A Novel Flexible Model for Piracy and Robbery Assessment of Merchant Ship Operations

Sascha Pristrom, Zaili Yang, Jin Wang*
[a]*Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, Liverpool, UK*
Xinping Yan
National Engineering Research Center for Water Transport Safety (WTSC)
Wuhan University of Technology, Wuhan, China

Abstract

Maritime piracy and robbery can not only cause logistics chain disruption leading to economic consequences but also result in loss of lives, and short- and long-term health problems of seafarers and passengers. There is a justified need for further investigation in this area of paramount importance. This study analyses maritime piracy and robbery related incidents in terms of the major influencing factors such as ship characteristics and geographical locations. An analytical model incorporating Bayesian reasoning is proposed to estimate the likelihood of a ship being hijacked in the Western Indian or Eastern African region. The proposed model takes into account the characteristics of the ship, environment conditions and the maritime security measures in place in an integrated manner. Available data collected from the Global Integrated Shipping Information System (GISIS) together with expert judgement is used to develop and demonstrate the proposed model. This model can be used by maritime stakeholders to make cost-effective anti-piracy decisions in their operations under uncertainties. Discussions are given on industrial response to maritime piracy in order to minimize the risk to ships exposed to attacks from pirates. Further recommendations on how maritime security and piracy may be best addressed in terms of maritime security measures are outlined.

Keywords: Maritime security, maritime piracy, hijacking, best management practice.

1. Introduction

Internationally, more than 55,000 merchant ships carry more than 8.4 billion tonnes of goods each year (HM Government, 2014). It is important to understand how maritime security issues are addressed through the most efficient use of available resources. It is also necessary to carefully assess and prioritise the maritime security risks and opportunities we face, in order to allocate our resources rationally.

Maritime security is defined as "the advancement and protection of a nation's interests, at home and abroad, through the active management of risks and opportunities in and from the maritime domain, in order to strengthen and extend the nation's prosperity, security and resilience and to help shape a stable world" (HM Government, 2014). While risk is defined as "a combination of the probability of occurrence of an undesired event and the degree of its possible consequences" (Wang and Trbojevic, 2007), this study focuses on the occurrence likelihood of attacks from pirates, having known that the involved consequences are usually severe. Maritime security issues broadly include:

- Terrorism affecting a nation and its maritime interests, including attacks against cargo or passenger ships;
- Disruption to vital maritime trade routes as a result of war, criminality, piracy or changes in international norms;
- Attack on a nation's maritime infrastructure or shipping;
- The transportation of illegal items by sea, including weapons of mass destruction (WMD), controlled drugs and arms; and
- People smuggling and human trafficking.

* Corresponding author, e-mail: j.wang@ljmu.ac.uk.

Maritime piracy needs to be distinguished from other clusters within the maritime security domain as maritime terrorism, armed robbery and theft are driven by different motives (Schneider, 2012). It is noted that the modus operandi of pirates is very different from that of terrorists but both phenomena are constantly evolving and may develop characteristics that make a distinction between them more and more difficult. While piracy is, to some extent, predictable depending on sea areas (Piracy High Risk Area (HRA) versus low risk areas), weather conditions and/or the implementation of Best Management Practices (BMP), maritime terrorism cannot be confidently predicted and is still debated (Schneider, 2012). Whereas pirates seek financial gains from attacks, terrorists pursue a political agenda. Pirates as well as terrorists that attempt to attack a ship at sea face challenges unknown, compared to attacks carried out ashore (Pristrom, 2013).

This paper presents a novel model which can be used for predicting the likelihood of a ship being attacked by pirates given the characteristics of the ship, environment conditions and the maritime security measures in place. The rest of the paper is organized as follows. Section 2 reviews the current status through investigating recent maritime piracy accidents. Section 3 is dedicated to developing a new model for estimating the occurrence likelihood of successful hijacking of a ship in the Western Indian/Eastern African Region. In Section 4, a case study is presented to demonstrate the proposed model. Industrial response to maritime piracy is discussed in Section 5. The paper is concluded in terms of possible application of the proposed model in Section 6.

2. Current Status

2.1 Maritime Piracy Patterns

The shipping industry and international organisations have made enormous effort in the resolution to the menace of piracy. Several States have sent naval assets to the HRA to protect merchant shipping from attacks and several UN organisations have dedicated expert teams to improve the situation. The International Maritime Organization (IMO) supported the setting up of a regional cooperation agreement, the Djibouti Code of Conduct, aimed at assisting littoral States that are affected by Somali piracy to implement a set of measures to suppress piracy using their own resources. The IMO was also instrumental in establishing the framework for collaboration among the littoral states of the Straits of Malacca and Singapore and the South China Sea, the so-called Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) agreement (IMO, 2012a). A major step in addressing maritime crime in the Gulf of Guinea region has been made in June 2013 when Heads of States or their representatives from 25 West and Central African countries signed the Code of Conduct concerning the repression of piracy, armed robbery against ships, and illicit maritime activity in West and Central Africa.

The positive development in the suppression of piracy and armed robbery against Somalia-based piracy can be attributed to the fact that many organizations have made efforts to address maritime piracy activities in Somali waters and the wider Western Indian Ocean. For example, the United Nations Political Office for Somalia (UNPOS)[1] started developing and implementing the National Security and Stabilization Plan through active engagement with the Federal Government of Somalia.

Modern pirates use state-of-the-art equipment in their operations (Psarros *et al*., 2011). Their crimes range from simple robbery to murder and hijacking of entire ships for ransom demand. Modern piracy became a significant threat in the late 1990s and early years after the Millennium in South East Asia and in particular the Malacca Strait whereas the current piracy hot-spots are the waters off the coasts of West and East Africa. However, incidents in the Malacca Strait are rising and siphoning oil cargo from product tankers – similar to incidents in the Gulf of Guinea – has been reported also for this region. By analysing the available statistical material from the IMO's monthly piracy reports during the period 2000–2009, it is found that incidents off and around the African continent have led to fewer deaths as compared to those in South China Sea and Malacca strait (Psarros *et al*., 2011). This

[1] The United Nations Assistance Mission in Somalia (UNSOM) was established on 3 June 2013 and replaced UNPOS. The different regions of Somalia together with the Federal Government of Somalia now work on the implementation of the Integrated Strategic Framework.

demonstrates that the attack rates on specific vessel segments and the recorded incidents for each geographical area develop their own trends. The highest occurrences of piracy incidents during the period from 1 January 2007 to 1 December 2014 are the waters off the East African coast; this was by far the most dangerous area for ships to become a victim of piracy. The statistics of incidents show that three other piracy hotspot areas are: the South East Asia region comprising the South China Sea and its adjacent waters, the Indian Ocean and West Africa (Source: IMO Global Integrated Shipping Information System (GISIS database)).

The ship type that has been mostly attacked since 1994 is bulk carriers, followed by tankers and general cargo ships as shown in Table 1 which may be a reflection of the proportion of ship types in operation in conjunction with their vulnerability to pirate attacks. This gives the average number of attacks per month as 27.1 (i.e. 6,637/(20×12+5)).

Table 1 All incidents of piracy and armed robbery from 1 July 1994 - 01 December 2014 (*Source: IMO GISIS database*)

Ship type	Total number	Ship type	Total number
Bulk carrier	1425	Gas Tanker	169
Tanker	1228	Reefer	95
General cargo ship	949	Ro-Ro	75
Container ship	933	Car carrier	38
Chemical tanker	580	Passenger ship	21
Special purpose*	406	Ferry	13
Small craft†	381	Barge	49
unspecified	275		
Total:	**6637**		

**includes*: *dredgers, landing crafts, heavy load carriers, MODUs, offshore supply ships, research ships, tugs*
† *includes*: *fishing vessels, dhows, yachts*

As the intention of pirates is not necessarily to hijack a ship, it is useful to analyse the attacks where pirates managed to board the ship (a piracy/robbery incident in Table 1 may not necessarily lead to a boarding incident). For 4,109 successful boarding events during the period from 1 July 1994 to 1 December 2014 the highest rate of boarding while the ship was underway is for the category 'Special purpose', followed by 'Oil tankers', 'Small craft' and 'General cargo'. The ship types categorised under 'Special purpose' and 'Small craft' are listed at the bottom of Table 1. It underlines that ships with a slow speed and low freeboard are particularly at risk of becoming a victim of piracy. Gas carriers and bulk carriers are of less risk of being boarded while steaming. This is largely due to their relatively high freeboard.

Ships with the highest risk of becoming a victim of piracy off the East African coast are small craft (31% of the total pirate attacks). However, the risk for general cargo ships (20%), bulk carriers (18%) and chemical tankers (12%) while steaming in the piracy-infested waters off the coast of Somalia is significantly higher than that in the other regions around the world. Due to the success in the suppression of Somalia-based piracy the number of attacks has significantly decreased since the second half of 2012. The last successful hijacking of a SOLAS ship (i.e. a ship that is large enough to fall under the International Convention for the Safety of Life at Sea) was in May 2012.

A significant difference with regard to the type and number of incidents off Africa exists in comparison to South America where the boarding rate while steaming is significantly lower. However, in South America, small craft are still exposed to the greatest threat of becoming a victim of piracy, followed by chemical tankers and container ships.

In the case of West Africa the statistics are closer to the worldwide average in the sense that the highest threat by ship type while steaming is for small craft and special purpose ships. The ratio of boarding is well below 20% for tankers, general cargo ships and bulk carriers.

The statistical analysis of ship types for different geographical regions shows that ships with the highest risk of being boarded while steaming do not differ significantly in different geographical areas. Small craft, special purpose ships and chemical tankers are, in the vast majority of the cases, vessels with a low freeboard and a slow speed and therefore easier to board, irrespective of their geographical locations.

2.2. Maritime Piracy in Geographical Regions of Significance

2.2.1 Piracy off the coast of Somalia

Somali piracy had been increasing since 2005, not only in terms of the number of attacks but also in the amount of ransom received by Somali pirates (Ehrhart and Petretto, 2012). However, in 2011 and 2012 the number of hijackings went down compared with the figures in the previous years. This latest change of trend may be largely attributed to robust targeting of pirate action groups by international navies in the high-risk waters off Somalia (Mukundan, 2012), the better implementation of BMP by ship operators and masters and the increased use of Privately Contracted Armed Security Personnel (PCASP).

Despite better maritime domain awareness (MDA) through the analysis of Long Range-Identification and Tracking (LRIT) data, the deployment of Maritime Patrol and Reconnaissance Aircraft (MPRA), drones and other surveillance systems, a considerable number of attacks and approaches off the East African coast were reported to either the IMO through the flag States or the industry-led IMB (International Maritime Bureau). Table 2 indicates the trend of attacks by Somali pirates. It should be noted though that the real number of attacks is likely to be considerably higher (Pristrom *et al.*, 2013). These attacks were either attempted or boarded/hijacked. Hijacking for ransom is a distinguishing criterion (Ehrhart and Petretto, 2012) for Somali pirates compared with those from other piracy risk areas in the world. Given the magnitude of the impact of Somali-based piracy on human life, predominantly on seafarers, several international shipping initiatives have been established along with cooperation agreements among States, their navies and private initiatives. The vulnerability of ships passing the HRA resulted in a boost in maritime security technology development and a hike in the number of newly founded private security companies entering this new market.

Table 2: Somali piracy (Source: IMO GISIS database)

Year	Ships attacked	Hijackings	Success
2007	52	12	23.1%
2008	120	40	33.3%
2009	258	51	19.8%
2010	253	61	24.1%
2011	239	32	13.4%
2012	103	13	12.6%
2013	23	2	8.7%
2014*	15	0	0%
Σ	1063	211	

** as of 1 March 2015*

2.2.2 West Africa Piracy

Ships which are at risk in the Gulf of Guinea are mainly those which are deployed for the oil industry. The way pirates operate in the Gulf of Guinea is different, compared to their East African counterparts who hijack ships for ransom. A substantial proportion of West African pirates, who are usually more violent, are based in Nigeria. They often attack victim ships that are at anchor or drifting while waiting for cargo or orders to proceed to the port. Hence West African perpetrators do not have to attack while the ship is at full speed. The nature of West African piracy has changed from petty theft

of crew personal effects and ships stores in and around port areas (UK P&I Club, 2011) into a more sophisticated and violent criminal activity. West African piracy can be grouped into the three main categories: 'Armed robbery', 'Cargo theft' and 'Kidnapping'.

While armed robbery is somewhat opportunistic and aimed at ransacking the ship valuables including personal belongings of the crew, it differs from incidents of the same category in other regions of the world as the level of violence applied by the attackers is generally higher. Very often such attacks cause serious harm to the crew including the ship's master.

West Africa piracy has its own characteristics and impact on the shipping industry. A very unique type of piracy that is endangering shipping in this part of the world is oil cargo theft, usually during Ship-To-Ship (STS) transfers. In order to target a ship to siphon off its oil cargo, a minimum of intelligence is necessary to prepare for an STS transfer. Further, it requires some advanced seamanship and personnel who know how to operate the pumping system, the oil hoses and manifold on board a tanker in order to transfer oil cargo from one ship to another. The third category of piracy that is common in this area is 'Kidnapping' of crew members, often targeting smaller offshore supply vessels (OSV).

The number of attacks in the West African region has been relatively constant over the recent years but it is well-known that a large number of attacks are not reported. Sloggett (2013) argues that by anchoring closely together masters gain a degree of mutual protection from pirates. At Lagos anchorage, the risk of hijacking is much lower for the 60 tankers that are at anchor on a typical day compressed into an area of typically 180 - 260 km^2 than those ships at the periphery.

2.2.3 South-East Asia Piracy

Incidents in the South-East Asia region were constant at a level of about 70/year for the years 2007-2009. In 2010, however, incidents doubled with most of the attacks occurring in the Straits of Malacca and Singapore and the South China Sea. Hijacking for ransom is not a common practice among perpetrators in this region as the main aim is to ransack the ship which is usually limited to ships' stores and crews' valuables. In many cases the victim ships were at anchor and the robbers usually lightly armed, often with knives. Upon being spotted by the crew, the robbers often flee the scene without attacking the crew. However, violent attacks where crews were seriously injured also occurred. Although there was a positive downward trend of piracy and armed robbery in the Malacca Strait after the ReCAAP was signed in 2004, the number of incidents flared up again in 2011. This might be related to the international financial crisis in 2008 and its aftermath. The resources of the ReCAAP member States are limited and one could likewise assume that with the success of the early years of ReCAAP complacency had a negative impact. However, unlike Somalia and West Africa, this region has a functioning Maritime Domain Awareness and a wide arsenal of assets for its law enforcement agencies. The ReCAAP mechanism itself is one of the means to quickly organize assistance if a vessel comes under an attack. It is also noteworthy that the risk of being successfully attacked while steaming at full speed is significantly lower in this part of the world than that in the Western Indian Ocean. A ship-owner may therefore focus more on measures to prevent attacks while the ship is at anchor or in port. However, the situation begins to change again with the upward trend of attacks in the Straits of Malacca and Singapore so that masters are well advised to implement some of the BMP, despite their applications for the Somalia Piracy HRA only. The Asia-Pacific Information Fusion Centre (IFC) confirms the latest trend in rising numbers of sea robbery and theft incidents reported by ships in Southern Approaches of the Malacca Strait, Phillips Channel and waters Northeast of Pulau Bintan (IFC, 2014). However, most of these incidents were petty theft in nature.

2.2.4 South America

Table 3 shows that out of a total of 195 incidents in South America from 1 January 2007 to 1 December 2014 only 24 incidents occurred while the ship was steaming. This equals 12% of all incidents. The large majority of attacks were carried out while the ship was at anchor. Most of the 24

incidents occurred while the ship was steaming but one should bear in mind that in some of these incidents the ship had to reduce its speed to a minimum to take a pilot on board with the pilot ladder rigged. In approximately 25% of the attacks, the crew was harmed physically. Hence it can be concluded that the potential risk in this area is largely limited to situations where ships are at anchor or have to reduce speed while approaching port.

Table 3 Incidents in the South America from 1 January 2007 to 01 December 2014
(*Source: IMO GISIS database*)

Ship status	No of incidents	Consequences	Number
Steaming	24	Actual violence against the crew	46
At anchor	140	Threat of violence against the crew	45
Not stated	31	None/not stated	103
		Ship hijacked	1
Total	195		

3. A Proposed Model for Estimating Occurrence Likelihood of Successful Hijacking of a Ship in the Western Indian/East Africa Region

3.1 Background

Most research findings on maritime security involving piracy and robbery have been reported over the past decade. The reported research has targeted two main research topics. One is about the study of the nature of maritime piracy and robbery related activities while the other focuses on technical modelling of them with a view to making decisions on which risk control options to select.

A number of reported studies have been conducted to investigate the nature of maritime piracy and robbery issues from a variety of angles, particularly over the past decade. Psarros *et al.* (2011) estimated the probability of an attack through logistic regression modelling and using the IMO data from 2000 to 2009. One finding is that the success attack rate decreases with vessel size. Another finding is that pirates are aiming at successful attacks regardless of their tactics and the success rate becomes higher as the pirates' capability is improved. A study on the international legal actions against maritime terrorism and its national countermeasure was conducted in order to supress maritime terrorism (Lee, 2006). Issues relevant to international regulations applicable to acts of terrorism at sea were assessed with suggestions of national countermeasures. A risk assessment on maritime terrorism was conducted to investigate the extent of the threat posed by maritime terrorism to commercial ports and shipping in Southeast Asia (Raymond, 2006). Inherent weaknesses present in the maritime transport industry and the terrorist groups in the region with maritime capabilities were identified. Potential consequences of a maritime terrorist attack and possible counter-measures and risk-treatment options were outlined. Globalization has led to a strong growth in seaborne trade; however, it simultaneously increases vulnerability to not only terrorism but also shipping piracy, threatening the world's supply chain. In addition to the direct impact on ships, crews and cargoes, and on the maritime industry and governments, piracy also threatens global seaborne trade, and has an impact on energy security and the environment (Lu *et al*., 2010). A structured formal vulnerability assessment methodology was developed to assess vulnerabilities of maritime supply chains (Berle and Asbjornslett, 2010). Piracy as an unforeseen disruption risk was considered in the study to see how the security of energy supplies can be estimated. PCASP employed by Private Maritime Security Companies (PMSCs) have been contracted by ship owners to protect their vessels against pirates. One argument is that the use of PCASP may not be a long term solution to the piracy problem unless they are used in a coordinated way by ship owners and the international society (Struwe, 2012). Maritime piracy can not only cause supply chain disruption leading to economic consequences but also result in loss of lives, and short- and long-term health problems of seafarers and passengers. While most studies focused on the former, one investigation modelled possible psychological consequences in victims of maritime piracy (Ziello *et al*., 2014). Based on the available occupational health data in

merchant marine and epidemiological data from the International Maritime Bureau (IMB), the health risks associated with the victims of maritime piracy and robbery were assessed (Nebojsa and Eduard, 2014). There are many challenges in maritime security analysis and different approaches have to be used to quantify maritime security risks. Formal Safety Assessment (FSA) developed at the IMO can be applied to maritime security and piracy analysis. Novel uncertainty and risk modelling techniques may be developed and applied to facilitate the transformation of maritime safety culture from a reactive prescriptive scheme towards a proactive goal-setting regime (Yang *et al*., 2013).

On the technical modelling side, some useful studies have been reported. A quantitative risk assessment was conducted on Somali-based maritime piracy through judgemental data with respect to the threat's capability, intent and likelihood of exploiting a ship's vulnerability (Liwang *et al*., 2013). Based on the collected description of the threat, the study analysed the probability of successful boarding; an influence diagram describing the probability of successful boarding was given although no detailed analysis was demonstrated. An agency-based model of maritime traffic in piracy-effected waters was developed for simulating pirate activities and piracy countermeasures (Vanek *et al*., 2013). The complex dynamics of the maritime transportation system threatened by maritime piracy were investigated in order to assess a range of piracy countermeasures. A spatial analysis of shipping routes was conducted to assess shipping safety at the South China Sea through considering many influencing factors such as extreme weather and piracy (Wang *et al*., 2014). The annual and seasonal navigation risk was evaluated along the shipping routes using a fuzzy analytic hierarchy process and geographic information science, and validated by comparison to actual incident reports. A novel fuzzy rule-based reasoning approach was proposed to facilitate quantitative implementation of the International Shipboard and Port Facility Security (ISPS) Code (Yang *et al*., 2014). It can be used either as a stand-alone technique for prioritising vulnerable systems or as part of an integrated decision making method for evaluating the effectiveness of security control options. A Bayesian network (BN) to manage piracy risks of offshore oil fields was proposed to provide a solution to the problem of offshore piracy from the perspective of the entire processing chain covering the detection of a potential threat to the implementation of a response (Bouejla *et al*., 2014). The BN model was used to investigate attack scenarios of offshore installations associated with a number of influencing parameters and identify appropriate countermeasures. It is noted that such influencing parameters' dependency and their interactions were not fully modelled in the study.

Furthermore, researchers have tried to use a variety of advanced models to address challenges with a particular focus on maritime piracy and robbery assessment. These include:

- An agent-based simulation of maritime traffic for choosing a route so as to minimize the probability of hostile encounter (Vanek *et al*., 2010, 2011);
- A sequential defend-attack-defend model for supporting the owner of a ship in managing risks from piracy in the area off the Somali coasts (Sevillano *et al.*, 2012);
- A new multi-agent generative model for the purpose of simulating a maritime piracy situation in order to make counter-piracy decisions (Dabrowski and de Villiers, 2015a);
- A dynamic Bayesian network for context-based behavioural modelling and classification in a maritime piracy situation (Dabrowski and de Villiers, 2015b);
- An agency simulation model and statistical design of experiments for gaining insight into how meteorological and oceanographic forecasts can be used to dynamically predict relative risks for commercial shipping (Esher *et al*., 2010); and
- Collaborative human-centric information support systems for improving the ability of every nation to predict and prevent pirate attacks (Bosse *et al.*, 2013).

While the conducted statistical analysis in Section 2 highlights the need for further study in the area, the above literature review indicates that one of the most powerful tools to analyse risk and to ease the decision-making process can be achieved by utilizing a method of evidence-based reasoning. A BN is a *directed acyclic graph (DAG)* that encodes a *conditional probability distribution (CPD)* at its nodes on the basis of arcs received. It is a method to reason probabilistically (Korb and Nicholson, 2003)

while, at the same time, describing the state of the world. It is capable of replicating the essential features of plausible reasoning (reasoning under conditions of uncertainty) and combine the advantages of an intuitive visual representation with a consistent, efficient and mathematical basis in Bayesian probability (Eleye-Datubo *et al*., 2006). A BN model itself consists of variables which can have different states (e.g. variable A 'Maritime Crime' may take the state of a1: 'Piracy' or a2: 'Human trafficking'). If a node (variable) in a BN has parent nodes, it is accompanied by a Conditional Probability Table (CPT) for each of its states. If a node does not have a parent node, it is accompanied with an unconditional probability table. One of the great advantages of BNs is the easy adaptability of the model so that with every new information the model can be up-dated so as to reflect the real world. The key feature of BNs is that they enable modelling and reasoning about uncertainty (Pearl, 1988). This uncertainty can be due to imperfect understanding of the domain, incomplete knowledge of the state of the domain at the time where a given task is to be performed, randomness in the mechanisms governing the behaviour of the domain, or a combination of these. All the available ship security models are rather intuitive and do not sufficiently take into account the fact that many influencing factors are inter-related and subjective in nature. This study will develop a flexible novel reasoning network based on the Bayesian principles, addressing the dependency between the considered parameters and their subjectivity.

3.2 Major factors influencing the occurrence likelihood of successful hijacking of a ship

Major factors influencing the occurrence likelihood of successful hijacking of a ship in the Western Indian/East African region are identified through a combination of literature review and questionnaires on the piracy/robbery threats. Six experts were consulted through giving the following scenario:

"A ship-owner nowadays is required to meet the requirements of the SOLAS chapter XI-2 and the ISPS Code which requires security measures to be taken in order to minimize the risk of a security incident. Some countries require explicitly anti-piracy provisions in ship security plans (SSPs). A ship-owner then has to decide what measures are appropriate for his/her ship. According to BMP ships can be classified into two main categories: low and high risk ships. Ships with high risk are those with a low operational speed, low freeboard and with a minimum crew to operate the ship. Such ships comprise small tankers, coasters, fishing vessels and some other special-type ships. Your expertise is required for the general risk, not the risk for a particular ship on a particular voyage. Hence your judgment should reflect the overall risk for a common cargo ship transiting the HRA. Some ship owners and masters have taken a wide range of defensive and protective measures, others may have limited their emergency and response plans to a minimum of security measures to respond to pirate attacks."

The background and expertise of the six experts are briefly described as follows:

1. Expert 1 has served for more than 10 years in the Coast Guard as a seagoing officer and has been involved in several projects related to the suppression of maritime piracy and armed robbery. The weight assignment for this expert is 3 from a range of 1 to 5.
2. Expert 2 works on piracy and armed robbery in an international shipping organization with extensive seagoing experience with the UK naval forces. He is involved in the implementation of measures to enhance maritime security in the East African and West African regions and works closely with the naval forces operating in those areas. His expert weight is therefore assigned with the maximum value of 5.
3. Expert 3 has no sea-going experience but has been heavily involved in establishing a coastal monitoring system in the East African region. He has expert knowledge on systems deployed for a functioning maritime domain awareness using modern technologies such as Automatic Identification System (AIS), radar, LRIT and Ship Security Alert Systems (SSAS). His weight is assigned with the value of 1.
4. Expert 4 is an ex-marine officer with vast experience in the Royal Navy. He has served in different ships and different conflict zones, and has worked for a number of international

organisations that are involved in the suppression of piracy and armed robbery in the East African region. His weight is therefore assigned with 5.

5. Expert 5 is the Deputy Director of a well-known piracy international reporting centre that relays piracy incident reports to law enforcement agencies in order to rescue ships that have come under attack. He has an extensive experience as a naval officer and gained further experience with one of the largest port authorities in the world. He is assigned with a weight of 1.
6. Expert 6 is the expert group from the NATO Allied Maritime Command Northwood (NATO Shipping Centre). This credible source comprising several naval officers directly involved in anti-piracy operations in the HRA as NATO security forces is commanded from Northwood. This expert's weight is therefore 5.

The six experts' opinions have been collected and weighted. Suppose expert i's judgement is represented by x_i. The following equation is used to find the combined measure of expert judgements, x.

$$x = \omega_1 \times x_1 + \omega_2 \times x_2 + \omega_3 \times x_3 + \omega_4 \times x_4 + \omega_5 \times x_5 + \omega_6 \times x_6 = \sum_{i=1}^{6} w_i x_i \quad (1)$$

where each ω_i (i = 1, 2, …, 6) is the normalised expert i's weight and $\sum_{i=1}^{6} \omega_i = 1$.

Furthermore, the statistical analysis conducted in Section 2 is also used to identify major factors influencing the occurrence likelihood of successful hijacking of a ship. For example, the speed of the ship is identified as an influencing factor.

Firstly the first level events influencing hijacking of a vessel in the Western Indian/East African region are identified as follows:

1. Defence measures. There are a wide range of defence measures which may vary considerably from ship to ship. Some ships may deploy only passive measures such as barbed wire mounted on the bulwark, 'bumping drums' attached to the ship's hull close to the waterline or electric fences. More sophisticated defence measures are propeller arresters, armed guards or long range acoustic devices. The decision to fit a ship with a particular system depends on its vulnerability.

   This variable has two states of 'Yes' and 'No'.

2. MSCHOA (Maritime Security Centre Horn of Africa). MSCHOA is the coordination centre of the European Naval Force (EUNAVFOR) which is assigned to coordinate the naval forces in their mission to suppress acts of piracy in the Gulf of Aden, the Somali Basin and off the Horn of Africa. Its role is not limited to coordinate the assets provided by the EUNAVFOR operation 'Mission Atalanta' (the US-led Combined Task Force (CTF 150)) alone but to liaise with other cooperation centres and naval forces in the region such as the NATO Combined Task Forces 151 (CTF 151) and ships operating independently. The BMP were developed by the industry and promulgated by the IMO on 14 September 2011 (MSC.1/Circ.1339). BIMCO *et al*. (2011) advised ship owners and masters not only to register with MSCHOA but also to report to United Kingdom Maritime Trade Operations (UKMTO) Dubai [2] and the Marine Liaison Office (MARLO) before entering the region.

   This variable has two states of 'Registered' and 'Unregistered'.

3. Lookout. This variable reflects the probability of having extra personnel on board to function as lookouts. Their main duty is to detect possible pirates at an early stage. Rule 4.28 of Part B of the ISPS Code in conjunction with regulation V/14 of the SOLAS Convention forms the legal basis for safe manning on board ships. The former requires administrations to ensure that ships are sufficiently manned in order to implement the provisions of the Ship Security Plan (SSP) effectively. Further, BMP 4 (BIMCO *et al*., 2011) advises ship masters and companies to increase lookout personnel on board and it is assumed that ships which have the necessary personnel resource comply with this advice.

[2] The UK Maritime Trade Operations (UKMTO) office in Dubai acts as a point of contact for merchant ships with naval forces. UKMTO Dubai also passes information on to MSCHOA.

This variable has two states of ‘Additional’ and ‘No Additional’.

4. Time. Piracy and armed robbery incidents follow a pattern according to the obtained statistics. Generally speaking, there were more incidents during the day time than the ones in the night time in the Western Indian Ocean or the waters of East Africa although this pattern will vary in other locations worldwide. The day time in the regions studied is from 5am to 6pm although the definition of day time in other regions may be different.

   This variable has two states of ‘Daytime’ and ‘Night’.

5. Visibility. Although no statistical data for the visibility in this area has been analysed, the professional literature for masters (UK MoD-HD, 1987; UK Navy-Hyd, 1967) indicates that the visibility is mainly good or very good, although dust may reduce the visibility in summer in the region around the Persian Gulf and the Gulf of Aden. As outlined in (UK MoD-HD, 1987) the visibility deteriorates between June and August to less than 5nm about 1 out of 4 or 5 days on the African side and 1 out of 2 days on the Arabian side. The visibility variable is less important for this sea area but this model may be modified to apply to other sea regions where the visibility is more significant and thus has been retained here.

   This variable has three states of ‘Good’, ‘Moderate’ and ‘Poor’.

6. Season. The monsoon season is known for winds and high waves and thus poses restrictions on the operation of the small twin-engine fishing skiffs pirates use (Bevege and Hassan, 2009). According to NRL Monterey, Marine Meteorology Division (2002) the annual weather patterns for the Arabian Sea and Gulf of Aden are divided into four seasons:

   i. Northeast Monsoon, December to March.

   ii. Transition season, April and May.

   iii. Southwest Monsoon, June to September.

   iv. Transition season, October and November.

   A slightly different pattern on the monsoon seasons can be found in Miller (2010) where it is claimed that the Southwest Monsoon lasts only until August. Further, Bergen Risk Solutions (2010) states that the Northeast Monsoon only lasts until February, not March as indicated by NRL Monterey, Marine Meteorology Division (2002).

   This variable has two states of ‘Monsoon’ and ‘Calm’.

7. Freeboard. The freeboard is defined in the International Convention on Load Lines, 1966 as the distance measured vertically downwards amidships from the upper edge of the related load line (IMO, 1966). The term load line refers to the summer load line, the winter load line and so forth. The freeboard of a ship depends not only on its size but also on its purpose. A fully laden PANAMAX-bulk carrier, despite a tonnage of approximately 75,000 dwt and with a depth of 18.70m at a draught of 13.55m has a freeboard of 5.15m only (BRL-Shipping, 2004).

   This variable has three states of ‘High’, ‘Medium’ and ‘Low’.

   The type of ship, gross tonnage and draught can be analysed to assign ‘High’, ‘Medium’ or ‘Low’ to the freeboard variable. As bulk carriers are minimum freeboard ships (Blakemore, 2004) the categories for them have been determined as follows:

   i. Low freeboard: bulk carriers/tankers of gross tonnage $\leq$ 20,000 gt.

   ii. Medium freeboard: bulk carriers/tankers of gross tonnage > 20,000 gt and $\leq$ 100,000 gt.

   iii. High freeboard: bulk carriers/tankers of gross tonnage > 100,000 gt.

   For containerships and general cargo ships a similar approach is applied. The hijacked containership *HANSA STAVANGER* has a maximum depth of 10.58m (Clarksons, 2010) and would at a draught of 5.50m have a freeboard of approximately 5m. This would, according to the assessment made for bulk carriers, qualify as a medium-freeboard ship.

i. Low freeboard: container/general cargo of gross tonnage ≤ 15,000 gt.

ii. Medium freeboard: container/general cargo of gross tonnage > 15,000 gt and ≤ 30,000 gt.

iii. High freeboard: container/general cargo of gross tonnage > 50,000 gt.

For vehicle carriers, 'High' is always assigned whereas for supply ships, tugs, dhows, yachts and other small ships, 'Low' is assigned.

8. Speed. The speed of a ship is a significant factor to assess the risk of a ship when under attack. It is known that ships which are capable of making a speed of 15 knots or more have not been successfully attacked unless gross negligence of good seamanship had been the root factor.

   This variable has three states of 'At anchor', '< Fifteen knots' and '≥ Fifteen knots'.

9. Guards. The estimation of this parameter can be carried out based on the consultation with ship owners and other sources (Leander, 2010). It can be assumed that the number of accredited armed security personnel on board merchant ships will significantly increase with the promulgation of the new ISO Standard 28007 for PMSCs which is part of the ISO 28000 series on maritime security.

   This variable has three states of 'Armed', 'Not armed' and 'No guards'.

10. Naval Support. This variable stands for the military response time (i.e. the time necessary to render assistance to the ship under threat). The fastest way in many cases is the dispatch of a helicopter with special forces on board. Other means are navy ships' own fast boats but this would require a very close proximity to the victim ship. Since there are many military forces in the region, such as NATO, the EUNAVFOR and a number of countries which operate only under their own country's mandate such as Russia, Iran and China, no central register with all such information is available. The rationale for this is certainly linked to the confidentiality of military operations. However, a first step for closer co-operation has been made by establishing SHADE, the Shared Awareness and Deconfliction forum which is attended by the military forces acting in the region such as NATO and EUNAFFOR. The aim is to co-operate with each other and to exchange information at an operational level. Apart from the fact that no data is available to researchers on response time it is easy to comprehend that any such assistance depends on the distance of a navy ship and the victim ship. A ship in the Gulf of Aden while being part of a group transit scheme can expect close proximity to navy ships whereas a naval ship closer to the Indian sub-continent might be hundreds of miles away. However, naval support in close distance provides no guarantee for not being successfully attacked. The boarding of the general-cargo ship *SUEZ* (Matthews and Meade, 2010) in the IRTC within 5 minutes by pirates shows that even the heavily protected Internationally Recommended Transit Corridor (IRTC) in the Gulf of Aden is not an entirely safe area.

    This variable has three states of 't15', 't30' and '> t30'. The first state (t15) reflects situations where military support is rendered within 15 minutes, the second state (t30) reflects assistance rendered between 16 and 30 minutes and the third state (> t30) is for all other situations.

Secondly, the intermediate level events are identified in a way that each of them is influenced by a combination of some first level events.

1. Ship type. This variable has 2 parent nodes, the variables 'Freeboard' and 'Speed'. In many cases small and fast ships have a small freeboard (e.g. small container feeders and passenger ship catamarans) whereas slow-steaming ships usually have a higher freeboard (large bulk carriers, super tankers). However, there are also ship-designs that contradict this general assumption such as fast super-large post-panamas containerships or fast RoPax-ferries which have a very high freeboard while often capable of steaming more than 25 knots. There are also small-freeboard ships that travel at low speeds such as tugs or some coasters. However, in the context of maritime piracy modelling, the dependency between "Freeboard" and "Speed" is considered negligible.

   This variable has two states of 'High risk' and 'Low risk'.

2. Environmental condition. This variable has 3 parent nodes, the variables 'Time', 'Visibility' and 'Season'. The exact environmental condition for each single piracy case comprising visibility and sea state are not included in any records or databases (e.g. GISIS), nor was it possible to decide exactly on the day/night divide in each case. It is known that pirates prefer to attack at dawn but to identify the daylight in each single case was not feasible in this study. Therefore it is necessary to make approximations or use techniques such as Monte Carlos simulation when estimating this parameter (Pristrom, 2013).

   This variable has two states of 'Favourable' and 'Poor'.

3. BMP. This variable has 3 parent nodes, the variables 'Defence measures', 'MSCHOA' and 'Lookout'. BMP to deter piracy off the coast of Somalia and in the Arabian Sea are developed and continuously updated by the shipping industry. The IMO welcomes this effort of the industry and promulgates the BMP as MSC.1 Circulars which can be seen as a complementary guidance to existing IMO recommendations and guidelines. As the measures of the BMP vary, depending upon the ship type, compliance with the BMP is to be assessed individually (BIMCO *et al*., 2011).

   This variable has two states of 'Yes' and 'No'.

Thirdly, a third level event 'Attack' is determined by the second level events. This variable has three parent nodes, the variables 'Ship Type', 'Environmental Condition' and 'BMP'. It describes the status of a vessel in the HRA being attacked given the application of BMP, the prevailing weather conditions and the vessel's characteristics. This variable has two states, i.e. 'Yes' and 'No'.

Fourthly, the last (fourth) level events are identified. They can be explained as follows:

1. 'Hijacked'. This variable has three parent nodes, the variables 'Naval Support', 'Guards' and 'Attack'. This variable describes the status of the vessel in the HRA being hijacked given the available naval support, the use of guards on the ship and the status of the ship being attacked.

   This variable has two states of 'Yes' and 'No'.

2. 'Unsuccessful Attempt'. The variable 'Attack' either leads to the vessel being hijacked or to an unsuccessful attempt. If the variable 'Attack' takes the state 'No' then the variable 'Unsuccessful Attempt' is the consequence. Thus the decision not to attack concurs with the variable 'Unsuccessful Attempt' as the pirates are targeting any ship. Nevertheless, a ship may be attacked but not hijacked, especially in cases where pirates do not attack with the aim to demand ransom for a ship but only want to steal valuable on board.

   This variable has two states of 'Yes' and 'No'.

3.3 A proposed model

A model for predicting the probabilities of a ship being attacked, hijacked and unsuccessful attempt in the Western Indian/East African region is developed by considering the events at four levels and also their relationships described in Section 3.2. The model is shown in Figure 1. In the BN model shown in Figure 1, the level 1 events described in Section 3.2 are root nodes representing original causes ('Defence Measure', 'MSCHOA', 'Lookout', 'Speed', 'Freeboard', 'Time', Visibility', 'Season', 'Naval Support', and 'Guards'). The level 4 events are leaf nodes representing the final effects ('Hijacked' and 'Unsuccessful Attempt'). The level 2 events 'Ship Type', 'Environmental Condition' and 'BMP', and level 3 event 'Attack' are intermediate events linking up the root nodes and leaf nodes. In Figure 1, each of the three second level nodes 'Ship Type', 'Environmental Condition' and 'BMP' has their own parent root nodes. Level 3 node 'Attack' has three parents which are also intermediate nodes. Leaf node 'Hijacked' has three parents, two of which are root nodes ('Naval Support', and 'Guards') and the other is an intermediate node ('Attack'). 'Unsuccessful Attempt' has an intermediate node ('Attack') as its parent. When executing the model in Section 4, the probabilities of each node will be taken from a statistical analysis or quantified by domain experts with sufficient knowledge and professional experience.

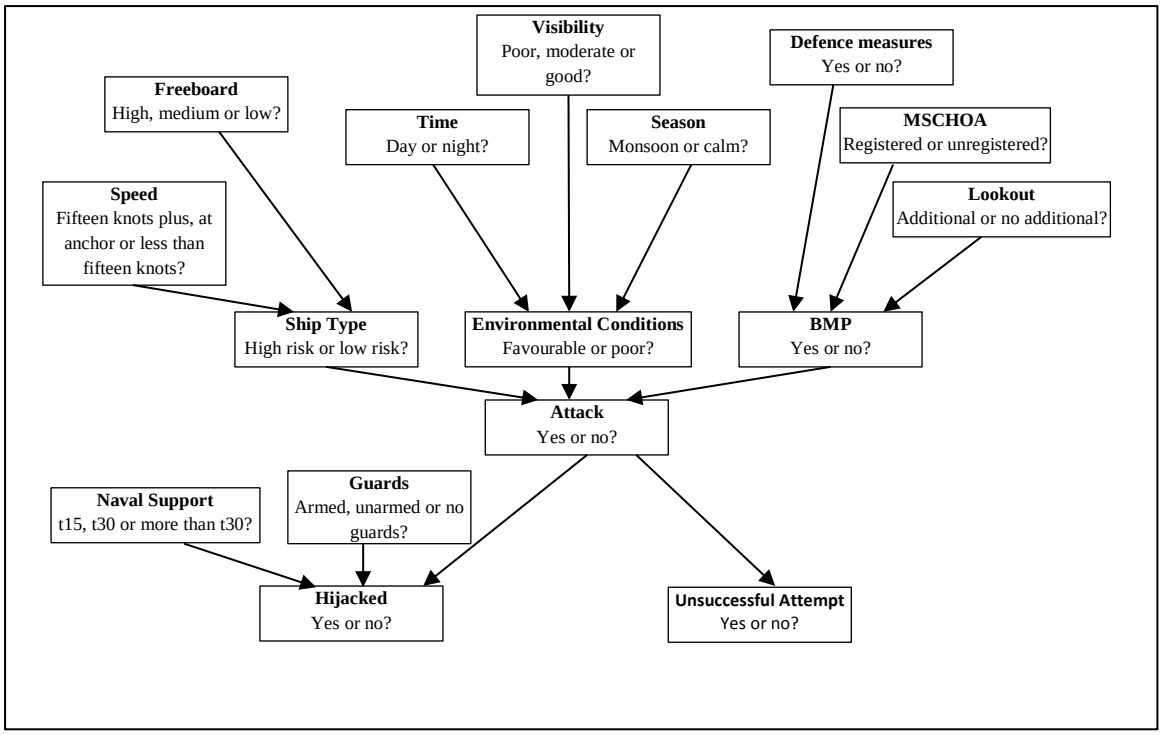

Figure 1 BN model of pirate attack and hijacking

No matter how complex a BN may appear its nodes will always be linked through a serial connection, a diverging connection or a converging connection. D-separation can be defined as a configuration in a causal network where two variables A and B are separated, through all paths, by an intermediate variable I, and either of the following is true (Jensen and Nielsen, 2007):

- The connection is either serial or diverging and the state of I is known, or;
- The connection is converging and the state of I or any of its descendants is not known.

A d-separation test has been undertaken to demonstrate that the model shown in Figure 1 is a simplified network without superfluous nodes involved.

3.4 Partial validation of the model

Given the lack of sufficient statistical data and the high level of uncertainties in data, it is challenging to fully validate the proposed model. Lack of available benchmarks in the literature and also in the domain makes the full validation even more challenging. A sensitivity study (SA) is therefore used to provide a degree of confidence that the model has been built correctly and is working as intended. SA is essentially a measure of how responsive the output of a model is to variations in the inputs. If the model shown in Figure 1 is reasonable, then the following listed axioms must be satisfied at least (Jones *et al*., 2009):

1. Axiom 1. A slight increase/decrease in the prior probabilities of each parent node should certainly result in the effect of a relative increase/decrease of the posterior probabilities of the child node.
2. Axiom 2. Given the variation of probability distributions of each parent node, its influence magnitude to the child node values should keep consistency.
3. Axiom 3. The total influence magnitudes of the combination of the probability variations from x attributes (evidence) on the values should be always greater than the one from the set of x-y ($y \epsilon x$) attributes (sub-evidence).

4. An Illustrative Example

The likelihood of a ship transiting through the Western Indian/East African region is used to demonstrate and validate the proposed BN model. Both expert judgements using the six experts described in Section 3 and statistical data from sources such as the IMO GISIS are used to provide quantitative inputs into the BN model. The six selected experts described in Section 3.2 were given questionnaires for obtaining the conditional probabilities in the CPTs of the nodes in the BN where statistical data is not available (e.g. the CPT for "Attack"). Their judgemental estimates were synthesised using Equation (1) with their weights as 0.2273 (5/22), 0.2273 (5/22), 0.0454 (1/22), 0.0454 (1/22) and 0.2273 (5/22) respectively. The consensus among their judgements to a large extent verify the prior probabilities in such CPTs.

4.1 Data collection and analysis for the nodes of the BN model

4.1.1 Assignment of data for the root nodes

1. 'Defence Measure'

There is a lack of statistical data for probability assignment into this node. This node's 'Yes' and 'No' states are assigned probabilities of 0.75 and 0.25 respectively through expert judgements (Pristrom, 2013).

2. 'MSCHOA'

Approximately 80% of the ships transiting the area register with MSCHOA and the remaining 20% thus fail with the BMP developed by the industry and promulgated by IMO through MSC.1/Circ.1339 (Farrington 2009; Pristrom, 2013).

3. 'Lookout'

BMP 4 (BIMCO *et al*., 2011) advises ship masters and companies to increase lookout personnel on board and it is assumed that ships which have the necessary personnel resource comply with this recommendation. Given that only 80% of ships follow the BMP, this node's 'Additional' and 'No Additional' states are assigned with probabilities of 0.8 and 0.2 respectively.

4. 'Time'

Out of 579 incidents with the sufficient information relating to 'Time' reported in GISIS, 359 occurred during the time period between 5am and 6pm, henceforth referred as 'daytime'. 220 incidents occurred during the remaining time. This node's 'Daytime' and 'Night time' are assigned with probabilities of 0.62 and 0.38 respectively.

5. 'Visibility'

The visibility is dominantly good or very good in this sea area throughout the year. The states 'Good', 'Moderate' and 'Poor' of this node are assigned with probabilities of 0.80, 0.15 and 0.05 through expert judgement respectively.

6. 'Season'

Out of 800 incidents relating to 'Season' in GISIS collected for ten and a half years, 361 out of 800 took place during the Monsoon period. 'Monsoon' and 'Calm' of this node are assigned with probabilities of 0.45 and 0.55 respectively.

7. 'Freeboard'

Based on 604 incidents with the sufficient information relating to 'Freeboard' in GISIS, 12% is assigned to 'High", 38% to 'Medium' and 50% to 'Low'.

8. 'Speed'

The 551 incidents (with sufficient information relating to 'Speed') reported in GISIS for a period of three and a half years have been analysed. Out of these 551 incidents, there were 96 at anchor, 370 running at a speed of 15 knots or more, and 85 running at a speed of less than 15 knots. This node's '≥

Fifteen knots', '< Fifteen knots' and 'At anchor' are assigned with probabilities of 0.155, 0.175 and 0.670, respectively.

9. 'Guards'

According to security specialist Cook (Leander, 2010), 12% to 15% of ships passing through the Gulf of Aden deploy security companies. As a result, the probability of 'No guards' of this node is assigned with 0.865 (i.e. 1 - the middle value of the range from 12% to 15%). It is believed that two third of these are armed. Cook's estimates were based on the consultation with ship owners and other sources (Leander, 2010). Thus 'Armed' and 'Not armed' of this node are given 0.09 (i.e. 0.135×2/3) and 0.045 (i.e. 0.135×1/3) respectively.

10. 'Naval Support'

The probabilities associated with the three states 't15', 't30' and '> t30' of this node are assigned through assessing the reports from IMO reported by various member States and commercial credible entities such as the International Maritime Bureau (IMB) together with expert judgement. 't15', 't30' and '> t30' of this node are given 0.05, 0.10 and 0.85 respectively.

4.1.2 Assignment of data for the intermediate nodes and leaf nodes

1. 'Ship Type'

Through investigating the data in GISIS reported for three and a half years, 554 incidents have been analysed to produce the CPT for "Ship Type" as shown in Table 4. It is worth noting that the freeboard values for 'High' and 'Medium' are merged as one value in GISIS while in the proposed BN model, 'Freeboard' has three states 'High', 'Medium' and 'Low'. It is also worth noting that the statistical data may present a paradox here as the data suggests that the risk of being involved in a piracy accident might be higher when steaming than at anchor. The simple reason for this lower risk is due to the very limited number of ships at anchor in the region as this would contradict the BMP. For analysing the general risk this fact, however, reflects reality.

Table 4 CPT for 'Ship Type'

Speed	Fifteen knots plus			Less than fifteen			At anchor		
Freeboard / Ship Type	High	Medium	Low	High	Medium	Low	High	Medium	Low
High risk	0.103	0.103	0.2	0.063	0.063	0.455	0.047	0.047	0.132
Low risk	0.897	0.897	0.8	0.937	0.937	0.545	0.953	0.953	0.868

2. 'Environmental Condition'

The CPT for 'Environmental Condition' shown in Table 5 is assigned through studying the GISIS data together with approximate calculation and expert judgement (Pristrom, 2013). The poor visibility can be compared with the restricted visibility conditions as described in the Collision Regulations for Ships (COLREGS). Suppose two adverse states would give a 20% reduction in pirate attacks due to added complication to pirate operations. 55% of all attacks occurred during the day and that 45% of all recorded incidents took place during monsoon winds. If the visibility is poor then the percentage of a favourable environmental condition is equal to 1%. If all three parents are equally weighted, then the probability value for the state 'Favourable' of 'Environmental Condition' is calculated as 0.55 × 1/3 + 0.45 × 1/3 + 0.01 × 1/3 - 0.2 = 0.14 (Pristrom, 2013). It can be seen in Table 5 that P('Env. conditions' = 'Favourable' | 'Time' = 'Day', 'Season' = 'Monsoon', 'Visibility = 'Poor') is 0.14.

Table 5 CPT for ‘Environmental Condition’

Time	Day						Night					
Season	Monsoon			Calm			Monsoon			Calm		
Visibility / Env. Condition	Poor	Mode-rate	Good	Poor	Mode-rate	Good	Poor	Mode-rate	Good	Poor	Mode-rate	Good
Favourable	0.14	0.25	0.6	0.37	0.33	0.63	0	0.12	0.37	0.14	0.25	0.56
Poor	0.86	0.75	0.4	0.63	0.67	0.37	1	0.88	0.63	0.86	0.75	0.44

3. ‘BMP’

The CPT for ‘BMP’ shown in Table 6 was assigned using the judgements from the six described domain experts (Pristrom, 2013).

Table 6 CPT for ‘BMP’

Defence Measures	Yes				No			
MSCHOA	Registered		Not registered		Registered		Not registered	
Lookout / BMP	Add.	No add.	Add.	No add.	Add.	No add.	Add.	No add.
Yes	0.93	0.67	0.69	0.39	0.43	0.17	0.18	0.04
No	0.07	0.33	0.31	0.61	0.57	0.83	0.82	0.96

4. ‘Attack’

The CPT for ‘Attack’ shown in Table 7 was also assigned using the judgements from the six described domain experts (Pristrom, 2013).

Table 7 CPT for ‘Attack’

Ship Type	High risk				Low risk			
Environmental Condition	Favourable		Poor		Favourable		Poor	
BMP / Attack	Yes	No	Yes	No	Yes	No	Yes	No
Yes	22.1	24.9	12.5	15.7	19.6	23.9	5.5	7.7
No	77.9	75.1	87.5	84.3	80.4	76.1	94.5	92.3

5. ‘Hijacked’

The CPT for ‘Hijacked’ shown in Table 8 was assigned using the judgements from the six described domain experts (Pristrom, 2013).

Table 8 CPT for ‘Attack’

Attack	Yes									No								
Naval Support	t15			T30			>t30			t15			T30			>t30		
BMP	Armed	Unarmed	No	Armed	Unarmed	No	Armed	Unarmed	No	Armed	Unarmed	No	Armed	Unarmed	No	Armed	Unarmed	No

Hijacked																		
Yes	0.06	0.22	0.3	0.14	0.3	0.36	0.22	0.41	0.47	0	0	0	0	0	0	0	0	0
No	0.94	0.78	0.7	0.86	0.7	0.64	0.78	0.59	0.53	1	1	1	1	1	1	1	1	1

6. 'Unsuccessful attempt'

The variable 'Attack' either leads to the vessel being hijacked or to an unsuccessful attempt. If the variable 'Attack' takes the state 'no' then the variable 'Unsuccessful Attempt' is the consequence. A ship may be attacked but not hijacked, especially in cases where pirates do not attack with the aim to demand ransom for a ship but only want to steal valuable on board. Therefore 10% of the cases where an attack is carried out may not lead to a successful attempt. The CPT for 'Unsuccessful attempt' is shown in Table 9.

Table 9 CPT for 'Unsuccessful attempt'

Attack / Unsucc. Attempt	Yes	No
Yes	0.9	1
No	0.1	0

4.2 Results and partial model validation

Figure 2 shows the results for the BN example. According to the model, the general likelihood of a ship being attacked in the Western Indian/East African region is 11.8% per passage. The value (11.8%) is obtained given that the prior probabilities of the four root nodes "time", "season", "free board" and "speed" are based on the statistics of the reported incidents. For example, in terms of "speed", if we define the population as "all reported incident" to analyse its prior probability, it is 67% "at anchor", 15.5% "<15 knots" and 17.5% ">15 knots". If we change the population from "all reported incidents" to "the vessels passing through", the probability of ">15 knots" will significantly increase and consequently the likelihood of a ship being attacked will be reduced accordingly. Such an attack may be abandoned at an early stage when the attackers become aware of the defence measures on board or the attack is not successful because the ship is out-manoeuvring the attacking skiffs. The variable 'Hijacked' then reflects the risks of being hijacked when under attack. The BN then suggests that the likelihood of a ship being hijacked is about 4.4% in the area given circumstances of the influencing factors such as naval support and use of guards.

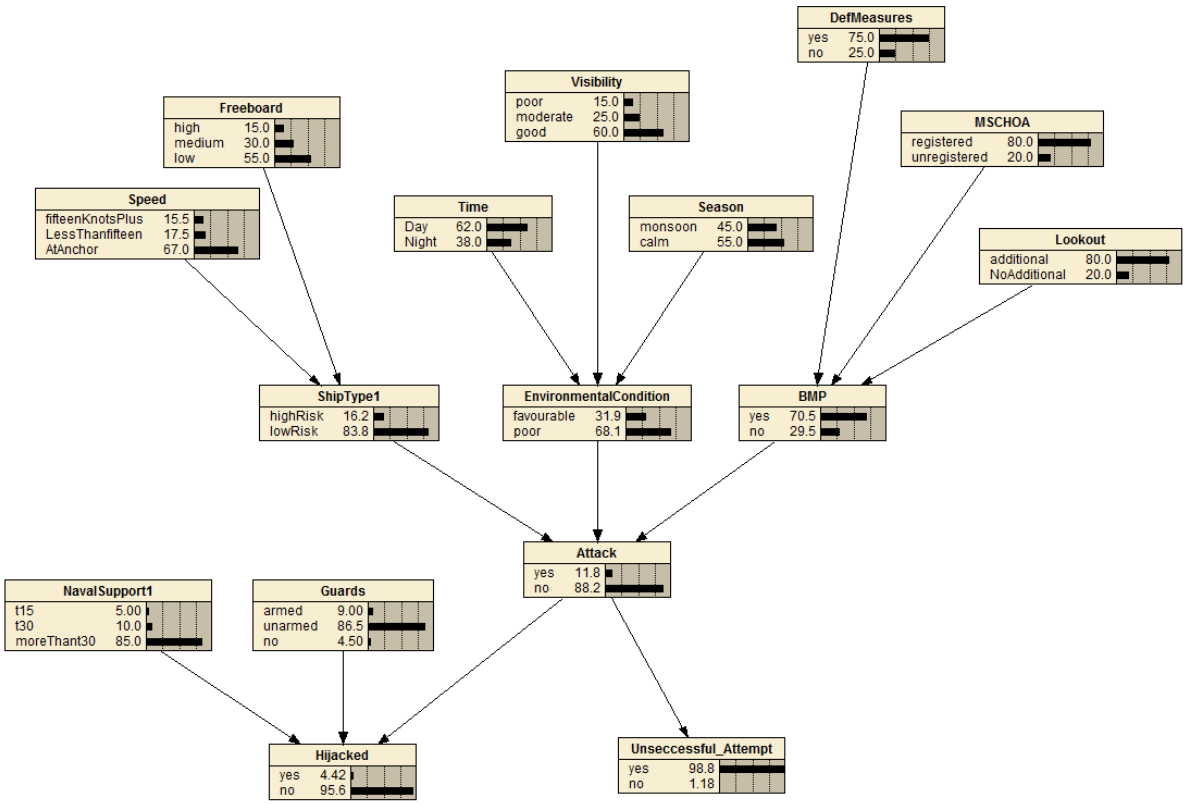

Figure 2 The results from the BN model

Test of Axiom 1

Table 10 shows that the BN behaves as it is expected and changing the value of each parent node of 'Attack' changes the belief of the query variable itself as it would be in real life. If the ship becomes a high-risk ship, the probability of an attack increases from 11.8% to 16.5%. Similarly if the ship is a low-risk ship, the probability of an attack reduces to 10.8%. If the environmental conditions are favourable, the probability of attack increases from 16.2% to 21.2%. Similarly, if the environmental conditions are poor, then the probability of being attacked is down to 7.3%. If the BPM are not applied, the probability of attack increases from 11.8% to 13.8%. Similarly, if the BMP are applied, then the probability of being attacked is down to 10.9%. Table 11 shows the same conclusion for the node 'Hijacked'.

Table 10 Test of Axiom 1 for the node 'Attack'

Ship Type High risk probability	Attack Yes
0.162 1 0	0.118 0.165 0.108
Env. Conditions Favourable probability	Attack Yes
0.319 1 0	0.118 0.212 0.073
BMP not applied probability	Attack Yes
0.295 1 0	0.118 0.138 0.109

Table 11 Changes of node ‘Hijacked’ due to changes of its parent nodes

Armed Guards		Hijacked
BN value	0.09	0.044
	1	0.024
	0	0.053
Naval support < 15 min (t15)		
BN value	0.05	0.044
	1	0.024
	0	0.047

Test of Axiom 2

Figure 3 shows the change of probabilities for the node ‘Attack’ in accordance to changes made to its parent variables ‘Ship Type’, ‘Environmental Condition’ and ‘BMP’. The shapes of the curves indicate that there are no outliers or sharp-kneed features. A consistent change of probabilities for ‘Attack = Yes’ due to change of probabilities of ‘Ship Type = High risk’, ‘Environmental Condition = Favourable’ or ‘BMP = No’. A similar observation can be made when analysing the node of ‘Hijacking’ in Figure 4.

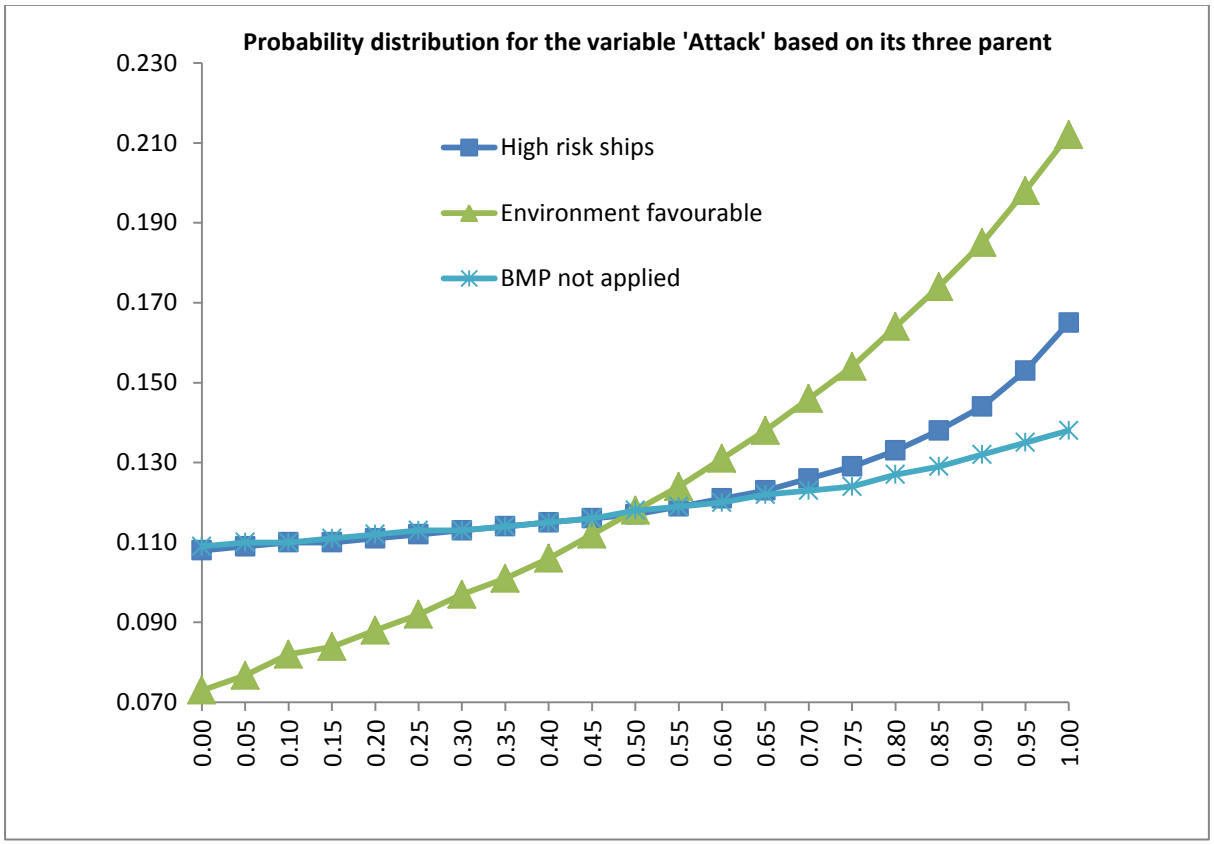

Figure 3 Test of Axiom 2 for the node ‘Attack’

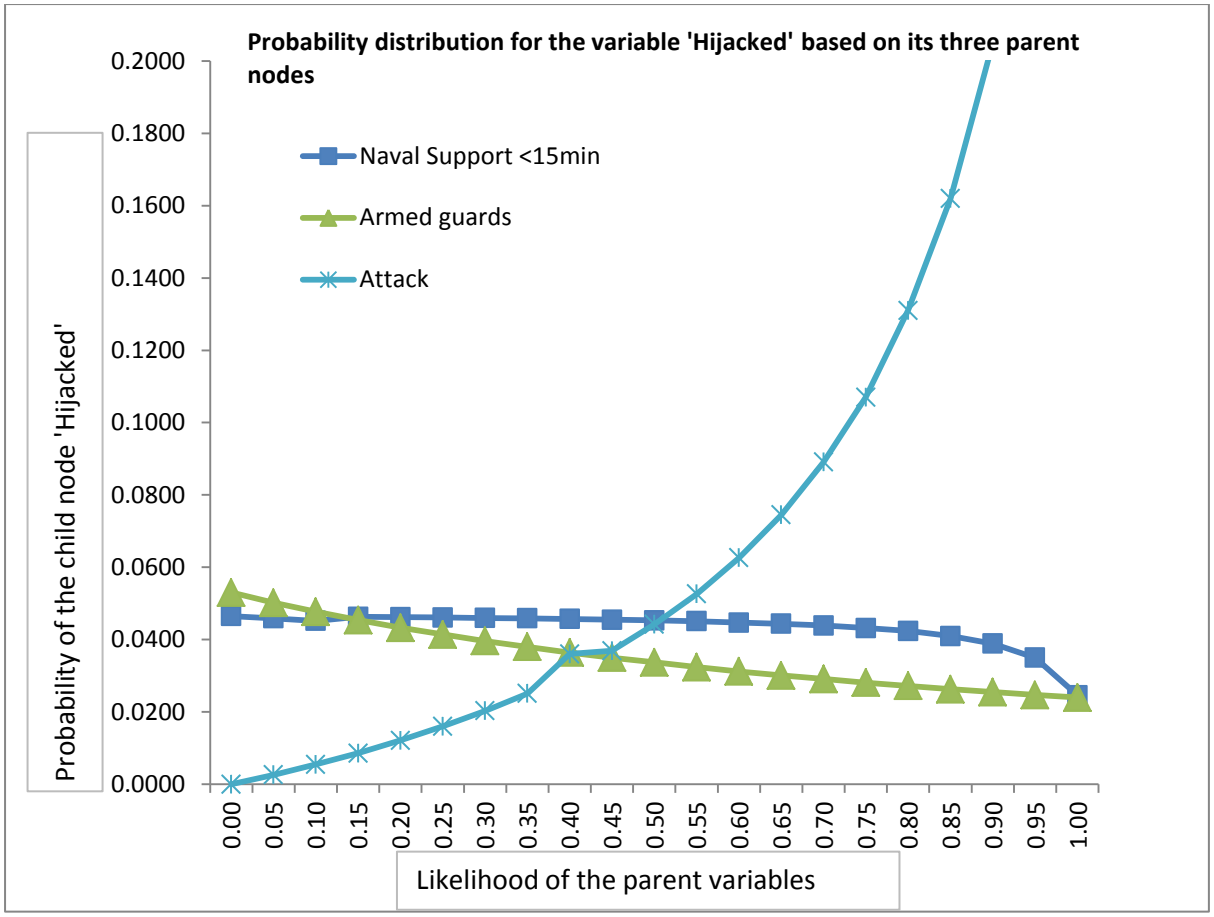

Figure 4 Test of Axiom 2 for the node 'Hijacked'

Test of Axiom 3

Axiom 3 requires that sub-evidence should have less influence on the values of a node than evidence received from the parent nodes has. 'BMP' (evidence) is composed of 'Defence measures', 'MSCHOA' and 'Lookout' (sub-evidence). When each sub-evidence of 'Defence measures = No', 'MSCHOA = Unregistered' and 'Lookout = No Additional' is entered, the probabilities of 'Attack = Yes" are 0.139, 0.124 and 0.129 respectively. When 'Defence measures = No', 'MSCHOA = Unregistered' and 'Lookout = No Additional' are entered into the model, the probability of 'Attack = Yes" is 0.212. This is in line with Axiom 3. Further tests are also conducted for 'Environmental Conditions' and 'Ship Type" together with their corresponding sub-evidence. All the obtained results are in harmony with Axiom 3.

4.3 Sensitivity study

As this model mainly serves to study the threat of an attack and the consequent hijacking, these two variables have been analysed in their sensitivity to other variables. Table 12 obtained through the software package NETICA shows the results of the sensitivity analysis for the variable 'Attack'. The second column of Table 12 introduces the term entropy reduction (Norsys Software Corp 2010; Pristrom 2014). Entropy is a term used in information technology and can be regarded as an indicator of how disordered a dataset is. Entropy is described as a value that, when increased, can be interpreted as increase in uncertainty of a dataset which would then require more information in order to describe that data. The reason for calculating the entropy of probability distributions is to compare different probability distributions that have been derived from observed data. The expected reduction in

entropy for the nodes shown in Figure 2 is displayed in Table 12. It shows how sensitive the node 'Attack' is to its parent nodes, although the figure only considers the four parent nodes 'Ship Type', 'Environmental Condition', 'Time' and 'BMP'. These four nodes have been singled out after analysing NETICA's results derived from Table 12 which clearly reveal that these nodes are the most significant for changing the probabilities of the node 'Attack', bearing in mind that 'Hijacked' and 'Unsuccessful Attack' are the consequences of 'Attack' and therefore not considered to be of value when analysing the measures that lead to an attack. The nodes that influence the query variable most can be identified through looking at their entropy reduction. As can be seen further from Table 12, those nodes that influence the variable 'Attack' most significantly can be found and used in the analysis represented in Tables 13 and 14. The most significant single node is therefore the variable 'Environmental Condition' which may lead to a likelihood for an attack as low as approximate 7.5% or up to a maximum of 21.2%. Mainly responsible for this impact is the parent node 'Time' of the node 'Environmental Condition' which as a single factor can change the probability by 3.5% alone. For the node 'Hijacked' the most significant node is naturally the node 'Attack' as there are very few cases where a ship is hijacked without being attacked in the way 'Attack' is defined here. Because of 'Attack' being the main influencing variable for the node 'Hijacked' it is apparent that the parent nodes of the former contribute significantly to the probabilities about 'Hijacked'. Hence it is the node 'Environmental condition' that can cause a probability range of 13.7% for the variable 'Attack'.

Table 12 Sensitivity of the node 'Attack' (Entropy reduction)

Node	Entropy Reduction (%)
Attack	100
Hijacked	28.5
Unsuccessful Attempt	7.09
Environmental Condition	5.04
Ship Type	0.57
Time	0.369
BMP	0.225
Season	0.202
Visibility	0.0753
Freeboard	0.0742
Defence Measures	0.0502
Lookout	0.0118
MSCHOA	0.0103
Speed	0.0086
Naval Support	0
Guards	0

Table 13 Sensitivity of node 'Attack'

Sensitivity of the node 'Attack'			Yes: 11.9%		No: 88.1%		
BN-value	Environmental Condition – Favourable [%]					Range [%]	Min	max
31.9%	0	25	50	75	100	13.7	7.5	21.2
	0.0747	0.0933	0.119	0.155	0.212			

BN-value	Ship Type – High Risk Ships [%]					Range [%]	Min	max
16.2%	0	25	50	75	100	5.7	10.8	16.5
	0.108	0.112	0.119	0.131	0.165			
BN-value	Time – Day [%]					Range [%]	Min	max
62.0%	0	25	50	75	100	3.5	10.5	14.0
	0.14	0.128	0.119	0.111	0.105			
BN-value	BMP – Yes [%]					Range [%]	Min	max
70.5%	0	25	50	75	100	2.9	11.0	13.9
	0.139	0.126	0.119	0.114	0.110			

Table 14 Sensitivity of the node ‘Hijacked’

Sensitivity of the node ‘Hijack’		Yes: 4.5%		No: 95.5%				
BN-value	Attack – Yes [%]					Range [%]	Min	max
11.9%	0	25	50	75	100	37.6	0	37.6
	0	0.0161	0.0446	0.108	0.376			
BN-value	Environmental Condition – Favourable [%]					Range [%]	Min	max
31.9%	0	25	50	75	100	13.7	7.5	21.2
	0.0747	0.0933	0.119	0.155	0.212			
BN-value	Ship Type – High Risk Ships [%]					Range [%]	Min	max
16.2%	0	25	50	75	100	5.7	10.8	16.5
	0.108	0.112	0.119	0.131	0.165			
BN-value	BMP – Yes [%]					Range [%]	Min	max
70.5%	0	25	50	75	100	2.9	11.0	13.9
	0.139	0.126	0.119	0.114	0.110			

Practical considerations call for an analysis of the effect of the other two parent variables of 'Hijacked', i.e. 'Naval support' and the deployment of 'Guards'. The worst case scenario for a ship under attack would be that there are no guards at all on board and no assistance is rendered by naval forces within 30 minutes. The risk of being hijacked in such a case is believed to be 5.58 %. On the other hand, if the ship has armed guards on board and naval forces are available within 15 minutes after being informed of an attempted attack, the risk of being hijacked decreases to 0.71%. The BN behaves as expected to the changes made and are in line with Axiom 1. The reduction from 5.58% to 0.71% due to the presence of 'Naval support' and 'Guards' also in part justifies the need of the recommendations to be discussed in Section 5.

The model developed can be used to update the estimation of the likelihood of a ship being hijacked in the Western Indian/East African region when any new evidence becomes available. The outcomes from the model can be used by maritime stakeholders to make decisions in their operations. In particular, decisions as to how maritime piracy and robbery is suppressed can be made in a cost-effective way. An example is to deploy effectively naval forces to achieve the best reduction in piracy and robbery incidents/accidents in the region. Another example is that the obtained estimates of maritime security risks from the formulated model can help the industrial stakeholders respond to maritime piracy and robbery. Implementation of maritime security measures such as BMP can be determined or justified through a cost benefit analysis incorporating the results obtained from the proposed model.

More influencing variables can be easily added to the model if considered necessary without having to re-design it entirely. The model only requires the prior probabilities of the newly added nodes and those they influence, having the remaining part of the network unchanged. For example, two parents "Type of ship" and "Cargo" can be added to "Freeboard"; "Hijacked" can have one more parent "Cargo loaded" as shown in Figure 5. Figure 5 is an expanded version of Figure 2.

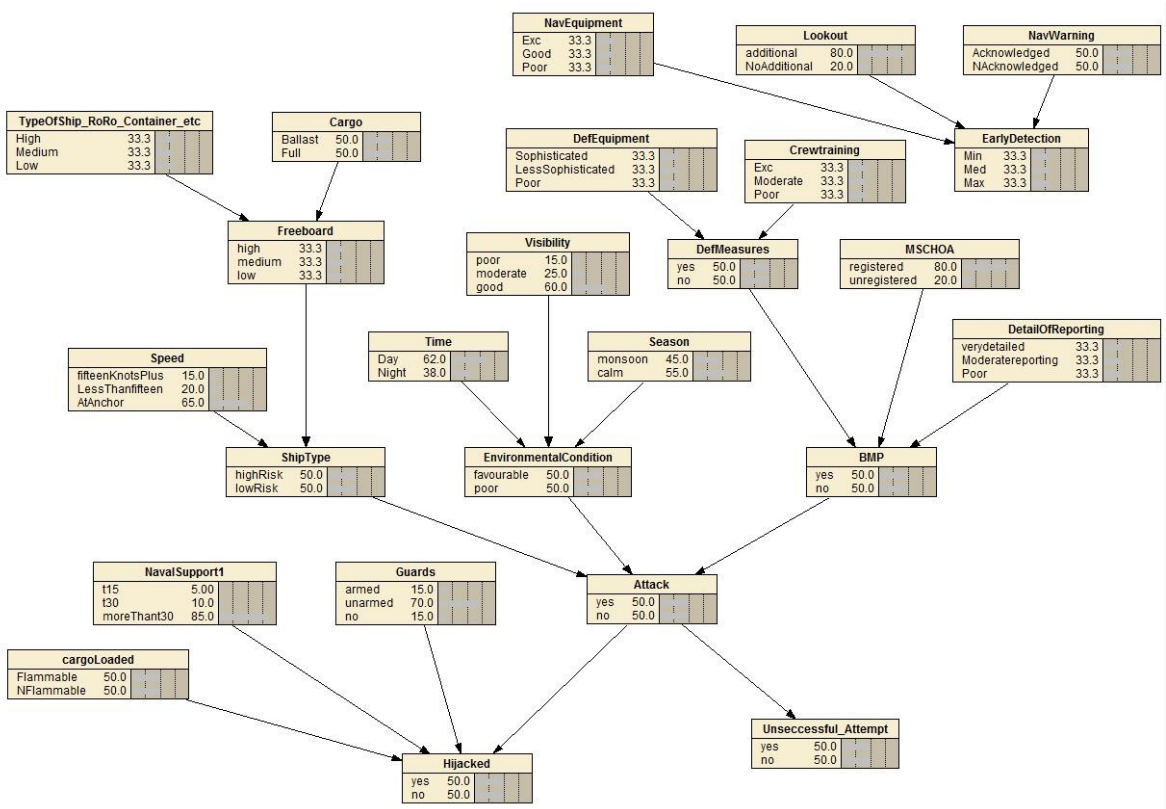

Figure 5 An expanded BN with more influencing nodes added

5. Industrial Response to Maritime Piracy

The identified significant influencing factors may individually or in combination contribute to the ship's piracy and robbery risks. At any time and location and given the characteristics of the vessel and also the security measures in place, the ship's security level can be estimated. Through such a study, possible security measures such as BMP and naval support can be studied to see how they would influence the likelihood of the ship's piracy and robbery attacks so as to determine the best operational security strategy in terms of cost-effectiveness. Through a sensitive analysis, it is found that security measures in terms of BMP, guards and naval support are playing important roles in reducing the likelihood of ships being hijacked and therefore are described in more detail as follows.

The great success in reducing the number of incidents in the HRA is, to a large extent, attributable to the naval forces. Starting from a more restrained role in the early days of Somali piracy, most Governments have given them greater backing in apprehending pirates. The reactive role has more and more been replaced by a proactive role to render Pirate Action Groups (PAGs) harmless. The international co-operation mechanism established through the Shared Awareness and Deconfliction (SHADE) process is unique in naval history. It is held every three months and focuses on improving cooperation and coordination of the maritime forces operating in the region while considering new initiatives and programmes designed to disrupt, and ultimately prevent future pirate attacks (Combined Maritime Forces, 2012). The navies have established the IRTC in the Gulf of Aden and maintain the Mercury information sharing platform which functions like an internet chat room - a very quick way for navies and Governments' Rescue Co-ordination Centres (RCC) to communicate suspicious activities and piracy attacks in the HRA. The navies also regularly provide escorts and military Vessel Protection Detachments (VPD) to World Food Programme (WFP) ships providing humanitarian aid to Somalia.

The BMP (BIMCO *et al*., 2011) are the shipping industry's response to the threat posed by pirates to their ships, crews and cargoes within the HRA. The contributors to the BMP comprise ship owner associations, special ship type associations such as tanker, passenger and dry cargo associations as well as the maritime insurance industry, navies and others. The BMP are to be implemented on board ships by their masters with guidance and support from the ship operators in order to avoid, deter or delay piracy attacks in the HRA. Failure to do so may result in disputes with maritime insurers who may make provisions in the insurance cover that require adherence to the BMP (Marsh, 2011).

The International Association of Ports and Harbours (IAPH) adopted a Resolution on Piracy which also includes a provision regarding arming of seafarers in 2010. IAPH believes that 'arming or military training of civilian crews will only escalate violence in pirate encounters. The use of weapons should remain restricted to military staff on internationally agreed missions' (IAPH, 2010). However, the latest estimate on the use of armed guards shows that the likely number of armed transits is 16,500 out of around 55,000 vessels transiting the Indian Ocean (McMahon, 2012a,b).

5.1. The Use of PCASP on board Ships

The initially fast-growing private maritime security industry is attempting to fill the gap where the protection of ships has not been sufficiently provided by navies. The terms PCASP and PMSCs are synonymous with private businesses and should be clearly distinguished from security provided by States or on behalf of a State. In the absence of any international laws regulating the PMSCs, serious concern has been voiced by IMO member States as well by ship owners and their associations about the righteousness of some of those PMSCs that use firearms to protect ships from attacks by pirates. The increase in private armed guards on board ships also puts flag States' Administrations under pressure as ship owners have, until recently, overwhelmed them with requests to approve the use of PCASP on board their ships (Fairplay, 2011).

The authorization of PCASP on board ships - as agreed by IMO member States - is a matter for flag States in consultation with ship owners, companies and ship operators and is not governed by the IMO (IMO, 2012b). One of the inadequately resolved difficulties on carrying of armed guards on board ships is the compliance of masters with some of the port or coastal States' legislation which may not

allow arms in their territorial waters. Failure to do so may result in serious delays for the ship or even the arrest of the master. The difficulty arising from the use of PCASP is that, for the time being, their deployment has only been discussed for the HRA and the guidance provided by the IMO and the industry is limited to this area only. However, concern has been raised within the industry that this may set a precedent and could soon be extended to other parts of the world.

5.2. Industry Perspective

It is the national ship owners' view that private armed guards are a clear second best choice to military personnel (ICS, 2011). A number of criteria for PMSCs have been listed that should be taken into account by a ship-owner (DNK, 2011); these criteria are very similar to the IMO guidance. Some of the criteria for vetting PMSCs that are not explicitly described in the IMO guidance but by maritime underwriters and insurers such as Den Norske Krigsforsikring for Skib (DNK) who recommends signing the 'International Code of Conduct for Private Security Providers', a 'publicly available code of conduct', a 'publicly available code of business ethics' and 'membership of an appropriate professional organisation' (DNK, 2011).

5.3. IMO Guidance

A key conclusion of all discussions on the use of PCASP was that the IMO guidance is not intended to endorse or institutionalize the use of PCASP. The IMO, however, has realized that a need had arisen to provide guidance to ship owners, masters, flag States and port and coastal States as it had become common practice among many ship owners to protect themselves using armed security services. The industry-developed BMP also provide guidance on PCASP (BIMCO *et al*., 2011), which in essence coincides with the IMO guidance.

The two key recommendations contained in the flag State guidance request flag States to:

1. Provide clarity to the masters, seafarers, ship-owners, operators and companies on the flag State policy on PCASP.
2. Develop a flag State policy on the authorization of PCASP.

The development of port and coastal State guidance was derived from the need for 'flag States, the shipping industry and the PMSCs who provide PCASP to know whether and under what conditions the embarkation and disembarkation of PCASP and/or firearms and security-related equipment for use by PCASP is allowed' (IMO, 2011). It was one of the conclusions of the Maritime Security Working Group (MSWG) that due to different 'legislative regimes among Member States, it was appropriate for only high-level recommendations to be developed at this stage' (IMO, 2011). Thus the guidance, similar to the IMO guidance for flag States, provides no detailed requirements on technical, legal or operational matters. It is therefore mentioned in the text that the recommendations 'do not address all the legal issues that might be associated with the movement of PCASP or of the firearms or equipment intended for use by them'.

5.4. Maritime Security Technologies and Education

For a ship operator's or managing company's emergency services, it is important to have up-to-date and reliable information about the ship's position. Modern satellite-based tracking systems are capable of providing position information on a frequent basis. AIS's position data as well as those from the LRIT are important for the identification of ships when coming under attacks from pirates. Such information is used by navies and law enforcement agencies to find and identify ships that have requested assistance.

The use of citadels has been a successful measure in the protection of ships that have been boarded by pirates. A citadel is defined in BMP4 (BIMCO *et al.*, 2011) as 'a designated pre-planned area purpose built into the ship where, in the event of imminent boarding by pirates, all crew members will seek protection. A citadel is designed and constructed to resist a determined pirate trying to gain entry for a

fixed period of time'. The success of such rescue operation depended on the proximity of the ship that had already been boarded by pirates. BMP also state that the 'citadel approach is lost if any crew member is left outside before it is secured'. In addition to the requirement of 100% crew assembled safely in the citadel, two more criteria must be met by the ship before a navy intervention can be considered: 1) The crew must have self-contained, independent and reliable 2-way external communications in addition to VHF communication and 2) the pirates must be denied access to ship propulsion (BIMCO *et al.*, 2011).

Another innovation that has entered the maritime security market is high security door locking solutions at bulkheads. When installed on tankers they must, in addition to the security requirement, also be able to be operated safely in potentially explosive atmospheres (Woodbridge, 2012). The locks would only allow crew members with a valid electronic 'permit to work' to access critical parts of the ship such as restricted areas.

The maritime industry is more and more considering making maritime security and defence a new profession. A more universal approach to the security and defence of the maritime industry as a whole should be taken far beyond currently recognized 'high risk' regions (Kuhlman, 2012). One of the questions that may be of interest in this respect is, how much of security education and training a seafarer should receive. The IMO member States have clearly indicated that seafarers should not be armed as they are not security experts. However, further requirements on security-related training for all or some seafarers become only internationally binding if the International Convention on Standards of Training, Certification and Watch-keeping for Seafarers (STCW) is amended. The threat posed by piracy is addressed in the latest revision of the Code to this convention (2010 Manila Amendments) and it remains to be seen in the future whether further amendments will be made to enhance the security elements for the seafarer qualification.

The proposed model can be used to help make security-based cost-effective decisions with respect to security measures, security policies, operational strategies and maritime security education.

6. Conclusion

Commercially operated ships are at high risk of becoming a victim of piracy unless robust security measures are taken to prevent from and react to such attacks. This paper analyses previous maritime piracy related incidents in the major piracy hotspot areas. Due to the highly complex environment a ship is operating in, the likelihood of a successful hijacking depends on many factors such as wind and weather conditions, ship characteristics such as freeboard and speed, the presence of naval forces in the sea area, and the security measures taken by the crew.

A model incorporating BN is proposed for estimating the likelihood of a ship being hijacked in the Western Indian/East Africa region, taking into account the associated influencing factors with uncertainties. The model is demonstrated through a case study with data obtained from both report data records and expert judgement. The model can be used as a standalone technique to update the estimation of the probability of ships being hijacked in the Western Indian/East Africa region when any new information becomes available. It can be also used by maritime stakeholders such as ship operators to make security-based operational decisions, providing essential input information in security cost benefit analysis. In the current difficult economic climate for ship operations with low freight rates and tonnage overcapacity for many cargoes a ship owner is reluctant to invest in unnecessary security measures. Especially the cost of a professional private armed security team is a great expenditure that has to be well thought through. It has to be analysed based on a realistic and profound risk analysis in order to balance the risk, costs and benefits.

The proposed model can take data from diverse sources for estimating the likelihood of a pirate attack and the ship being hijacked given a ship's characteristics, its operational environment and any security measures in place. The model can be used to investigate how influencing factors individually or in combination determine the probability of a ship being attacked or hijacked so as to select appropriate maritime security measures. It would be desirable if more test cases are applied to the described model in order to further demonstrate its industrial applicability. In fact, it is widely accepted that any

developed safety or security analysis approach should preferably be introduced into a commercially stable environment in order that the application has the chance to become established to prove feasible, otherwise it is more likely that its full potential will not be realised.

Disclaimer

This paper is the opinion of authors and does not necessarily represent the belief and policy of their employers.

Acknowledgements

This research was supported by a Leverhulme Research Fellowship (RF/7/RFG/2010-0019), an EU Marie Curie grant (REFERENCE – 314836), and an International Exchange grant from the Royal Society (IE140302). The authors would also like to thank the three anonymous reviewers for their constructive suggestions.

References

Bergen Risk Solutions, The Indian Ocean Monsoon, http://www.bergenrisksolutions.com/index.php?dokument=759, 2010.

Berle O., Asbjornslett B.E., "Formal vulnerability assessment: A methodology for assessing and mitigating strategic vulnerabilities for maritime supply chains", Reliability, Risk and Safety: Safety and Applications Vols.1-3, European Safety and Reliability Conference (ESREL), Prague, 7-10 Sept. 2009, 1005-1011.

Bevege A., Hassan A., Somali pirates end monsoon lull with hijacks, attacks, Reuters News online, http://af.reuters.com/article/topNews/idAFJOE56C0GO20090713 (accessed: 1 December 2014), 2009.

BIMCO *et al*., Best management practices for protection against Somalia based piracy, 4th Ed., Witherby, Edinburgh, 2011.

Blakemore R., www.mcga.gov.uk/c4mca.htm (accessed: 1 Dec. 2014), 2004.

Bosse E., Shahbazian E., Rogova G., Prediction and recognition of piracy efforts using collaborative human-centric information systems, IOS Press, US, 2013.

Bouejla A., Chaze X., Guarnieri F., Napoli A., "A Bayesian network to manage risks of maritime piracy against offshore oil fields", Safety Science, Vol.68, 2014, 222-230.

BRL-Shipping, www.brldata.com/documents/fleetbulkcarrier.doc (accessed: 11 Dec. 2014), 2004.

Clarksons, http://www.clarksons.net (accessed: 1 Dec. 2014), 2010.

Combined Maritime Forces, http://combinedmaritimeforces.com/2012/03/16/combined-maritime-forces-host-23nd-shade-meeting/ (accessed 18 April 2012), 2012.

Dabrowski J.J., de Villiers J.P., "Maritime piracy situation modelling with dynamic Bayesian networks", Information Fusion, Vol. 23, 2015a, 116-130.

Dabrowski J.J., de Villiers J.P., "A unified model for context-based behavioural modelling and classification", Expert Systems with Applications, Vol. 42, 2015b, 6738-6757.

DNK, Guidance on the selection of private security companies (PSC), MSC 89/J3, Den Norske Krigsforsikring for Skib (DNK), 2011.

Ehrhart H., Petretto K., The EU and Somalia: Counter-piracy and the question of a comprehensive approach, Study for the Greens/European Free Alliance. http://www.greens-efa.eu/the-eu-and-somalia-5416 (accessed: 3 March 2012), 2012.

Eleye-Datubo A.G., Wall A., Saajedi A., Wang J., "Enabling a powerful marine and offshore decision-support solution through Bayesian network technique", Risk Analysis, Vol.26, No.3, 2006, 695-721.

Esher L., Hall S., Regnier E., Sanchez P., Hansen J., Singham D., "Simulating pirate behavior to exploit environmental information", Proceeding of the 2010 Winter Simulation Conference, Baltimore, Maryland, USA, 5 - 8 December 2010, 1309-1314.

Fairplay, Ships with Guns Warned of South Africa Arrest, Fairplay Daily News online, 05 April 2011.

Farrington R., "Contact Group on Piracy off the coast of Somalia (CGPCS) – Briefing", Presentation by Chief of Staff (CoS) of the EUNAVFOR, London, 16 to 17 November 2009.

HM Government, The UK National Strategy for Maritime Security, May 2014.

IAPH, Resolution on Piracy, IMO Press Release, International Association of Ports and Harbours (IAPH), 2010.

ICS, ICS Reference Document: Flag State Rules and Requirements on arms and Private Armed Guards on board vessels, Reference number 1161, International Chamber of Shipping (ICS), 2011.

IFC, Spot Commentary 2/14 - Sea robbery and theft incidents in southern approaches of Malacca Strait, Phillips Channel and Northeast of Bintan. Republic of Singapore Navy, 10 December 2014.

IMO, International Convention on Load Lines, IMO, London, 1966.

IMO, Report of the Inter-sessional Working Group on Piracy and armed robbery against ships, MSC 90/20/1, IMO, London, 2011.

IMO, IMO Conference Proceeding on Capacity-Building to Counter Piracy off the Coast of Somalia, Circular letter No.3252, IMO, London, 2012a.

IMO, Revised Interim Guidance to Ship-Owners, Ship Operators, and Shipmasters on the use of Privately Contracted Armed Security Personnel on board Ships in the High Risk Area, MSC.1/Circ.1405/Rev.2, IMO, London, 2012b.

Jensen F.V., Nielsen T.D., Bayesian networks and decision graphs. 2nd Edition, Springer, 2007.

Jones B., Jenkinson I., Wang J., "Methodology of using delay-time analysis for a manufacturing industry", Reliability Engineering & System Safety, Vol.94, Issue 1, 2009, 111-124.

Korb K., Nicholson A., Bayesian artificial intelligence, Chapman & Hall/CRC, 2003.

Kuhlman J.L., "When is the maritime industry going to train maritime professionals?", The Maritime Executive, 13 June 2012.

Leander T., Security fears grow after hijackings and terror attack, Lloyd's List, 2010

Lee Y., "A study on the international legal actions against maritime terrorism and its national countermeasures in Korea", Maritime Law Review, Vol.18, Issue 1, 195-238.

Liwang H., Ringsberg J.W., Norsell M., "Quantitative risk analysis – Ship security analysis for effective risk control options", Safety Science, Vol.58, 2013, 98-112.

Lu C.S., Chang C.C., Hsu Y.H., Metaparti P.A., "Introduction to the special issue on maritime security", Maritime Policy and Management, Vol.37, No.7, 2010, 663-665.

Marsh, Piracy: the insurance implications, Brochure of MARSH insurance company, 2011.

McMahon L., Maritime security firms hope ISO meeting will accelerate armed guard regulation, Lloyd's List, 30 July 2012a.

McMahon L., Study notes at least three patterns behind attacks: Research pinpoints trends as Somali-based incidents widen their reach, Lloyd's List, 4 April 2012b.

Miller T., Indian Ocean - Southwest Monsoon Advisory, Website. http://www.hellenicwarrisks.com/warrisks/hwr/infopool.nsf/html/HBAK-85TK7N?OpenDocument, 2010.

Mukundan P., "IMB stats confirmed piracy fall", Safety at Sea, Vol.46, 2012, 15.

NATO Shipping Centre, Dhow community engagement, submitted by email to the IMO, 2 November 2011.

Nebojsa N., Eduard M., "Piracy on the high seas – threats to travellers' health", Journal of Travel Medicine, Vol.20, Issue 5, 2013, 313-321.

Norsys Software Corp, Netica-J Reference Manual, Vancouver, BC, Canada, 2010.

NRL Monterey, Marine meteorology division, Arabian Sea/Gulf of Aden Winds - SW monsoon introduction Tutorial, Website. http: //www.nrlmry.navy.mil/sat_training/world_wind_regimes/GulfOfAden/SW_Monsoon/index.html, 2002.

Pearl J., Probabilistic Reasoning in Intelligent Systems, Networks of Plausible Inference, Morgan Kaufmann, San Mateo, California, 1988.

Pristrom S., Development of a model to suppress piracy and other maritime crimes using scientific reasoning, PhD Thesis, Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, School of Engineering, Technology and Maritime Operations, Liverpool John Moores University, UK, 2013.

Pristrom S., Li K.X., Yang Z.L., Wang J., "A study of maritime security and piracy", Maritime Policy & Management, Vol.40, Issue 7, 2013, 675-693.

Psarros G., Christiansen A.F., Skjong R., Gravir G., "On the success rates of maritime piracy attacks", Journal of Transportation Security, Vol. 4, No. 4, 2011, 309-335.

Raymond C.Z., "Maritime terrorism in Southeast Asia: A risk assessment", Terrorism and Political Violence, Vol.18, 2006, 239-257.

Schneider P., Maritime security governance: A German perspective, A paper for the international Studies Association (ISA) - Annual Convention, San Diego, CA, USA, April 2012.

Sevillano J.C., Insua D.R., Rios J., "Adversarial risk analysis: The Somali pirates case", Decision Analysis, Vol. 9, Issue 2, 2012, 86-95.

Sloggett D., "Piracy focus shifts to Gulf of Guinea", Safety at Sea, Vol.47, 2013, 14.

Struwe L.B., "Private security companies (PSCs) as a piracy countermeasure", Studies in Conflict & Terrorism, Vol.35, Issue 7-8, 2012, 588-596.

UK MoD-HD, Ocean passages for the world, Vol. 4th Ed., Hydrographic Department, Taunton, UK, 1987.

UK Navy-Hyd, Persian Gulf Pilot, Vol. 11th Ed., Hydrographic Department, Taunton, UK, 1967.

UK P&I Club, Bulletin 763 - 05/11 - Piracy: A change of tactics - West Africa, UK P&I bulletin, 2011.

Vanek O., Jakob M., Hrstka O., Pechoucek M., "Agent-based model of maritime traffic in piracy-affected waters", Transportation Research Part C, Vol36, 2013, 157-176.

Vanek O., Bosansky B., Jakob M., Pechoucek M., "Transiting areas patrolled by a mobile adversary", Proceedings of 2010 IEEE Symposium on Computational Intelligence and Games (CIG), Dublin, 18-21 August 2010, 9 - 16.

Vanek O., Jakob M., Lisy V., Bosansky B., Pechoucek M., "Iterative game-theoretic route selection for hostile area transit and patrolling", Proceeding of the 10th International Conference on Autonomous Agents and Multiagent Systems, Vol. 3, Taipei, Taiwan, 2 - 6 May 2011, 1273-1274

Wang J., Li M., Liu Y., Zhang H., Zou W., Cheng L., “Safety assessment of shipping routes in the South China Sea based on the fuzzy analytic hierarchy process”, Safety Science, Vol.62, 2014, 46-57.

Wang J., Trbojevic V., Design for safety of large marine and offshore engineering products, Institute of Marine Engineering, Science and Technology, London, UK, 2007, 403 pages (ISBN 1-902536-58-4).

Woodbridge, D., “On board with security”, Tanker Operator, Vol.6, 2012, 31–32.

Yang Z.L., Ng A.K.Y., Wang J. “Incorporating quantitative risk analysis in port facility security assessment”, Transportation Research Part A: Policy and Practice, Vol. 59, 2013, 72-90.

Yang Z.L., Wang J., Li K.X., “Maritime safety analysis in retrospect”, Maritime Policy & Management, Vol.40, No.3, 2013, 261-277.

Ziello A.R., Angioli R.D., Fasanaro A.M., Amenta F., “Psychological distress in families of victims of maritime piracy - the Italian experience”, International Maritime Health, Vol.5, Issue 1, 2014, 28-32.