding months, yet the Malacca Strait remains an area that is particularly susceptible to a higher prevalence of piracy.



(**a**)



(**b**)

Figure 7. (**a**) Distribution of piracy attacks in Southeast Asia from January to March 2023, (**b**) distribution of piracy attacks in Southeast Asia from June to August 2023.

From Figure 7a,b, in Singapore waters, January to March is in the non-monsoon zone, while the weather in the non-monsoon zone is relatively stable, with less wind and waves and high visibility, which is conducive to the navigation of pirate vessels and approaching the target ship. Thus, the risk of pirate attacks is high compared to the monsoon zone period from June to August, when the rainy season period brought about by the monsoon will be environmentally harsh, and the pirate activities become problematic, resulting in a substantially lower risk of attack than in March. On the other hand, Malaysia has no seasons throughout the year, due to the influence of the Northern Hemisphere monsoon in the north and the Southern Hemisphere monsoon in the south, resulting in a stable situation of pirate attacks. As such, it can be concluded that the risk of pirate attacks is higher when the environment is favorable and decreases as the environmental conditions

change. Based on the analysis, it can be concluded that the average risk of pirate attacks is lowest in the second half of the year and highest in the first half.

In addition to the influence of the monsoon factor, many other dynamic factors can affect the risk of a ship being attacked by pirates. Table 6 compiles incidents of pirate attacks on ships sailing in Southeast Asia from January to March 2024 in the IMO database.

Table 6. Pirate attacks in Southeast Asia from January to March 2024.

Time	Ship Type	Ship State	Pirate Number	Pirate Weapons
3 January 2024—22:00 UTC	bulk-cargo ship	anchor	Five people	cane knife
9 January 2024—18:30 UTC	bulk-cargo ship	navigation	Five people	cane knife
30 January 2024—20:00 UTC	bulk-cargo ship	anchor	Six people	firearms
19 February 2024—21:00 UTC	bulk-cargo ship	anchor	Two people	cane knife
19 February 2024—19:10 UTC	Ordinary cargo ship	navigation	Five people	firearms
3 March 2024—18:50 UTC	bulk-cargo ship	anchor	Two people	do not have
4 March 2024—18:10 UTC	bulk-cargo ship	anchor	Three people	firearms
5 March 2024—16:30 UTC	bulk-cargo ship	anchor	Five people	firearms
29 March 2024—19:58 UTC	bulk-cargo ship	navigation	Three people	knife

As can be seen from Table 6, in the piracy attacks in Southeast Asia, the time of occurrence is generally at night, when it is dark; the low visibility at night provides cover for the pirates, coupled with the fact that the night is the crew's rest time, the activities onboard are reduced, and the crew's alertness is lowered, which makes it easier for them to approach the ship without being detected. As a result of the increased difficulty in monitoring and the reduced alertness of the crew at night, once pirates are detected, the response time of the ship may be shortened, reducing the opportunity to take effective defensive measures, so the time factor is one of the important factors affecting pirate attacks. In addition, the attacked ships are generally bulk carriers. On the one hand, because the Southeast Asian region is the main transportation area of coal, encouragement, and other bulk cargo, the main transportation ships are bulk carriers. On the other hand, it is because the dry side of bulk carriers is lower than those of passenger ships and cruise ships, which makes them more vulnerable to landing by pirates. Therefore, the ship's risk factors also affect the occurrence of pirate attacks on ships. In a ship in distress, most of the ship is in the port state. Because the port area is vast, monitoring facilities may not be able to cover it thoroughly, and the pirates can use the monitoring of the blind spot to approach. In the ship's port, it is usually slower or in the mooring state. Reducing the pirates' need to catch up with the pirates' speed can make the ship's approach and boarding easy. In regions with a high incidence of piracy, factors such as the number of pirates and the level of pirate capacity, such as the weapons used, may also affect the risk of a ship being attacked by pirates. When the number of pirates is small, for example, one or two, and when they are unarmed or use only simple tools, the risk of a pirate attack is significantly reduced because the system is resilient. However, the risk increases if the number of pirates exceeds five and they use sophisticated weapons and equipment.

For the piracy attacks on Southeast Asian ships, Jiang [12] and others also used the BN model to study the impact factors of piracy attacks. In his study of the model, including the ship, the environment, and anti-piracy measures, there are many factors affecting piracy attacks on Southeast Asian ships, so in this paper, based on the above-influencing factors, the impact of pirate factors, the number of pirates, and the weapons used by the pirates are important factors affecting the pirate attacks. In the prediction result of the BN model established in the end, Jiang et al. predicted that the probability of the ship being attacked and hijacked is 1.95%. However, the prediction result of the model established in this paper is 70.1%.

In the risk assessment of pirate attacks, when pirate groups are large and equipped with advanced equipment, their ability to hijack ships is significantly higher, which increases the risk of maritime transportation. However, Jiang et al.'s study failed to fully

consider the impact of pirate capability level on the success rate of attacks, which may have led to their prediction results underestimating the actual risk to a certain extent. To compensate for this shortcoming, this paper provides a more accurate analysis of pirate attacks by constructing a BN model. The model not only considers the number of pirates and their equipment but also integrates a variety of other influencing factors to build a more comprehensive and detailed risk assessment model. The predictive results of the model in this paper provide a deeper understanding of the behavioral patterns and development trends of pirate attacks, as well as identifying the key factors influencing the risk of pirate attacks. Such an analysis provides a solid theoretical basis and detailed data support for shipping companies and relevant maritime organizations in formulating effective measures to prevent pirate attacks. In addition, the model can help decision makers make more scientific and rational decisions in resource allocation, route planning, and emergency response strategy development, thus improving the overall level of maritime security, safeguarding the safety of ships and crews, and reducing the potential impact of pirate attacks on international trade and the global economy.

By analyzing the prediction results, this paper provides some improvement suggestions for China's shipping policy, as follows:

Enhanced technology and surveillance systems: The early identification and surveillance of piracy can be improved through the deployment of advanced surveillance technologies, such as drones and satellite technology. These technologies can provide real-time images and location data in Southeast Asian waters. In addition, installing automatic identification systems (AISs) and other electronic surveillance equipment, such as radar and sonar systems onboard ships, enhances the visibility of ships in poor weather conditions and improves surveillance capabilities at night. The integrated use of these technologies can significantly improve surveillance centers' tracking and response speed to suspected pirate ships, thus enabling effective intervention at the onset of piracy.

Improving emergency response and coordination: Establishing rapid response teams and strengthening the role of the International Maritime Organization are key to improving emergency response and regional coordination. Rapid response teams should comprise multinational naval forces specially trained to respond to pirate attacks, and these teams can be deployed quickly in the early stages of a pirate attack, significantly reducing the likelihood of a successful attack. At the same time, the International Maritime Organization can assume a central role in coordinating international anti-piracy efforts by establishing a dedicated surveillance and response center to achieve the centralized management and sharing of information on piracy activities and to promote real-time communication and strategic deployment among member states.

Measures at the economic and social levels: Economic hardship is an important factor driving piracy. By promoting regional economic development and providing more employment opportunities and economic support, the incentives for people to join pirates can be effectively reduced. In addition, reducing the emergence of piracy can be achieved by raising social awareness of the impact of piracy through education and public outreach, emphasizing its destructive effects on international trade and regional security. Such a comprehensive strategy at the social and economic levels will help to radically reduce piracy while protecting the safety of ships and crews and promoting regional peace and stability.

7. Conclusions

Based on the research of scholars, domestic and international, this paper provides an in-depth analysis of the risk of pirate attacks on ships in Southeast Asian waters by constructing a BN model and using EM algorithms to train the model parameters using the Global Ship Piracy Attack Report in the IMO GISIS database for the period from 2013 to 2022. Through the training of the BN model and sensitivity analysis study, it is found that the number of pirates, whether it is in the monsoon period or not, the period of sailing (day or night), and the state of the ship in the port are the main factors affecting the risk of pirate attacks. Based on this study's results, this paper proposes targeted

policy recommendations, including voyage monitoring, cooperation and coordination, and the development of emergency response plans, to reduce the risk of pirate attacks in Southeast Asia and improve the safety of ships. Considering the findings and to further the scope of this research, we suggest future work to include an expansion of the BN model to incorporate additional variables that may impact pirate attack risk. Additionally, we recommend exploring the integration of real-time data feeds to enhance the predictive capabilities of the model. The continuous monitoring and assessment of the pirates' attack risk factors will also be essential to adapt to the evolving nature of maritime security threats.

Author Contributions: Conceptualization, Q.C. and J.G.; methodology, J.Z.; software, Q.C.; validation, J.G., J.Z. and Y.-Y.L.; formal analysis, J.L.; investigation, M.C.-P.P.; resources, P.Z.; data curation, Q.C.; writing—original draft preparation, J.Z.; writing—review and editing, J.G.; visualization, Q.C.; supervision, Y.-Y.L.; project administration, M.C.-P.P.; funding acquisition, P.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by [Xiamen Society Scientific Research [2023]] grant number [No. C08], [research on the path of high-quality development of higher education reform in Fujian enabled by green shipping] grant number [FGJY202315] and [the National Social Science Fund of China] grant number [23&ZD138].

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Dataset available on request from the authors.

Acknowledgments: This achievement is a general project of higher education reform and research of the Fujian Higher Education Research Institute (research on the path of high-quality development of higher education reform in Fujian enabled by green shipping + FGJY202315), and research on Building a New Highland for Marine Scientific Research and Innovation in Xiamen (Xiamen Society Scientific Research [2023] No. C08). This work is supported by a project granted by the National Social Science Fund of China (23&ZD138).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Baksh, A.-A.; Abbassi, R.; Garaniya, V.; Khan, F. Marine transportation risk assessment using Bayesian Network: Application to Arctic waters. *Ocean Eng.* **2018**, *159*, 422–436. [CrossRef]
2. Fan, H.; Lu, J.; Chang, Z. A risk-based game theory model of navy and pirate behaviors. *Ocean Coast. Manag.* **2022**, *225*, 106200. [CrossRef]
3. Fan, S.; Yang, Z.; Blanco-Davis, E.; Zhang, J.; Yan, X. Analysis of maritime transport accidents using Bayesian networks. *Proc. Inst. Mech. Eng. Part O J. Risk Reliab.* **2020**, *234*, 439–454. [CrossRef]
4. Hossain, N.U.I.; Nur, F.; Hosseini, S.; Jaradat, R.; Marufuzzaman, M.; Puryear, S.M. A Bayesian network-based approach for modeling and assessing resilience: A case study of a full-service deep-water port. *Reliab. Eng. Syst. Saf.* **2019**, *189*, 378–396. [CrossRef]
5. Wang, L.; Yang, Z. Bayesian network modelling and analysis of accident severity in waterborne transportation: A case study in China. *Reliab. Eng. Syst. Saf.* **2018**, *180*, 277–289. [CrossRef]
6. Psarros, G.A.; Christiansen, A.F.; Skjong, R.; Gravir, G. On the Success Rates of Maritime Piracy Attacks. *J. Transp. Secur.* **2011**, *4*, 309–335. [CrossRef]
7. Pristrom, S.; Li, K.X.; Yang, Z.; Wang, J. A Study of Maritime Security and Piracy. *Marit. Policy Manag.* **2013**, *40*, 675–693. [CrossRef]
8. Li, H.; Yang, Z. Towards safe navigation environment: The imminent role of patio-temporal pattern mining in maritime piracy incidents analysis. *Reliab. Eng. Syst. Saf.* **2023**, *238*, 109422. [CrossRef]
9. Vaněk, O.; Jakob, M.; Hrstka, O.; Pěchouček, M. Agent Based Model of Maritime Traffic in Piracy-Affected Waters. *Transp. Res. Part C Emerg. Technol.* **2013**, *36*, 157–176. [CrossRef]
10. He, Z.; Wang, C.; Gao, J.; Xie, Y. Assessment of global shipping risk caused by maritime piracy. *Heliyon* **2023**, *9*, e20988. [CrossRef]
11. Bouejla, A.; Chaze, X.; Guarnieri, F.; Napoli, A. A Bayesian network to manage risks of maritime piracy against offshore oil fields. *Saf. Sci.* **2014**, *68*, 222–230. [CrossRef]
12. Jiang, M.; Lu, J. The analysis of maritime piracy occurred in Southeast Asia by using Bayesian network. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *139*, 101965. [CrossRef]

13. Hu, X.; Xia, H.; Xuan, S.; Hu, S. Exploring the Pirate Attack Process Risk along the Maritime Silk Road via Dynamic Bayesian Network Analysis. *Mar. Sci. Eng.* **2023**, *11*, 1430. [CrossRef]
14. Fan, H.; Chang, Z.; Jia, H.; He, X.; Lyu, J. How do navy escorts influence piracy risk in East Africa A Bayesian network approach. *Risk Anal.* **2024**, 1–21. [CrossRef] [PubMed]
15. Kefeng, L.; Lizhi, Y.; Ming, L. Application of Cloud Model and Bayesian Network to Piracy Risk Assessment. *Math. Probl. Eng.* **2021**, *2021*, 6610339.
16. Pristrom, S.; Yang, Z.; Wang, J.; Yan, X. A novel flexible model for piracy and robbery assessment of merchant ship operations. *Reliab. Eng. Syst. Saf.* **2016**, *155*, 196–211. [CrossRef]
17. Fan, H.; Lyu, J.; Chang, Z.; He, X.; Guo, S. Spatial patterns and characteristics of global piracy analyzed using a geographic information system. *Mar. Policy* **2023**, *157*, 105816. [CrossRef]
18. Dempster, A.P.; Laird, N.M.; Rubin, D.B. Maximum likelihood from incomplete data via the EM algorithm. *J. R. Stat. Soc. Ser. B Methodol.* **1977**, *39*, 1–22. [CrossRef]
19. Gong, X.X.; Lu, J. Strait/canal security assessment of the Maritime Silk Road. *Int. J. Shipp. Transp. Logist.* **2018**, *10*, 281–298. [CrossRef]
20. Chen, C. Exploring how to do a good job in the maintenance and upkeep of ship machinery and equipment. *Mod. Manuf. Technol. Equip.* **2020**, *4*, 204–208.
21. Cao, Y.; Wang, X.; Wang, Y.; Fan, S.; Wang, H.; Yang, Z.; Liu, Z.; Wang, J.; Shi, R. analysis of factors affecting the severity of marine accidents using a data-driven Bayesian network. *Ocean Eng.* **2023**, *269*, 113563. [CrossRef]
22. Chang, Z.; He, X.; Fan, H.; Guan, W.; He, L. Leverage Bayesian Network and Fault Tree Method on Risk Assessment of LNG Maritime Transport Shipping Routes: Application to the China–Australia Route. *J. Mar. Sci. Eng.* **2023**, *11*, 1722. [CrossRef]
23. Wang, Z.; Zhang, R.; Ge, S.; Ju, Y.; Cao, Z. Natural Environmental Risk Zoning of the Arctic Northeast Passage: Taking the Northern Sea Area of Russia as an Example. *Ocean Eng.* **2017**, *35*, 61–70.