Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 6610339, 14 pages
https://doi.org/10.1155/2021/6610339

Research Article

Application of Cloud Model and Bayesian Network to Piracy Risk Assessment

Kefeng Liu,[1] Lizhi Yang,[2] and Ming Li[1]

[1] *College of Meteorology and Oceanography, National University of Defense Technology, Nanjing 211101, China*
[2] *Unit 78127, Chengdu 610000, China*

Correspondence should be addressed to Ming Li; mingli152@163.com

Received 26 November 2020; Revised 28 December 2020; Accepted 17 January 2021; Published 5 February 2021

Academic Editor: Jian Shi

Piracy is a major threat to maritime safety. Assessing piracy risk is crucial to ship safety, travel security, and emergency plan preparation. In the absence of a thorough understanding of the factors and mechanisms that influence piracy, no perfect mathematical equation can be set up for such risk assessment. Therefore, the major factors that influence piracy were identified to construct an indicator system for assessment. These factors were analyzed, keeping in view the overall hazard, vulnerability, and antirisk properties, and then the Bayesian network was introduced into the risk assessment model to fuse multiresource information. For some indicators, which have only qualitative information or fragmentary statistical data, the cloud model theory was adopted to realize prior probability settings of the Bayesian network and thus made up for the deficiency in parameter settings. Finally, the inherent hazard of the South China Sea was assessed, as an example for the model, and two real piracy cases were studied to validate the proposed model. The assessment model constructed here can be applied to all cases, similar to the ones studied here.

1. Introduction

Maritime piracy is a problem of international concern, which poses human, economic, and environmental threats. The core international channel continues to be the most vulnerable high-risk region for long. According to the statistics of the International Maritime Organization (IMO), many counterpiracy missions have been launched since 2008, but piracy continues unabated. Moreover, with continual international strikes on Somalia, piracy activities have been tending to shift to the Arabian Sea and the Guinea Sea.

Piracy, a major threat to maritime safety, has become a hotspot in international academia. Many qualitative researches have been carried out since the early days to study piracy, such as exploring antipiracy means with a focus on laws and policies [1–4]. Later, the concept of mathematical modeling has also been brought in to study piracy. For instance, game theory [5, 6] and intuitionist fuzzy set [7] have been utilized to suggest transport routes that can avoid maritime pirates or to optimize counterpiracy patrolling strategies. Besides, maritime piracy situation has been modeled by several methods, such as dynamic Bayesian network [8]. Bouejla et al [9, 10] and Chaze [11] have applied Bayesian network and SARGOS system for modeling response decision and risk management systems for countering piracy attacks. Furthermore, risk assessments of maritime piracy have been carried out to assist ship owners and captains in managing risk during pirate attacks [12, 13].

To summarize, the Bayesian network, by virtue of the advantage it offers in directly extracting information from complicated networks, has been widely used in the research of piracy. However, it has not been applied so far to piracy risk assessment. What is more, the focus of current research on piracy risk assessment has so far been only on hazards of piracy, without paying due attention to vulnerability and antirisk properties. Furthermore, most of the existing researches are based merely on the qualitative analysis or simple probability statistics.

As travel security and emergency plan are fundamental requirements to maritime safety, antipiracy studies will have to focus on quantitative risk assessment [14, 15]. So, the focus of this study has been on constructing a quantitative risk assessment framework for piracy, using Bayesian network and taking into account the overall hazard, vulnerability, and antirisk property. In fact, piracy risk assessment necessarily requires fusion of information from multiple sources, such as data statistics, expert knowledge, and qualitative textual messages. Bayesian network is considered the best mathematical tool for such fusion [16–18]. But, when setting the prior probability of some nodes using textual messages, expert knowledge, and fragmentary statistical data, no proper means is available to overcome aporia. The existing methods, such as Expectation Maximization algorithm and Gibbs algorithm, concentrate on conditional probability setting, ignoring the improvement in accuracy of prior probability setting. The expanded Bayesian model (Qualitative Bayesian Network) can very well be applied to knowledge-expression and data-mining problems, but it gives only a quantitative result.

Thus, for the leaf-nodes with expert knowledge, qualitative message, and fragmentary statistical data, the right choice to obtain their probability distribution is to explore the means for expressing the linguistic concept and extracting the distribution. However, this issue has not been mentioned by any of the previous researchers. Therefore, this study will introduce the cloud model theory to deal with context-based information expression and to optimize prior probability settings of the Bayesian network, based on which the quantitative assessment framework for piracy risk can be established. The outcome of this exercise would help the decision-makers in arriving at more intuitive and objective decisions. The optimized Bayesian network can also help in quantitative risk assessment of similar problems.

The remainder of the paper is organized as follows: Section 2 analyzes the major factors that influence the risk of piracy; Section 3 presents the risk assessment model, together with its major theory; Section 4 deals with the experiment on piracy risk assessment, based on historical data and scenario simulation; and Section 5 presents the conclusions of this study, followed by proposals for future work.

2. Theory of Piracy Risk

The definition of risk has not reached into a unified definition, so as the components of risk. Some researchers represent risk as the combination of three components: hazard (the possibility that the triggering event takes place), vulnerability (a particular condition or state of a system before the triggering event takes place), and consequence (potential losses) [19, 20], whereas some researchers represent risk as the combination of hazard, vulnerability, and antirisk property (the ability of the system or the exterior to resist the risk, it is also called coping capacities) [21, 22].

This paper accepts the latter components referred to in the last paragraph; that is, the risk consisted of hazard, vulnerability, and antirisk property. Therefore, the risk system of piracy can be deemed as a combination of the hazards of pirate, vulnerability of the attacked ship, and antirisk property of both the ships and the escort force on the sea. That is, when the attacked object confronts risk factors, its exposure and sensitivity to these factors will inflict loss on it, the magnitude of which depends on the intensity of risk factors, duration of exposure, and degree of sensitivity. Generally, the greater the magnitude (size and degree) of the risk factors is, the more the risk would be. However, the antirisk property of the boat and the resistance of the escort force will, to some extent, decrease the risk.

2.1. Analysis of Piracy Hazard. IMO reports provide the details of every pirate attack. According to these reports, pirates generally get away by taking some goods and materials from ships, just as thieves and robbers do. Sometimes, they also injure the workers on ships, or, less frequently, even kidnap them. The hazard of piracy comes from both the probability of being attacked by pirates and the severity of their attacks. Generally, the greater the probability (severity) of the attack is, the higher the hazard would be.

The probability of a ship attack can be assessed from several factors.

2.1.1. Historical Records of Piracy Attacks. The record of piracy attacks on the research area in recent years would be of significant help in assessing the probability of a ship being attacked. The more the recorded instances of attack are, the greater the probability of piracy would be.

2.1.2. Economic Situation of Circumjacent Countries. Generally speaking, when the economic conditions of a country deteriorate to the extent of impoverishing the people, then the people of that country tend to migrate to any of the surrounding countries, where the conditions are favorable. An excellent example in this regard is the emergence of Somali pirates. So, the worse the economic situation of a country is, the greater the risk of piracy in the circumjacent countries would be.

2.1.3. Political Situation of Circumjacent Countries. If the political situation of a country becomes turbulent, then the national mood will be instability, which leads to an increase in the number of domestic conflicts. As a consequence, the countrymen, who are badly affected by such conflicts, would tend to join some criminal organization or the other. Besides, political instability in a country can lead to deterioration of economic conditions, which, in turn, will lead to an increase in the number of refugees in the circumjacent countries and thus to the increase in the number of pirates.

2.1.4. Weather Conditions. Pirates are known to avoid hostile weather conditions, such as monsoon seasons, high winds, high waves, and strong ocean currents [23]. For example, more than 50% of pirates' attacks occurred during springtime, when the weather is favorable with mild winds, gentle waves, and good visibility. Therefore, the more favorable the weather conditions are, the greater the probability of piracy would be.

2.1.5. Geographical Conditions. The natural geographic setting of an area forms an important factor in defining the vulnerability of that area for piracy. Intricate geographical conditions provide an ideal hideout for pirates. For instance, the Indonesian Sea, which is popularly referred to as "thousand island country," is considered one of the most vulnerable sites for piracy in the South Sea. Generally, the more intricate the geographical setting is, the greater the probability of piracy would be.

Furthermore, the hazard of piracy in any area can be assessed by the historical account of the severity of the attacks in that area. Generally, the pirate gangs hang out in the same chosen area. If the historical accounts of piracy are events of mere thefts with no involvement of weapons, then it implies that the pirates in that area pose no serious threat and can, therefore, be easily dealt with. According to IMO reports, the severity of piracy in any area can be judged from two factors.

2.1.6. Number of Pirates. The statistical study of IMO reports shows that the more the number of pirates is, the higher their success rate would be. The annual IMO reports generally record the number of pirates involved in an attack into three categories, 1–4, 5–10, and more than 10, with risk level increasing in that order.

2.1.7. Weaponry of Pirates. IMO reports record the weapons used by pirates in the attack into four categories: none, knife, long knife, and gun. According to the reports, when the pirates attack without weapons, they tend to just steal a few goods and materials, and thus their success rate tends to be low; on the contrary, when they are armed with good weapons, they pose a serious threat to the safety of ship's crew, and thus their success rates tend to be high. Therefore, the more sophisticated the pirates' weapons are, the greater the threat to the ships would be and consequently the higher the hazard would be.

2.2. Analysis of Vulnerability of Attacked Objects. The vulnerability of attacked object is the inner property of that object, which renders it amenable to hazards. The propensity of being affected by a stimulus depends on both exposure and sensitivity of a system, where exposure is the condition of being subjected to detrimental effect; it thus reflects the biophysical nature of the stimulus, characteristic of the location, and nature of the system. Sensitivity refers to the degree to which a system responds to, or is affected by, a stimulus and is related to the characteristics of the system and to broader nonclimatic factors (e.g., land use, livelihood, infrastructure, and government policy) [24].

The pirates cause loss of goods and materials to the ships by dishonest means and, sometimes, even by endangering the safety of the ship's crew. Thus, the main targets of pirates' attacks are the goods and the crew, especially the goods. In piracy, the intensity of exposure depends on the value of the goods and the number of crew. The higher the goods' value is or the greater the crew number is, the greater the exposure would be and, consequently, the higher the risk would be. And, the main sensitivity of the ship, subjected to piracy, is the degree of domestic need for the goods on the ship, that is, the degree of dependency of that country on external supplies for those goods. If the dependency is very high, then domestic demand for the goods will be very high. So when the goods are lost, what matters is not their cost, but their nonavailability when needed, and hence the risk consequent to the loss will be high.

2.3. Analysis of Antirisk Property of the System. The antirisk property of the attacked object is the strength of that object to resist risk and to combat the pirates, and such strength comes from within the attacked object and the external system.

2.3.1. Escort Force. The strength of the escort force has a significant influence on piracy, especially because it can serve to frighten the small pirate groups. At present, the prevention of piracy has become a matter of international concern. The actions so far taken by the escort force and regional defense forces and those taken with international cooperation have given remarkable results, as reflected by the sharp decrease in the number of piracies.

2.3.2. Communication Facilities and Self-Defense Equipment of Ships. Once piracy occurs or about to occur, the attacked or about-to-be attacked ship sends a wireless message to the nearest information center. On receiving the message, the concerned authorities will undertake rescue operations. Therefore, communication facilities are crucial to timely rescue of ships. Furthermore, each ship should be equipped with self-defense weaponry and some security staff to contain the threat from pirates.

2.3.3. Quality of Emergency Plan and Ability of Action. Nowadays, many ship companies keep emergency plans ready to deal with piracy, because piracy is the singular, most critical issue that threatens the safety of ocean-going ships. Once a ship is attacked by pirates, the concerned ship company immediately activates its emergency plan to reduce possible loss, to the possible extent. A typical example in this regard is the ship of Shanghai Zhen Hua company, which was once attacked by pirates in Somalia area in February 2011. However, because of its strong emergency plan, the ship could successfully repel the pirates.

3. The Model for Evaluation

Li [25] proposed the cloud model to quantitatively represent the linguistic terms and to effectively integrate their fuzziness and randomness in a unified way, based on probability theory and fuzzy set. For this study, the authors' approach was to apply the cloud model theory to the Bayesian network for prior probability setting in order to obtain the probability distribution of nodes with fragmentary statistical data or qualitative information. Next, they introduce the process of their assessment model and illustrate its major theory.

3.1. Data Extracting and Processing. The data for piracy risk evaluation should cover the indicators referred to in Section 2. Data in respect of vulnerability and part of prevention capability are available with the attacked ship, while the hazard data were taken from IMO report, IFs index, ICAODS, and STEM30.

If the data were in quantitative terms, they were just recorded and their grading standard was set. If the data were in qualitative terms, experts' advice was sought for making linguistic comments on the condition of the indicators, based on the information available, and then the linguistic comments were recorded.

3.2. The Construction of Bayesian Network. Bayesian network (BN), also known as Bayesian reliability network, is not only a graphical expression of causal relationship among variables [26] but also a probabilistic reasoning technique. It can be represented by a binary: $B = <G, \theta>$.

(i) $G = (V, E)$ represents a directed acyclic graph. V is a set of nodes where each node represents a variable in the problem domain. E is a set of arcs, and a directed arc represents the causal dependency between variables.

(ii) θ is the network parameter, that is, the probability distribution of nodes. θ expresses the degree of mutual influence between nodes and presents quantitative characteristics in the knowledge domain.

Assume a set of variables $V = (v_1, \ldots, v_n)$. The mathematical basis of BN is Bayes Theorem showed by equation (1), which is also the core of Bayesian inference.

$$P(v_i \mid v_j) = \frac{P(v_i, v_j)}{P(v_j)} = \frac{P(v_i) \cdot P(v_j \mid v_i)}{P(v_j)}, \tag{1}$$

where $P(v_i)$ is the prior probability, $P(v_j \mid v_i)$ is the conditional probability, and $P(v_i \mid v_j)$ is the posterior probability. Based on $P(v_i)$, $P(v_i|v_j)$ could be derived by Bayes Theorem under the relevant conditions $P(v_j|v_i)$.

Bayesian network is generally used for causal representation of the phenomena involved in a complex system or process [27]. This approach allows for a better analysis of a knowledge-based system. It uses the Bayesian network as a modeling tool to quantify the risk of a complex system and obtain a better estimate of the probability distribution of the risk of a piracy event. Indeed, the scope of the Bayesian network is wide enough to permit analysis of the propagation of influences among the functions of different actors within the system (expressed as conditional probabilities).

3.3. Prior Probability Setting for Bayesian Network. To realize the Bayesian network, the probability of each node was set up. The widely used statistical methods for probability estimation mean that the node needs to possess a large amount of statistical quantitative data or a distinct concept. There are two kinds of data whose probability distribution is difficult to obtain: (a) fragmentary statistical quantitative data and (b) qualitative information. To obtain their probability distribution, the data of piracy events were used as follows.

3.3.1. Nodes with Qualitative Information. Some nodes offer only qualitative information. To obtain a quantitative and global result for intuitionistic acquaintance, a mathematical model is required to transform qualitative information into quantitative data. During such transformation, the nature of qualitative language should be retained to the maximum extent possible. Therefore, digital characteristics of cloud were used to transform the data, virtual cloud algorithm was used to synthesize multiexperts' views, and finally, the cloud generator was applied for generating cloud droplets with three characteristics (Ex, En, He), based on which the cloud chart can be obtained. Then, the probability distribution of one node is obtained by calculating the frequency of cloud droplets at each risk level in the cloud chart.

The major theories that were applied for processing are as follows.

The quantitative features (cloud) of the qualitative linguistic concept are always represented by three digital characteristics (Ex, En, He), which represent, respectively, expectation, entropy, and hyperentropy. The hyperentropy is a relatively new concept; it is a metric of uncertainty of entropy, which shows the degree of deviation from the normal distribution. It can also be considered a measure of the maturity of the cloud model and is always provided by the constructor of the model.

Virtual cloud algorithm is the most commonly used algorithm for cloud computing. It can be used to work out new digital characteristics, using the given digital characteristics. Cloud algorithm is of different kinds, like floating-cloud, integrating-cloud, decomposing-cloud, and geometrical-cloud algorithms. Among them, the floating-cloud and integrating-cloud algorithms are frequently used for cloud integration; the decomposing-cloud algorithm is inverted to the integrating-cloud algorithm by decomposing one cloud into several clouds to depict the concept in a more detailed and refined manner; the geometrical-cloud algorithm is used for fitting a complete cloud, based on some partial features [28].

Cloud generators can be divided into two kinds: forward and converse. The forward cloud generator can generate cloud droplets with three characteristics (Ex, En, He), which enable mapping to quantitative data from qualitative concept. Figure 1 shows the key features of the normal forward cloud generator, whose algorithm is as follows (here, the normal cloud is introduced because of its universality; the significant mathematical properties of the normal cloud are presented in detail in [29]):

(i) Generate a normal random value En' with En as the expectation and He^2 as the variance.

(ii) Generate a normal random value x with En as the expectation and En'^2 as the variance.

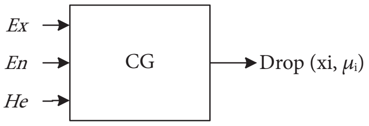

Figure 1: The normal forward cloud generator.

(iii) Calculate $\mu(x_i) = e^{-((x_i - \mathrm{Ex})^2/2(\mathrm{En}_i')^2)}$.

(iv) Generate x_i, with membership degree $\mu(x_i)$, as the cloud droplets in the number field.

(v) Repeat the above steps until the required amount of cloud droplets are generated.

3.3.2. Nodes with Fragmentary Statistical Quantitative Data. Every piracy event is reported by the attacked ship to IMO. However, some details of the event are generally lost in reporting, and this leads to missing data. To obtain the probability distribution of such nodes, the data distribution characteristics were extracted from the fragmentary data, using the cloud transform theory. Once the frequency distributions of the nodes were obtained, the distributions were divided into several Gaussian cloud distributions, some of which were overlapping each other. By setting a constraint condition for the relationship between these distributions, the Gaussian distributions were synthesized into several distributions that meet the constraint condition. Then, the membership to each risk level was obtained by the probability distribution of cloud droplets in the cloud chart.

The main aspects of the cloud transform theory are as follows.

Any data distribution can be transformed into overlays of several Gaussian distributions, and the process involved in such transformation is known as Gaussian transform [30]. The cloud transform used in converting the data distribution into Gaussian cloud distributions is based on the Gaussian transform. Then, by computing the amount of overlap between two clouds, which represents the maturity of partition, the partition of the data distribution was so readjusted that the overlap between the clouds was very little. For instance, Figure 2 shows the distribution curve (solid blue line) of 776 academicians in Chinese Engineering Academy, whose age ranges from 43 to 99 years. By Gaussian cloud transform, the age distribution data were divided into three and two kinds, as shown in Figures 2(a) and 2(b), respectively. When the data were divided into three kinds of clouds (see Figure 2(a)), the amount of overlap between the clouds is huge (especially the two clouds on the right), which means that the partition is ambiguous. When the data were transformed into two clouds (see Figure 2(b)), the overlap is within the acceptable limits, and hence the partition is considered much better.

Thus, the cloud transform helped in reducing data distribution and in depicting the areas of data concentration. By the transform, a numerical interval in which the data occupying larger probability can be obtained.

3.4. Conditional Probability Table Setting. The conditional probability is the probability of occurrence of an event, when it is known that another event has already occurred. When the mathematical relationship is not clear, it is always obtained by taking into account the experience of experts and statistical analysis of historical data [31].

For piracy risk, the influence of secondary nodes on the whole risk was not clear; so, it was difficult to construct mathematical models that reflect the influencing mechanism of each indicator. Therefore, fuzzy logic inference was applied to set up logical relationships of all kinds of scenarios and to sort out those belonging to the probability of risk levels. Using the scenarios so sorted out, the conditional probability table was generated randomly.

3.5. The Inference of Bayesian Network and Its Software Implementation. Based on the structure of Bayesian network and its parameters settings, posterior probability distribution of nodes can be inferred by probabilistic reasoning, whose mathematical basis is Bayes Theorem. Bayesian reasoning algorithm includes exact algorithm and approximate algorithm. Approximate algorithm is usually applied to large-scale network structure to deal with excessive computation [32]. Considering the scale of the network in our research, we apply the exact algorithm, joint tree inference algorithm, to obtain a posteriori distribution. The Bayesian reasoning algorithm used in the ***Netica*** software is the joint tree inference algorithm. When the users input prior information (the prior probabilities and conditional probability tables) into the *Netica* platform to obtain inferences, the results calculated will show up on the visual interface. The *Netica* is a practical Bayesian network simulation software that can realize most Bayesian classifications and reasoning. Besides, it has an intuitive and friendly user interface that allows users to draw the network and some algorithms that help in achieving structure and parameter learning. Lastly, *Netica* software can change node variable values arbitrarily and then automatically calculate the probability distribution of each node, based on the modified results.

To summarize, the flowchart of the model is illustrated in Figure 3.

4. Experiment of Piracy Risk Assessment

4.1. Data Sources and Processing. IMO has been recording the piracy events from 1982 till date. These reports contain, besides the historical accounts of the events, the details of each event, such as the number of pirates involved in each event and the weaponry they used [33]. These data were extracted from the report and their frequency statistics were computed.

International Monetary Fund (IMF), World Risk Index (WRI), and so on record every year several kinds of statistics relating to economy, such as GDP per capita, poverty population ratio, Gini coefficient, and CPI. The data are recorded in different units and metrics for different countries. Because of these differences, standardization of the

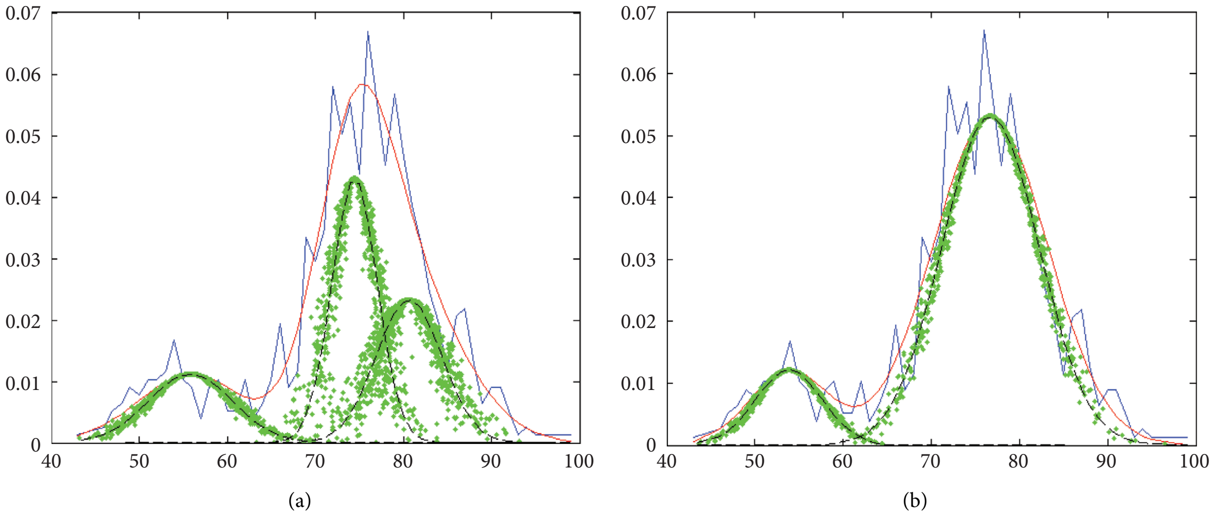

Figure 2: Gaussian cloud transform of academicians' ages.

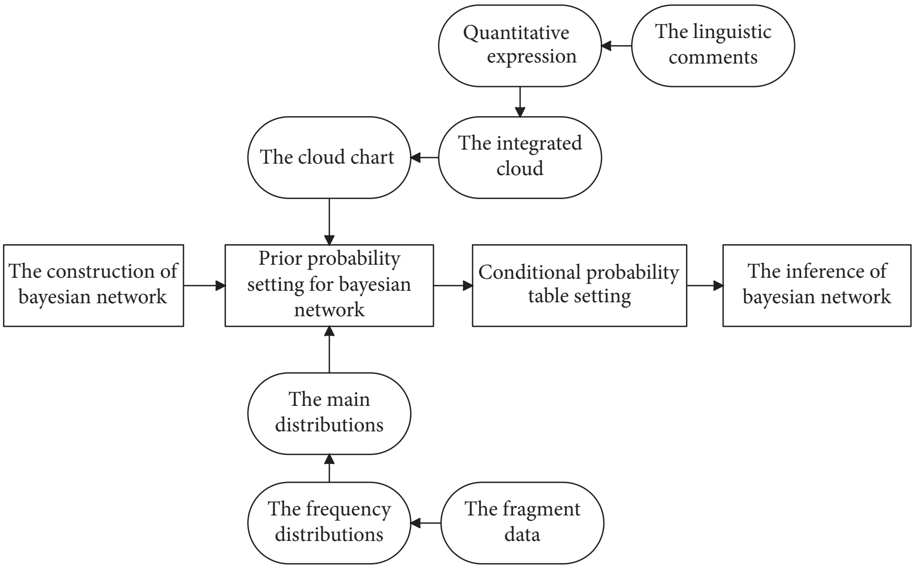
Quantitative expression
The linguistic comments
The integrated cloud
The cloud chart
The construction of bayesian network
Prior probability setting for bayesian network
Conditional probability table setting
The inference of bayesian network
The main distributions
The frequency distributions
The fragment data

Figure 3: The flowchart of the risk assessment model.

data is rather difficult. Therefore, the entire global data were divided into five levels, and the countries evaluated under these levels were given linguistic comments, according to their rankings.

The Transparency International (TI), World Govern Index (WGI), WRI, and so on record several kinds of statistics relating to politics, such as state failure instability event, state failure internal war event, governance corruption, and governance effectiveness. But, they do not contain the data of certain countries; besides, the data are recorded in different metrics for different countries. So, experts were invited to give their linguistic comments according to the rankings of the concerned countries.

The international comprehensive ocean atmosphere data set (ICOADS) provides surface marine data. The data set is merged from the disposed international data, including the ships (commercial, naval, and research) measurement or observation data, mooring and floating buoys data, coastal site data, and other ocean station data. The variables in this data set are wind velocity, wave height, visibility, and so on. However, these data cannot provide complete information on the weather condition that is relevant to piracy event. To make up for this lacuna, the variables relating to the event day were extracted and their frequency distribution analysis was carried out.

NASA and NIMA provide SRTM-3 (Shuttle Radar Topography Mission) data set, whose horizontal resolution is 90 m and the time scale is from 2000. The data set provides information on the geographic conditions of more than 80% of the global land surface.

4.2. Construction of Bayesian Network for Piracy Risk.

The structure of the Bayesian network for piracy risk assessment (see Figure 4) can be obtained based on expert knowledge, as explained in Section 2.

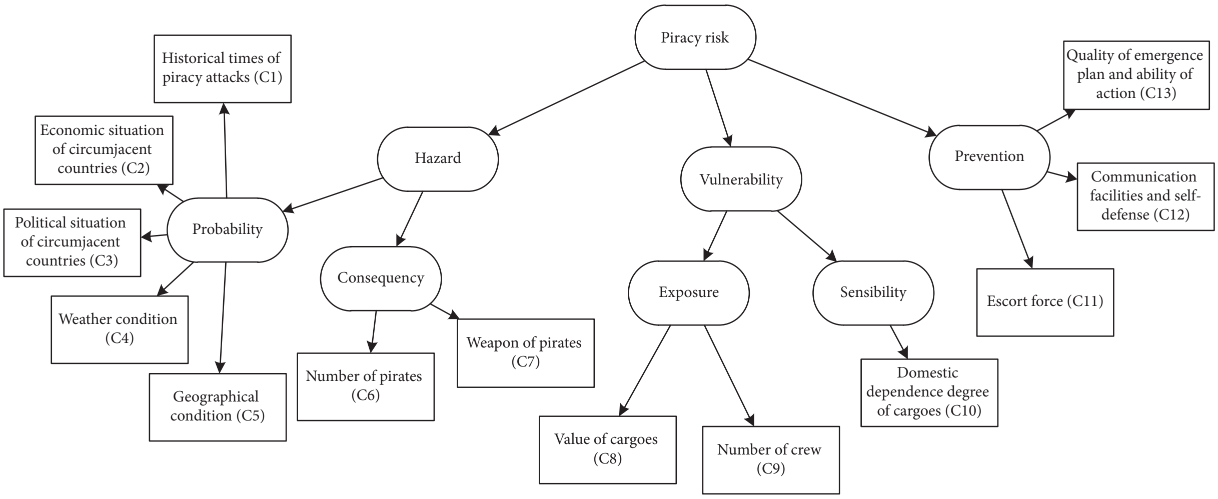
Piracy risk
Hazard
Vulnerability
Prevention
Probability
Consequency
Exposure
Sensibility
Historical times of piracy attacks (C1)
Economic situation of circumjacent countries (C2)
Political situation of circumjacent countries (C3)
Weather condition (C4)
Geographical condition (C5)
Number of pirates (C6)
Weapon of pirates (C7)
Value of cargoes (C8)
Number of crew (C9)
Domestic dependence degree of cargoes (C10)
Escort force (C11)
Communication facilities and self-defense (C12)
Quality of emergence plan and ability of action (C13)

Figure 4: The structure of Bayesian network for piracy risk.

4.3. Prior Probability Setting for Bayesian Network. As already mentioned, there are two kinds of piracy data, whose probability distribution is hard to get: (i) fragmentary statistical quantitative data and (ii) qualitative information. It may please be recalled that, in Section 3, the risk assessment model is introduced, along with the major theories involved in processing these data to obtain the probability distribution of each node. In this section, two examples are given to illustrate the application of these theories, one for qualitative information and the other for fragmentary statistical quantitative data.

4.3.1. The Nodes with Qualitative Information. There are two nodes in the data of such format, one relating to the economic situation of circumjacent countries and the other to political situation. To illustrate the application of cloud model theory, prior probability setting is introduced here for the economic situation of circumjacent countries node.

The economic situation of circumjacent countries is judged by certain indexes. Although there are many indexes, the following four were chosen for this study: per capita GDP, poverty percent less than \$1.25, domestic Gini, and human poverty index. The evaluated countries are around the South Sea area and include China, Indonesia, Vietnam, Philippines, Thailand, Malaysia, Singapore, Cambodia, and Brunei. Because of the big differences between their magnitude orders, standardizing their evaluations is very difficult. Based on the available data, the experts made their comments on each indicator, which are shown in Table 1. In this table, COM denotes comments, EL extremely low risk, RL relatively low risk, ME medium risk, RH relatively high risk, and EH extremely high risk.

The linguistic comments were then transferred to cloud digital characteristics. It was assumed that (0, 20), (20, 40), (40, 60), (60, 80), and (80, 100) represent, respectively, the linguistic comments "extremely low," "relatively low," "medium," "relatively high," and "extremely high." According to the normal cloud model, linguistic terms like "lower," "medium," and "higher" are restricted by bilateral boundaries, whose shape is a full bell. Its lower boundary was set as a and the upper boundary as b. Thus, such linguistic terms were quantified by equation (2). k is a constant value (0.1 for this study), which represents the maturity of this model, as decided by the experts [33]. However, such linguistic terms, such as "extreme low" and "extreme high," reached the left of the right boundary of the universe of discourse, and thus the bell shape of the cloud became a half-down or half-up bell cloud as shown in Figure 5. To represent these linguistic terms, if the boundary value a or b is set as Ex, then it will be quantified by equation (3).

$$\begin{cases} \mathrm{Ex} = \dfrac{(a+b)}{2}, \\ \mathrm{En} = \dfrac{(b-a)}{6}, \\ \mathrm{He} = k, \end{cases} \tag{2}$$

$$\begin{cases} \mathrm{Ex} = a \text{ or } b, \\ \mathrm{En} = \dfrac{(b-a)}{3}, \\ \mathrm{He} = k. \end{cases} \tag{3}$$

The digital characteristics of each comment are shown in Table 2. Because of the independence between indicators, the intersection within each indicator represents the economic situation best. Therefore, floating cloud was introduced to synthesize indicators` values. Then, the digital characteristics of the cloud model that represent the general economic situation of each country were computed and the results are shown in Table 2.

Finally, the general economic situation of the sea area under research, relative to that of the circumjacent countries, was calculated by integrating the results of the cloud algorithm, because the economic situation of every country should be taken into account. Then, the comprehensive risk

Table 1: Linguistic economic situation comments for the nine circumjacent countries.

	China	COM	Indonesia	COM	Vietnam	COM	Philippines	COM	Thailand	COM
GDP per capita ($\times 10^3$)	\$9.488	ME	\$8.274	RH	\$4.482	EH	\$5.737	EH	\$12.827	ME
Poverty percent less than \$1.25 ($\times 10^2$)	7.174	ME	14.938	EH	14.34	EH	16.724	EH	0.079	EL
Domestic Gini	0.422	RH	0.356	ME	0.359	ME	0.438	RH	0.397	ME
Human poverty index	4.845	ME	11.666	EH	9.283	RH	9.88	RH	5.309	ME
	Malaysia	COM	Singapore	COM	Cambodia	COM	Brunei	COM		
GDP per capita ($\times 10^3$)	\$20.73	EL	\$71.477	EL	\$2.639	EH	\$70.54	EL		
Poverty percent less than \$1.25 ($\times 10^2$)	0.014	EL	0	EL	17.008	EH	0	EL		
Domestic Gini	0.467	RH	0.431	RH	0.366	ME	0.19	EL		
Human poverty index	5.625	ME	2.661	RL	24.534	EH	2.276	RL		

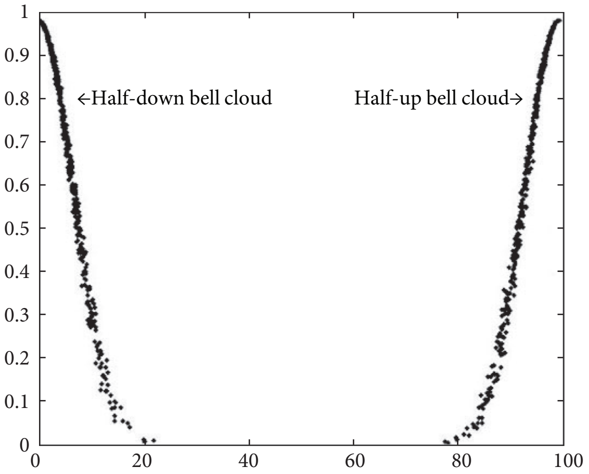

Figure 5: The half-down and half-up bell cloud.

Table 2: The digital characteristics of cloud model for the comments about economic situations of the nine circumjacent countries.

	China	Indonesia	Vietnam	Philippines	Thailand
GDP per capita	(50, 3.33, 0.1)	(70, 3.33, 0.1)	(100, 6.67, 0.1)	(100, 6.67, 0.1)	(50, 3.33, 0.1)
Poverty percent less than \$1.25 ($\times 10^2$)	(50, 3.33, 0.1)	(100, 6.67, 0.1)	(100, 6.67, 0.1)	(100, 6.67, 0.1)	(0, 6.67, 0.1)
Domestic Gini	(70, 3.33, 0.1)	(50, 3.33, 0.1)	(50, 3.33, 0.1)	(70, 3.33, 0.1)	(50, 3.33, 0.1)
Human poverty index	(50, 3.33, 0.1)	(100, 6.67, 0.1)	(70, 3.33, 0.1)	(70, 3.33, 0.1)	(50, 3.33, 0.1)
Economic situation	(55, 3.33, 0.1)	(80, 5, 0.1)	(80, 5, 0.1)	(85, 5, 0.1)	(37.5, 4.16, 0.1)
	Malaysia	Singapore	Cambodia	Brunei	
GDP per capita	(0, 6.67, 0.1)	(0, 6.67, 0.1)	(100, 6.67, 0.1)	(0, 6.67, 0.1)	
Poverty percent less than \$1.25 ($\times 10^2$)	(0, 6.67, 0.1)	(0, 6.67, 0.1)	(100, 6.67, 0.1)	(0, 6.67, 0.1)	
Domestic Gini	(70, 3.33, 0.1)	(70, 3.33, 0.1)	(50, 3.33, 0.1)	(0, 6.67, 0.1)	
Human poverty index	(50, 3.33, 0.1)	(30, 3.33, 0.1)	(100, 6.67, 0.1)	(30, 3.33, 0.1)	
Economic situation	(30, 5, 0.1)	(25, 5, 0.1)	(87.5, 5.835, 0.1)	(7.5, 5.84, 0.1)	

for economic situation of that area can be worked out in the form of digital characteristics (51.83, 18.94, 0.1). Finally, the positive cloud generator was brought in to obtain the risk cloud chart as shown in Figure 6. Because of the huge differences between the economic situations of the countries, there is great uncertainty in the cloud model. In addition, the cloud droplets out of range are reckoned as stretch of boundary value, so they are also considered as the notion with "extremely high" or "extremely low" concept.

The risk cloud chart comprises two thousand randomly generated cloud droplets. By counting the number of droplets in each comment interval, the proportion of the concepts occupying that interval was worked out. It can be seen that the proportion of cloud droplets in the extremely high-risk interval is 0.065, in the relatively high-risk interval 0.27, in the medium-risk interval 0.388, in the relatively low-risk interval 0.232, and in the extremely low-risk interval 0.045. By this way, the probability distribution of the nodes was obtained.

4.3.2. The Nodes with Fragmentary Statistical Quantitative Data. There are also two nodes with such data format as the weather condition and the number of pirates. Now, the prior

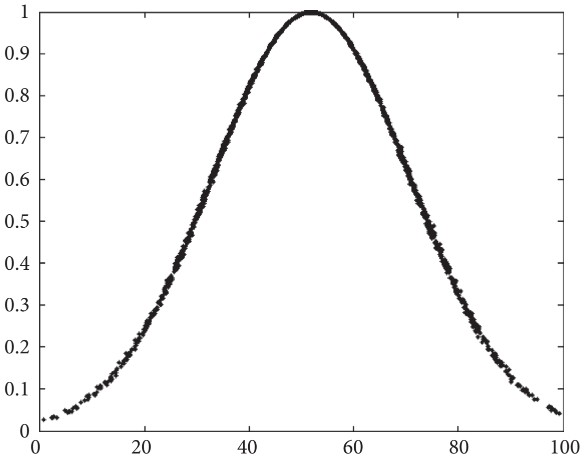

Figure 6: Risk cloud chart of economic situation of researched area.

probability setting for wind velocity node is presented to illustrate the application of cloud transform theory.

Using the data from ICAODS database, the frequency distribution of wind velocity was obtained as shown in Figure 7 (see the blue curve). Following the existing classification standards (the Beaufort Scale and the Visibility Classification of Chinese National Standard (QX/T 114–2010)), the hazard degrees of wind velocity, wave heights, and visibilities for this study were classified into five grades as shown in Table 3: extremely low risk, relatively low risk, medium risk, relatively high risk, and extremely high risk.

Applying the Gaussian transform $p(x) \longrightarrow \sum_{i=1}^{n}(a_i \cdot G(\mu_i, \sigma_i))$, the frequency distributions of the domain were converted into overlays of several Gaussian distributions. From these distributions, the corresponding Gaussian cloud distribution was obtained. Thus, by setting the constraint condition "the Gaussian clouds do not overlap each other," set a circulating algorithm:

(i) If the Gaussian clouds overlap each other,

(ii) then the number of Gaussian clouds is from M to $M-1$, and the two adjacent clouds are synthesized into one cloud

(iii) The synthesized cloud is compared with its adjacent cloud, and if they overlap, start (ii)

(iv) Finally, the clouds that do not overlap each other represent the distribution of the concept

Fitting the data distribution of wind velocity, via cloud transform, the cloud distribution of wind velocity is shown in Figure 7.

In this figure, the red line is the fitting curve of the Gaussian cloud, the green scatter is Gaussian cloud distribution, and the blue curve is the distribution of initial data.

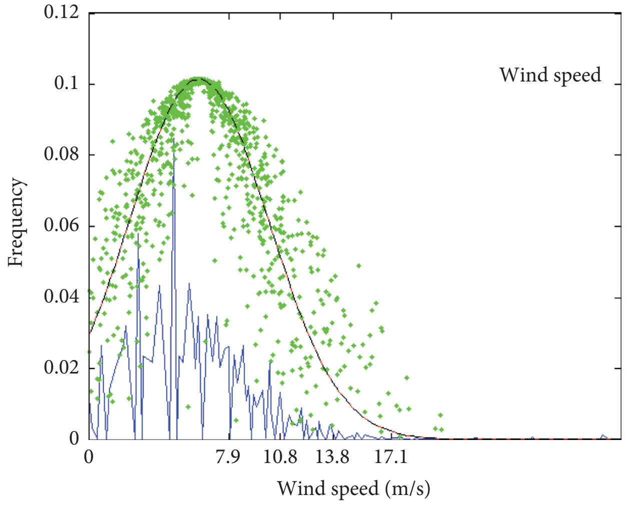

Figure 7: Gaussian cloud distribution chart of wind velocity.

From this figure, it can be seen that the proportion of the cloud droplets in the extremely high-risk interval is 0.656, in the relatively high-risk interval 0.193, in the medium-risk interval 0.103, in the relatively low-risk interval 0.025, and in the extremely low-risk interval 0.023. Thus, the probability of this node was obtained.

4.4. Conditional Probability Setting for Bayesian Network. Based on the logical relationships and the corresponding probabilities of risk level, the conditional probability table was generated randomly. For example, Table 4 shows the conditional probability table of "Hazard" node, generated on the basis of "Probability" and "Consequence" nodes.

From the first row of Table 4, it can be seen that when the risk levels of both "Probability" and "Consequence" are extremely high, the membership of "Hazard" to extremely high level is 96%, whereas the memberships to relatively high, medium, and relatively low levels are 2%, 1%, and 1%, respectively.

4.5. The Inference from Bayesian Network

4.5.1. Simulation Experiment of Hazard. The hazard of a system is inherent and does not vary with the risk-bearing objects. The risk confronted by the risk-bearing objects is the superimposition of system hazard, objective vulnerability, and antirisk property. The inherent hazard of the researched area can be calculated, based on historical data. To achieve this, the prior probability and conditional probability table were input into *Netica*, and then the inference was made on the network. After that, the membership degree to each risk level of the hazard of the research area was worked out as shown in Figure 8.

Table 3: Risk classification of wind velocity.

Risk level	Extremely low	Relatively low	Medium	Relatively high	Extremely high
Wind velocity (m/s)	17.1-	13.9–17.1	10.8–13.8	8–10.7	0–7.9

Table 4: The conditional probability table of "Hazard" node.

Probability	Consequence	Hazard (%)				
		Extremely high	Relatively high	Medium	Relatively low	Extremely low
Extremely high	Extremely high	96	2	1	1	0
Extremely high	Relatively high	45	45	4	3	3
Extremely high	Medium	46	3	47	3	1
Extremely high	Relatively low	44	3	4	48	1
Extremely high	Extremely low	44	5	0	6	45
Relatively high	Extremely high	49	45	5	1	0
Relatively high	Relatively high	7	93	0	0	0
Relatively high	Medium	3	40	47	5	5
Relatively high	Relatively low	3	43	3	43	8
Relatively high	Extremely low	2	46	3	3	46
Medium	Extremely high	50	2	47	1	0
Medium	Relatively high	1	45	47	5	2
Medium	Medium	0	1	98	1	0
Medium	Relatively low	1	3	42	42	12
Medium	Extremely low	96	2	96	2	1
Relatively low	Extremely high	96	2	45	45	4
Relatively low	Relatively high	45	45	46	3	47
Relatively low	Medium	46	3	44	3	4
Relatively low	Relatively low	44	3	44	5	0
Relatively low	Extremely low	44	5	49	45	5
Extremely low	Extremely high	49	45	7	93	0
Extremely low	Relatively high	7	93	3	40	47
Extremely low	Medium	3	40	3	43	3
Extremely low	Relatively low	3	43	96	2	1
Extremely low	Extremely low	2	46	45	45	4

Figure 8 shows that the membership of "probability" node to extremely high-risk level is up to 42.9%, thus indicating that the probability of ships being attacked by pirates is extremely high. The membership of "consequence" node to extremely high-risk level is the largest at 26.7%. The risk of inherent hazard of the researched area is thus inferred to be extremely high with the largest membership of 33.3%.

4.5.2. Validation of Model. In this section, two case histories, relating to the South China Sea, are presented to validate the proposed model.

(1) Piracy Accident, Bearing IMO No. 9522984. The whole event was recorded as follows. The tug departed from Singapore, en route to Cambodia, towing the Singapore-registered barge CALISTA with 12 crewmembers on board. It was hijacked by eight pirates dressed in black clothes and armed with rifles and parangs. Initially, the pirates locked all the crew members in their cabins and later, on the 10 February, set them adrift on a life raft. They were rescued on 11 February by the Malaysian Navy. The geographic coordinates of the area of incident are 13°04.00′N, 47°04.00′E.

Using the climatic conditions of that day and the geographic conditions of that area, together with other relevant data of the event, prior probabilities of the Bayesian network were obtained. For this, first, the parameters were input, and then the posterior probability of the target node was calculated. The result is shown in Figure 9.

As shown in Figure 9, the piracy risk is extremely high (with a membership degree of 30.7%), which is in good agreement with the result of the real event, wherein the pirates took hostage of the entire crew and hijacked the ship.

(2) Piracy Accident, Bearing IMO No. 9379662. The whole event was recorded as follows. Four pirates armed with long knives boarded the ship at the forecastle, where it was anchored. They attempted to disarm the two duty watchmen and enter the cabins, but some alert crew members locked all the entrances and the duty OOW raised alarm. So, the pirates could just steal some stores of the ship and escape. The geographic coordinates of the area of incident are 22°15.00′N, 91°44.00′E.

The result obtained by following the same procedure as that of case 1 is shown in Figure 10.

As shown in Figure 10, the piracy risk is rather low (with a membership degree of 42.6%), which is in conformity with the result of the real event, wherein the pirates could only steal some stores and escape.

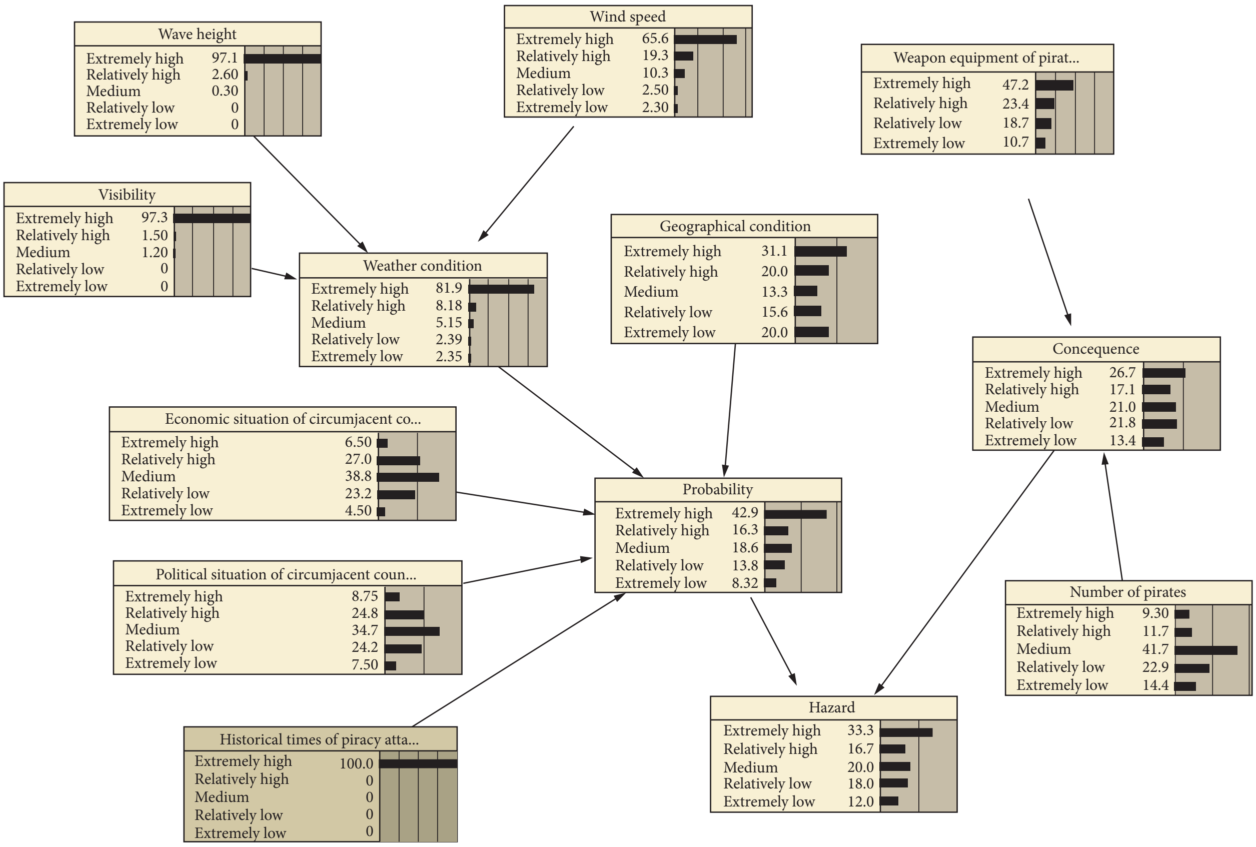

Figure 8: The Bayesian network inference of the hazard.

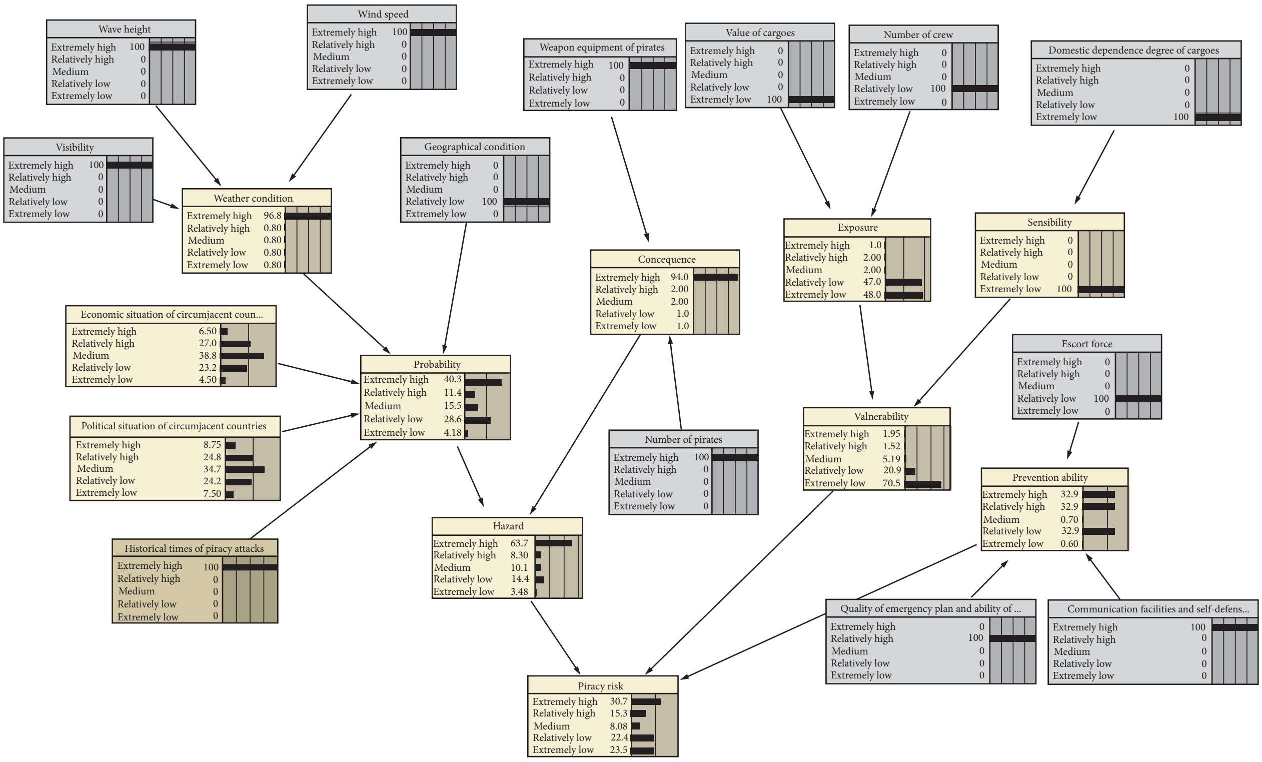

Figure 9: The Bayesian network inference of case 1.

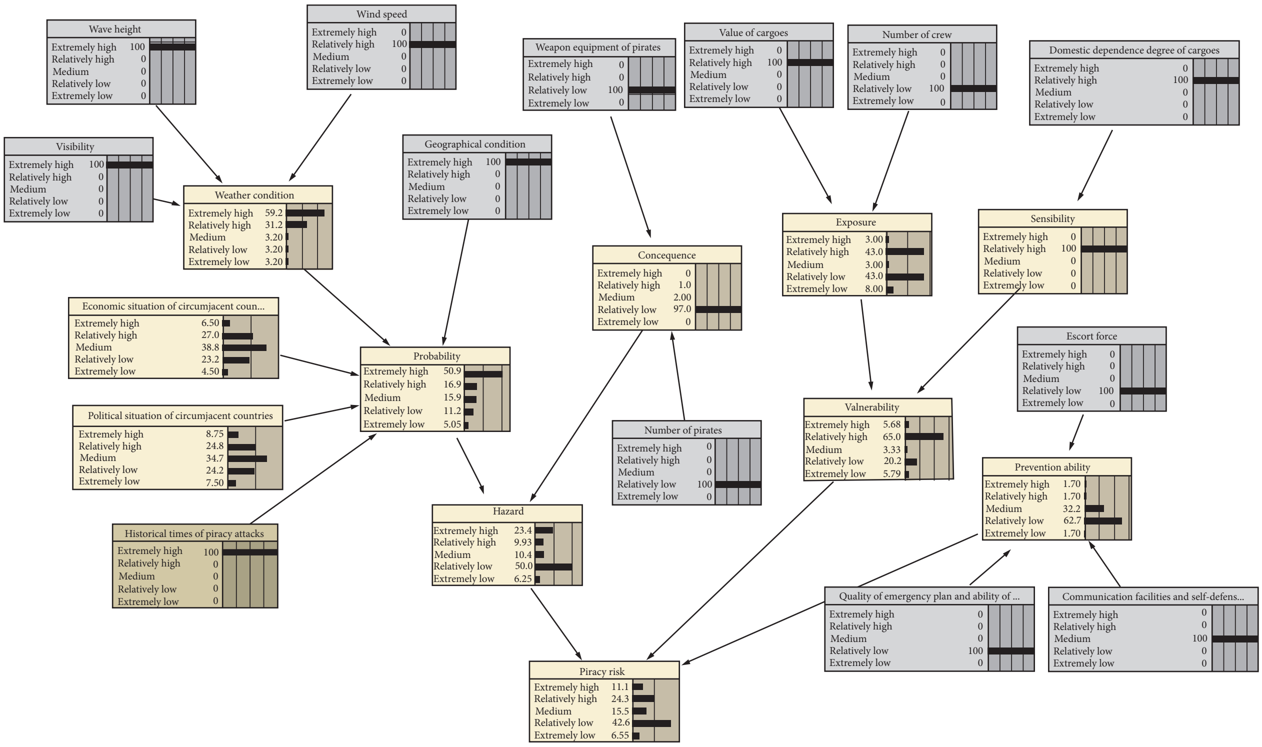

Figure 10: The Bayesian network inference of case 2.

5. Conclusion

In the present study, a quantitative risk assessment model for piracy was constructed, using the Bayesian network. Cloud model theory was used to achieve prior probability settings of Bayesian network for the nodes with qualitative information and fragmentary statistical quantitative data. Finally, the hazards of piracy risk on the South China Sea were used as an example for the application of the risk assessment model. Furthermore, two case histories of real piracy events were analyzed to validate the proposed model. The assessment result shows that the piracy hazard of the South China Sea is extremely high. Besides, the risk assessment results of the two cases are in conformity with those of the real events. Therefore, any ship or transport company can apply this model for piracy risk assessment and adjust their emergency plans according to the results of key nodes.

The piracy risk assessment is a fundamental requirement for allocating equipment and preparing emergency plans for ship travel. Similarly, prior probability settings of the Bayesian network are fundamental to risk assessment, of which requirement can be better solved by the proposed model than by the existing ones. The potential of the proposed model is summarized as follows:

(1) Prior probability of nodes can be obtained from qualitative information, using the cloud model theory. The cloud model reflects the uncertainty of linguistic comments better than the traditional fuzzy set does with random implementation and membership principle. And, exactly because of the randomness of the cloud model, the probability can be counted in terms of cloud drops. For cloud model, unlike the traditional method, the experts need to make only linguistic comments on the evaluated objectives and not to give their mathematical probability distribution. This is better suited to the human thinking model, because the cognition event of humans is always a fuzzy concept and is difficult to describe mathematically.

(2) Prior probability of nodes can be obtained from fragmentary statistical data, using the cloud transform theory. This theory can extract the distribution of quantitative data and classify it into appointed kinds of Gaussian clouds. If the Gaussian clouds do not overlap each other, then the main distributions of the quantitative data show up clearly. Because the cloud drops are random, the probability can be assessed by counting them. The proposed method works out the prior probability of the fragment statistic data which provides a solution under the condition with incomplete parameter, whereas the existing researches and expanding models mostly focus on the conditional probability settings with the incomplete parameter.

(3) Unlike the existing research methods on piracy risk, the risk assessment model proposed here takes into account the hazard of pirate, the vulnerability of attacked ships, and the antirisk properties of both the ships and their escort force. For this study, the major factors involved in the formation of piracy risk mechanism were analyzed and the indicator system for piracy risk assessment was constructed. The

results show that ships with different levels of vulnerability and different antirisk properties confront different types of risks.

(4) The risk assessment model can be applied even to cases with incomplete data set or qualitative information.

Admittedly, the piracy risk assessment model proposed here is not free from defects. Although the Bayesian network, especially the one based on software platform, can make real-time assessment of emergency events by changing the probability distribution of nodes, it can only obtain the risk, based on the known information and with delay. As there are no definitive laws to project piracy risk, the probability relationships between time slices remain unknown. So, dynamic risk assessment of piracy is difficult. To solve this problem, a lot more research has to be done. Particularly, the laws of piracy risk will have to be found out so that the probability relationships between the time slices can be set up to make dynamic risk assessment of piracy risk a distinct possibility. This, in turn, can help the decision-makers in taking appropriate timely decisions for preempting or containing piracy risk.

Data Availability

IMO has been recording the piracy events from 1982 till date. These reports contain, besides the historical accounts of the events, the details of each event, such as the number of pirates involved in each event and the weaponry they used. These data were extracted from the report and their frequency statistics were computed. International Monetary Fund (IMF), World Risk Index (WRI), and so on record every year several kinds of statistics relating to economy, such as GDP per capita, poverty population ratio, Gini coefficient, and CPI. The data are recorded in different units and metrics for different countries. Because of these differences, standardization of the data is rather difficult. Therefore, the entire global data were divided into five levels, and the countries evaluated under these levels were given linguistic comments, according to their rankings. The Transparency International (TI), World Govern Index (WGI), WRI, and so on record several kinds of statistics relating to politics, such as state failure instability event, state failure internal war event, governance corruption, and governance effectiveness. But, they do not contain the data of certain countries; besides, the data are recorded in different metrics for different countries. So, experts were invited to give their linguistic comments according to the rankings of the concerned countries. The ICOADS provides surface marine data. The data set is merged from the disposed international data, including the ships (commercial, naval, and research) measurement or observation data, mooring and floating buoys data, coastal site data, and other ocean station data. The variables in this data set are wind velocity, wave height, visibility, and so on. However, these data cannot provide complete information on the weather condition that is relevant to piracy event. To make up for this lacuna, the variables relating to the event day were extracted and their frequency distribution analysis was carried out. NASA and NIMA provide SRTM-3 (Shuttle Radar Topography Mission) data set, whose horizontal resolution is 90 m and the time scale is from 2000. The data set provides information on the geographic conditions of more than 80% of the global land surface.

Conflicts of Interest

The authors declare no conflicts of interest.

Authors' Contributions

Lizhi Yang and Kefeng Liu conceived and designed the experiments; Ming Li performed the experiments; Lizhi Yang analyzed the data; Kefeng Liu wrote the paper.

References

[1] H. R. Williamson, "New thinking in the fight against marine piracy: financing and plunder pre-empting piracy before prevention becomes necessary," *Case Western Reserve Journal of International Law*, vol. 32, 2013.

[2] C. M. Douse, "Combating risk on the high sea, an analysis of the effects of modern piratical acts on the marine insurance industry," *Tulane Maritime Law Journal*, vol. 19, 2010.

[3] J. Chen, "The economic analysis and the countermeasures of pirate crime," *Economy & Management*, vol. 25, 2011.

[4] B. Lucas, "Toward an international law of piracy sui generis. How the dual nature of maritime piracy law enables piracy to flourish," *Social Science Electronic Publishing*, vol. 29, no. 2, pp. 399–455, 2010.

[5] O. Vaněk, B. Bošanský, M. Jakob, and M. Pechoucek, "Transiting areas patrolled by a mobile adversary," in *Proceedings of the 2010 IEEE Symposium on Computational Intelligence and Games (CIG)*, pp. 9–16, Dublin, Ireland, August 2010.

[6] C. D. Marsh, "Counter piracy. A repeated game with asymmetric information," Thesis, Naval Postgraduate School, Monterey, CA, USA, 2009.

[7] Z. F. Rui, R. R. Ying, and L. I. Wei, "A methodology for military route selection using intuitionist fuzzy numbers," *Ship Science & Technology*, vol. 36, no. 1, pp. 144–157, 2014.

[8] J. J. Dabrowski and J. P. De Villiers, "Maritime piracy situation modelling with dynamic Bayesian networks," *Information Fusion*, vol. 23, pp. 116–130, 2015.

[9] A. Bouejla, X. Chaze, F. Guarnieri, and A. Napoli, "Bayesian networks in the management of oil field piracy risk," in *Proceedings of the 8th International Conference on Simulation in Risk Analysis and Hazard Mitigation*, vol. VIII, p. 12, Brac, Croatia, September 2012.

[10] A. Bouejla, X. Chaze, F. Guarnieri, and A. Napoli, "A Bayesian network to manage risks of maritime piracy against offshore oil fields," *Safety Science*, vol. 68, pp. 222–230, 2014.

[11] X. Chaze, A. Bouejla, A. Napoli, and F. Guarnieri, "Integration of a Bayesian network for response planning in a maritime piracy risk management system," in *Proceedings of the 2012 7th International Conference on System of Systems Engineering SOSE*, p. 6, Genova, Italy, July 2012.

[12] H. Liwång, J. W. Ringsberg, and M. Norsell, "Quantitative risk analysis - ship security analysis for effective risk control options," *Safety Science*, vol. 58, no. 10, pp. 98–112, 2013.

[13] J. C. Sevillano, D. Rios Insua, and J. Rios, "Adversarial risk analysis: the Somali pirates case the Somali pirates case," *Decision Analysis*, vol. 9, no. 2, pp. 86–95, 2012.

[14] M. P. Fanti, G. Iacobellis, and W. Ukovich, "A risk assessment framework for hazmat transportation in highways by colored petri nets," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 3, pp. 485–495, 2015.

[15] B. Cai, Y. Liu, Z. Liu, X. Tian, Y. Zhang, and R. Ji, "Application of bayesian networks in quantitative risk assessment of subsea blowout preventer operations," *Risk Analysis*, vol. 33, no. 7, pp. 1293–1311, 2013.

[16] D. Codetta-Raiteri and L. Portinale, "Dynamic bayesian networks for fault detection, identification, and recovery in autonomous spacecraft," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 1, pp. 13–24, 2015.

[17] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, and S. Huang, "Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems," *IEEE Transactions on Systems Man & Cybernetics Systems*, vol. 46, no. 10, pp. 1–16, 2015.

[18] B. Cai, Y. Liu, Y. Zhang, Q. Fan, Z. Liu, and X. Tian, "A dynamic Bayesian networks modeling of human factors on offshore blowouts," *Journal of Loss Prevention in the Process Industries*, vol. 26, no. 4, pp. 639–649, 2013.

[19] Y. Y. Haimes, "On the definition of vulnerabilities in measuring risks to infrastructures," *Risk Analysis*, vol. 26, no. 2, pp. 293–296, 2006.

[20] G. Tsakiris, "Flood risk assessment: concepts, modelling, applications," *Natural Hazards and Earth System Sciences Discussions*, vol. 14, no. 5, pp. 1361–1369, 2014.

[21] J. Q. Zhang and N. Li, *Quantitative Methods and Applications of Risk Assessment and Management on Main Meteorological Disasters*, pp. 32–34, Beijing Normal University press, Beijing, China, 2007.

[22] R. Zhang, *Characteristic Diagnosis of Marine Environmental Factors and Risk Assessment of Oceanic Military Activity*, pp. 238-239, Beijing Normal University press, Beijing, China, 2012.

[23] ICC International Maritime Bureau, *ICC-IMB Piracy and Armed Robbery against Ships Report-Annual Report*, ICC International Maritime Bureau, London, England, 2011, http://www.iccwbo.org/products-and-services/fighting-commercial-crime/international-maritime-bureau/.

[24] S. Belliveau, B. Smit, and B. Bradshaw, "Multiple exposures and dynamic vulnerability: evidence from the grape industry in the Okanagan Valley, Canada," *Global Environmental Change*, vol. 16, no. 4, pp. 364–378, 2006.

[25] D. Li, H. Meng, and X. Shi, "Membership clouds and membership cloud generators," *Journal of Computer Research & Development*, vol. 32, no. 6, pp. 15–20, 1995.

[26] M. Li and K. Liu, "Probabilistic prediction of significant wave height using dynamic bayesian network and information flow," *Water*, vol. 12, no. 8, p. 2075, 2020.

[27] M. Li, R. Zhang, and K. Liu, "A new ensemble learning algorithm combined with causal analysis for bayesian network structural learning," *Symmetry*, vol. 12, no. 12, p. 2054, 2020.

[28] K. Di, D. Li, and D. Li, "Cloud theory and its applications in spatial data mining and knowledge discovery," *Journal of Image & Graphics*, vol. 4, no. 11, pp. 930–935, 1999.

[29] D. Li, *Artificial Intelligence with Uncertainty*, National Defense Industry Press, Beijing, China, 2014.

[30] T. I. Alecu, S. Voloshynovskiy, and T. Pun, "The Gaussian transform of distributions: definition, computation and application," *IEEE Transactions on Signal Processing*, vol. 54, no. 8, pp. 2976–2985, 2006.

[31] B. Cai, Y. Liu, Q. Fan et al., "Multi-source information fusion based fault diagnosis of ground-source heat pump using Bayesian network," *Applied Energy*, vol. 114, no. 2, pp. 1–9, 2014.

[32] M. Li and K. Liu, "Causality-based attribute weighting via information flow and genetic algorithm for naive Bayes classifier," *IEEE Access*, vol. 7, pp. 150630–150641, 2019.

[33] L. Yang, R. Zhang, T. Hou, Z. Hao, and J. Liu, "Hesitant cloud model and its application in the risk assessment of "the twenty-first century maritime silk road," *Mathematical Problems in Engineering*, vol. 2016, no. 3, 11 pages, Article ID 5620803, 2016.