Maritime Piracy Situation Modelling with Dynamic Bayesian Networks

Joel Janek Dabrowski[a,*], Johan Pieter de Villiers[b,a]

[a] *University of Pretoria, 2 Lynnwood Rd, Pretoria, South Africa*
[b] *Council for Scientific and Industrial Research, Meiring Naudé Rd, Lynnwood, Pretoria, South Africa*

Abstract

A generative model for modelling maritime vessel behaviour is proposed for the fabrication of synthetic data. The proposed model is a novel variant of the dynamic Bayesian network (DBN) that builds upon a switching linear dynamic system (SLDS). The proposed model is applied to a maritime piracy problem. The DBN provides a model that simulates the behaviour of various vessels in a maritime piracy situation. Context based external factors that influence the system are catered for. Simulated observations of kinematic data such as position and velocity are generated by the DBN. The proposed model provides a means for generating data for the purpose of developing and evaluating counter-piracy methods and algorithms. A novel methodology for evaluating and optimising the proposed model is discussed. The log-likelihood, the Kullback-Leibler divergence and the Bhattacharyya distance measures are used for evaluation.

Keywords: Maritime Domain Awareness, Maritime piracy, Multi-Agent Simulation, Information Fusion, Dynamic Bayesian Network, Switching Linear Dynamic System.

1. Introduction

The increase in global maritime piracy has led to various counter-piracy measures and efforts. Maritime surveillance is essential in these efforts. Electronic surveillance provides a foundation for automatic situation and threat assessment. Situation and threat assessment methods generally require prior data. Prior real world data for illegal activities such as maritime piracy and illegal immigration is however scarce [1]. Maritime piracy reports are published by the International Maritime Bureau (IMB) [2]. Ship masters and operators may report piracy incidents through a reporting centre. These reports are incidental by nature. For the purpose of early detection algorithms, incidental data is incomplete. Early detection algorithms require data that describe maritime pirate behaviour before an attack. An alternative source for such data is synthetic data generation.

A multi-agent generative model of a maritime piracy situation using dynamic Bayesian networks (DBN) is proposed. The DBN is an extension of the switching linear dynamical system (SLDS). The proposed model provides a means for synthetic data generation and simulation. The DBN is applied to model the behaviour of various vessels in a maritime environment. Behaviour such as sailing, target acquisition, and attacking are modelled. The DBN provides the capability to model a vessel at the level of the motion state vector. Given the nature of a DBN, the proposed model is based on a statistical framework. The structure of the DBN is informed by a priori knowledge of the problem.

The novelty of this work lies in the use of a SLDS in the DBN to generate simulated track data. The evaluation methodology provides a novel framework for evaluating behavioural models. The purpose of this work is primarily for the testing of maritime pirate behaviour detection algorithms. Particularly, early detection algorithms that detect maritime pirate vessel behaviour before they attack.

2. Background and Related Work

Multi-agent systems have been applied in various fields. These include robotics, computer games, simulation, econometrics, military and social sciences [3, 4]. Multi-agent Based Simulation (MABS) is a relatively new paradigm for modelling and simulating entities in an environment [5]. Agents are generally considered to be autonomous, independent and able to interact with their environment and other agents [6, 5]. The military application of MABS is closely related to the application considered in this paper. Military applications intend to enhance training and support decision making [7]. A review of military based MABS applications are provided in [8].

The DBN [9] is a temporal extension of the Bayesian network (BN) [10]. The DBN has been applied to a wide variety of applications. Applications computer vision based human motion analysis [11], situation awareness [12] and vehicle detection and tracking [13]. The BN is a naturally applied for decision making. The influence diagram (ID) is a BN supplemented with decision variables and utility functions [14]. It could be argued that the higher levels of the model proposed in this paper form an influence diagram. IDs been applied to solve a vast number of decision problems. Poropudas and Virtanen have used IDs in the analysis of of simulation data [15]. Poropudas and Virtanen have extended this work to include the use of DBNs for the application of simulation [16, 17]. In their work,

*Corresponding author.
Email address: joeldabrowski@gmail.com (Joel Janek Dabrowski)

the time evolution is studied and what-if-analysis is performed. The DBN simulation approach is applied to the applications of server queueing and simulated air combat. The use of expert knowledge to construct the DBN is suggested as an possible extension to their work. The model proposed in this paper is an implementation of this suggestion.

The SLDS [18, 19, 20] is a form of a DBN. In literature, the SLDS is associated with various names. These include the switching Kalman filter and the switching state space model [19]. The SLDS has been successfully applied to various problems that include human motion modelling in computer vision [21], econometrics [22] and speech recognition [23].

A variety of maritime surveillance applications have been formulated within the field of information fusion. A simulation test-bed has been developed for coastal surveillance [24]. The test-bed is developed for the study of distributed fusion, dynamic resource and network configuration management, and self synchronising units and agents. The BN has been proposed for use in information fusion for maritime security [25, 26] and maritime domain awareness [27, 28]. The BN is applied for decision making and inference. A DBN has been proposed for multi-sensor information fusion [29]. The model is proposed to be applied for various sensors such as imaging sensors, acoustic sensors and radar sensors. A DBN has been applied for information fusion in a driver fatigue recognition application [30] and for human-computer interfaces [31].

Context-based applications incorporate and model contextual information. A survey of context modelling has been conducted by Strang and Linnhoff-Popien [32]. A more recent survey on context modelling and reasoning in pervasive computing has been conducted in [33]. Context-based information fusion has been applied to various applications such as video indexing [34], computer vision [35] and natural language processing [36]. Context-based information fusion has found application in various maritime situation and threat assessment applications [37, 38, 39]. A DBN has been applied in context based information fusion for location estimation [40]. This application has been extended to include fuzzy logic for imprecise contextual reasoning [41, 42].

Website applications for situation awareness have been made available. An on line data visualisation and risk assessment tool for maritime piracy is available [43]. The European Commission has developed the Blue Hub for maritime surveillance data gathering [44]. The platform is currently in development for maritime piracy awareness.

Maritime piracy is a problem of international concern. Maritime piracy poses humanitarian, economic and environmental risks [45]. In late 2008 three counter-piracy missions were deployed. These include the EU's Operation 'Atlanta', NATO's Operation 'Ocean Shield' and the US-led Combined Task Force-151 [46]. These operations have deployed war ships to patrol high risk regions and assist maritime piracy victims. Due to the vast patrol regions, patrolling efforts are partially successful. The use of technology is proposed to assist in combating maritime piracy [47].

Various applications have been proposed in literature for combating maritime piracy. Game theoretic applications have been proposed to optimise counter piracy strategies. Game theory has been utilised to suggest transport routes that avoid maritime pirates [48, 49]. A game theoretic approach that seeks to optimise counter piracy patrolling strategies has been implemented [50]. Various risk analysis applications have been proposed [51, 52]. The risk analysis applications generally seek to assist ship owners and captains in managing risk during a pirate attack. Applications for pirate detection have been proposed. An approach to detect pirates through satellite communication monitoring has been proposed [53]. Other approaches attempt to detect pirate vessels by classifying small craft in imagery [54], [55].

A state based multi-agent simulation environment has been proposed for simulating maritime entity behaviour [1]. Long-haul shipping, Piracy Behaviour and Patrolling behaviour are simulated in the system. Vessel behaviour simulations are implemented using finite state machines. Long-haul shipping behaviour is based on a model where cargo ships follow a route that minimizes travel time, costs and security. Pirate behaviour includes activities such as discovering, approaching and attacking vessels. Patrol vessels are placed at near optimum locations according to their deterrence potential as well as according to a risk map. An algorithm is used to determine a set of routes for a set of patrol vessels that maximizes deterrence.

A method of simulating pirate kinematic behaviour has been proposed [56]. The simulation is based on the model where pirates venture out in skiffs from a home base in search of targets. The skiffs motor out to a predestined location and drift until supplies have been depleted. Once the supplies have been depleted, the pirates return to the base to refresh their supplies. To simulate the drifting of the pirate vessels, meteorological and oceanographic forecasts are utilized.

3. Dynamic Bayesian Networks and the Linear Dynamic Switching System Model

The Bayesian network provides a means of statistically modelling causal relationships in data. The dynamic Bayesian network (DBN) extends the Bayesian network to allow modelling of sequential data [19, 20, 57, 58, 9].

The switching linear dynamic system (SLDS) is a mathematical model that may be considered a subclass of DBNs [20]. The switching linear dynamic system provides a means to model a system whose linear parameters change over time. A proposed variation of the classical SLDS model is described by the following state space equations:

$$x_t = A(s_t)x_{t-1} + B(s_t)u_t + v_t(s_t), \tag{1}$$

$$y_t^m = C(s_t)^m x_t + w_t(s_t)^m \tag{2}$$

and

$$u_t = f(x_{t-1}). \tag{3}$$

In (1), x_t is the state vector, u_t is the control vector, $A(s_t)$ is the system matrix, $B(s_t)$ is the input matrix and $v_t(s_t)$ is the state noise process. In (2), y_t^m is the observed measurement, $C(s_t)^m$ is the observation matrix and $w_t(s_t)^m$ is the measurement noise.

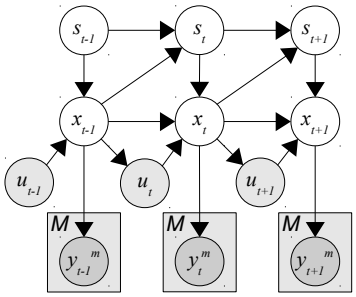


Figure 1: Dynamic Bayesian network (DBN) representation of a switching linear dynamic system (SLDS) for three time slices. The s_t node denotes the switching process state, the x_t node denotes the system state vector, the u_t node denotes the control input and the y^m_t node denotes the m^{th} sensors observed measurement vector at time t.

The variables in (2) describe the measurements from the m^{th} sensor selected from a set of M sensors. Equations (1) and (2) describe the typical linear dynamic system equations in state form [59]. In (3), u_t is the control vector and $f(x_{t-1})$ is the control function. The control function $f(x_{t-1})$, transforms the vessel's previous state x_{t-1} to a control vector u_t.

The additional parameter, s_t in the state equations is the switching processes state. It is assumed that that s_t follows a first order Markov process [60]. As the switching process state changes, the linear dynamic systems parameters change. This provides the means to model a complex dynamic system through varying states or activities.

The SLDS described by (1), (2) and (3) may be represented as the DBN model illustrated in Figure 1. The DBN model is described by the following joint probability distribution:

$$p(\bar{y}_{0:T}, x_{0:T}, u_{0:T}, s_{0:T}) = \prod_{t=0}^{T}\prod_{m=1}^{M} p(y_t^m|x_t)p(x_t|s_t, x_{t-1}, u_t)p(s_t|s_{t-1}, x_{t-1}). \quad (4)$$

The dependencies between variables correspond to the SLDS system equations provided in (1), (2) and (3).

4. Maritime Piracy Situation DBN Model

To model behaviour, it is proposed that the switching process state s_t in an SLDS be represented as a DBN. The proposed DBN for modelling vessel behaviour in a maritime piracy situation is illustrated in Figure 2. In this model, the process state, s_t is essentially expressed as a DBN that includes the class (C), journey parameters (JP), external parameters (EP) and the state parameter (SP) random variables. The x_t, y^m_t and the u_t variables are the state space equation vectors for the the SLDS as described in section 3. The ocean/weather (OW) variable is included to model the influences of ocean and weather conditions on the motion of vessels.

The DBN model in Figure 2 is represented in plate notation. Each of the N vessels in the environment are represented by a vessel plate. The time plate contains the dynamic nodes that transition between states over the T discrete time steps. A set of E external parameters are represented by the EP plates. The set of M sensors are represented by the sensor plates.

4.1. Class Variable (C)

The C variable represents the class of a particular vessel. The C variable describes either a pirate vessel, a transport vessel or a fishing vessel. The probability distribution of the transport vessel and fishing vessel classes may be determined by considering ocean traffic statistics. The statistics for pirate vessels may be inferred from piracy report statistics provided by the International Maritime Bureau (IMB).

4.2. Journey Parameters Variable (JP)

The JP variable is a random variable that selects the home location, the route via points and the destination location for a particular vessel. These variables are selected from to a list of predefined locations and routes. The predefined locations include world ports, fishing towns, pirate ports, fishing zones and pirate zones. Via points determine route paths. Route paths are straight lines between via points.

The JP variable is conditionally dependent on the C variable. The dependence places constraints on the possible locations that may be selected given the class. For example, a pirate class may only select a pirate zone as a destination location.

The world ports probability distribution may be constructed from world port rankings. The American Association of Port Authorities (AAPA) [61] produce world port rankings. Fishing zones may be inferred from fishing vessel traffic data or from legalized fishing zones. Pirate zones may be determined from attack locations provided in IMB published attack reports.

4.3. External Parameters (EP)

The external parameters variable describes context based external factors that influence the system. A set of E external parameters may be provided. External factors may include date, time, season, ocean conditions and weather conditions. The EP variables are considered to be observable. The observations of the variables may be obtained from data sources. Data sources may include oceanographic and climatic models or data.

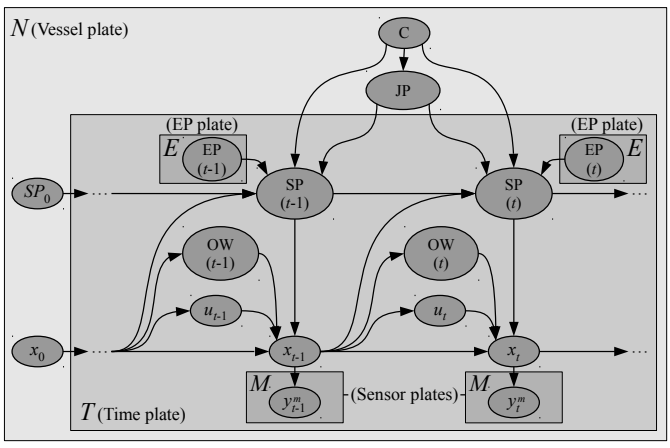


Figure 2: Dynamic Bayesian Network (DBN) model for a vessel in a maritime piracy situation.

4.4. State Parameters Variable (SP)

The SP variable provides an indication of the nature of a particular vessels kinematic activity or behaviour. The SP variable is defined to contain the *anchor*, *sail-out*, *sail-home*, *fish*, *drift*, *attack* and *abort-attack* states. The SP variable is conditioned on the C variable. This dependence dictates which SP states may be utilised for a particular vessel class. The state parameters and their associativity may be described with state transition diagrams illustrated in Figure 3.

The state transition diagram for the transport vessel is illustrated in Figure 3a. It is assumed that transport vessels travel from a home port to a destination location along the most economical route [62, 1]. The vessel is in an anchor state when located at its home location. The state transitions to the sail-out state when the vessel is required to sail to its destination. When reaching the destination port, the vessel returns to the anchor state.

The state transition diagram for a fishing vessel is illustrated in Figure 3b. It is assumed that fishermen prefer fishing during particular times and seasons. The fishing vessel will remain in an anchor state at its home location. At dawn or dusk, the vessel will transition to a sail-out state. The vessel sails out to a fishing zone. Once in the fishing zone, the fishing vessel will enter the fish state. After fishing, the fishing vessel will transition into a sail-home state. When the home location is reached, the fishing vessel returns to an anchor state.

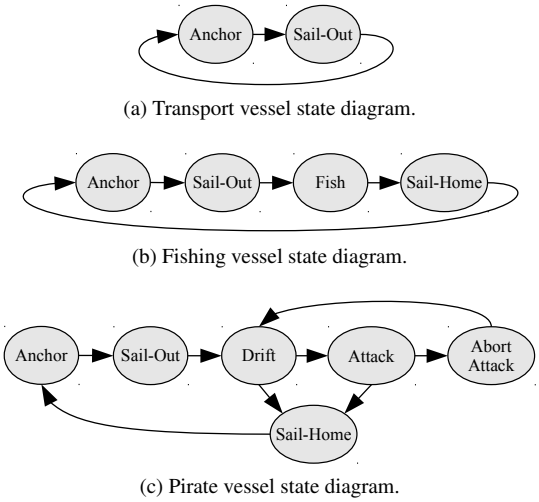
The state transition diagram for a pirate vessel is illustrated in Figure 3c. This model is based on the model proposed in [1]. A pirate vessel will leave its anchor state to sail out to a pirate zone in a mothership. When the pirate zone is reached, the pirate vessel transitions to a drift state where the pirates wait for a target [56]. On detection of a target, the pirate vessel will enter an attack state and attack the target with small high speed boats such as skiffs [63, 45]. If the attack is successful, the pirates will return home with the hijacked vessel to ransom it. The mothership is left abandoned. If the attack is unsuccessful, the pirate vessel enters the abort-attack state. In this state, the skiffs return to the mothership and return to the drift state.

The SP variable is dependent on the EP variable. External factors influence vessel behaviour. Time and ocean conditions are external factors that are considered. Pirates typically attack during hours of darkness [63]. Pirates are expected to avoid seasonal conditions such as high waves, high winds, high ocean currents and monsoon seasons [64, 2].

The pirate drift state is a target acquiring state. The pirate class is required have a perception of surrounding vessels. For this, the SP variable must be conditionally dependent on other vessels measurement vector y_t^m. This implies that there is conditional dependence between the N vessel plates.

4.5. Ocean Current/Weather Variable (OW)

The OW variable describes ocean conditions and weather conditions. This variable is included to influence the motion of vessels. The variable provides a means for the ship vessel to drift according to the ocean currents and wind specified at the particular location of the vessel. This variable is considered to be observable. The parameters for this variable may be obtained from oceanographic and climatic models or data. The OW variable is dependent on x_t at the previous time step. This provides a means to determine the localised ocean and weather conditions.



(a) Transport vessel state diagram.

(b) Fishing vessel state diagram.

(c) Pirate vessel state diagram.

Figure 3: State transition diagrams describing the state-parameters node for each class.

4.6. Dynamic Linear System Vectors

The dynamic linear system vectors include the state vector x_t, the control vector u_t and the observed measurement vector y_t^m. These vectors are described by the state space equations given in (1), (2) and (3). The control function $f(x_t)$ computes the control vector u_t such that the vessel sails between the via points specified by the JP variable.

5. Evaluation and Results

The proposed model is evaluated by comparing the real-world pirate data and simulated data. The spatial region of pirate attacks is limited to the region of the Gulf of Aden and the Indian ocean. A set of 235 reported attacks that occurred in this region are extracted from the 2011 IMB annual piracy report [2]. The set of 235 attack locations forms a real-world dataset to which the proposed model is compared. A set of simulations are run using the proposed model. Pirate attack locations are recorded during the simulation. The simulation is run until at least 235 pirate attacks have occurred. The set of recorded pirate attack locations form the simulated pirate attack dataset. The simulated dataset is compared with the real-world dataset.

The process of optimisation and evaluation of the proposed model is described by the block diagram in Figure 4. Prior knowledge is utilised to form the proposed model of pirate, transport and fishing vessel behaviour. The model is utilised to generate simulated pirate attack data. An estimate of the probability density function of the simulated pirate attack data is computed. The likelihood of the real-world dataset given the

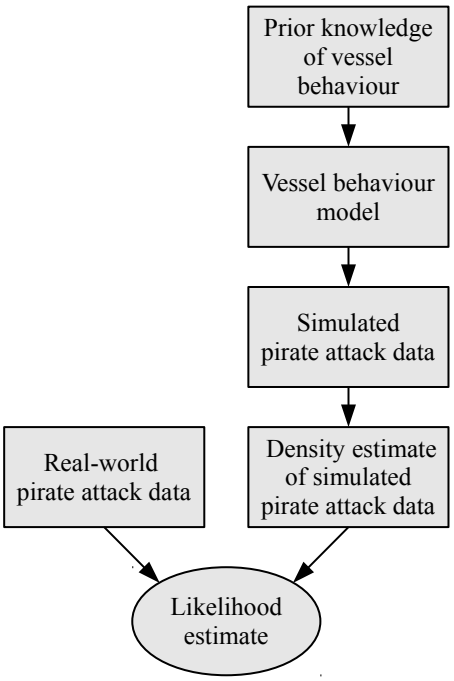


Figure 4: Block diagram of the optimisation and evaluation process of the proposed model.

simulated dataset is computed. The likelihood provides an indication of the ability of the proposed model to generate the real-world pirate data. The likelihood is applied for the evaluation of the proposed model. The model effectiveness is evaluated according to information gain, quality and robustness.

5.1. Gaussian Mixture Model Fitting

A Gaussian mixture model (GMM) is fitted to the simulated pirate attack dataset. The GMM serves as an estimation of the probability density function of the simulated dataset. Let $\bar{a} = (\bar{a}_1^T, ..., \bar{a}_n^T)^T$ describe the vector of the simulated pirate attack locations. Each $\bar{a}_j$, $j = 1, ..., n$ contains the longitude and latitude of the j^{th} pirate attack location. The g-component GMM describing this dataset is given as follows [65]:

$$q(\bar{a}_j; \psi) = \sum_{i=1}^{g} \pi_i \phi_i(\bar{a}_j; \mu_i, \Sigma_i). \tag{5}$$

The variable ψ describes the parameters of the GMM. These include the mixture weights π_i and the Gaussian parameters μ_i and Σ_i. The i^{th} Gaussian mixture component is represented by ϕ_i. The variable π_i describes the weight of the i^{th} Gaussian mixture component. Variables μ_i and Σ_i describe the mean and covariance of the i^{th} Gaussian mixture component respectively.

The likelihood for the model parameters ψ is formed from the observed data. The likelihood is given by [65]:

$$\mathcal{L}(\psi) = \prod_{j=1}^{n} q(\bar{a}_j; \psi). \tag{6}$$

The log-likelihood is often a more convenient representation of the likelihood in application. The log-likelihood is given by [65]:

$$\log \mathcal{L}(\psi) = \sum_{j=1}^{n} \log q(\bar{a}_j; \psi). \tag{7}$$

The GMM is fitted to the simulated dataset using the expectation maximization (EM) algorithm. The observed data vector $\bar{a}$ is considered to be incomplete in the EM algorithm. The complete data vector includes the associated component-label vectors $\bar{l} = (l_1, ..., \bar{l}_n)^T$ such that:

$$\bar{a}_c = (\bar{a}^T, \bar{l}^T)^T. \tag{8}$$

Each $\bar{a}_j$ is assumed to have arisen from one of the GMM components. The vector $\bar{l}_j$ is a g-dimensional vector containing indicator variables. Label l_{ij} is assigned the value 1 or 0 according to whether a_j arose from the i^{th} mixture component or not ($i = 1, ..., g$; $j = 1, ...n$). The complete-data log likelihood for ψ is given as [65]:

$$\log \mathcal{L}_c(\psi) = \sum_{i=1}^{g} \sum_{j=1}^{n} l_{ij} \Big(\log \pi_i + \log q(\bar{a}_{cj}; \psi) \Big). \tag{9}$$

The E-step of the EM algorithm requires the computation of the conditional expectation of $\log \mathcal{L}_c(\psi)$ given $\bar{a}$. In the k^{th} iteration of the algorithm, this value is given by the following expectation [65]:

$$\begin{aligned} Q(\psi; \psi^{(k)}) &= \mathbb{E}_{\psi^{(k)}} \left(\log \mathcal{L}_c(\psi) | \bar{a} \right) \\ &= \sum_{i=1}^{g} \sum_{j=1}^{n} \tau_i(\bar{a}_j; \psi^{(k)}) \Big(\log \pi_i + \log q(\bar{a}_{cj}; \psi) \Big). \end{aligned} \tag{10}$$

The value $\tau_i(\bar{a}_j; \psi^{(k)})$ describes the expectation of the random variable Z_{ij} with respect to the observed data $\bar{a}$. This value is given by [65]:

$$\tau_i(\bar{a}_j; \psi^{(k)}) = \tau_{ij}^{(k)} = \frac{\pi_i \phi(\bar{a}_j; \mu_i, \Sigma_i)}{\sum_{h=1}^{g} \pi_h \phi(\bar{a}_j; \mu_h, \Sigma_h)}. \tag{11}$$

The M-step of the EM algorithm requires the global maximization of $Q(\psi; \psi^{(k)})$ with respect to ψ. This computation exists in closed form for Gaussian components. The M-step involves the updating of the component means and covariance matrices at the k^{th} iteration. The update for the mean is given as follows [65]:

$$\mu_i^{(k+1)} = \frac{\sum_{j=1}^{n} \tau_{ij}^{(k)} \bar{a}_j}{\sum_{j=1}^{n} \tau_{ij}^{(k)}}. \tag{12}$$

The update for the covariance matrix is given as follows [65]:

$$\Sigma_i^{(k+1)} = \frac{\sum_{j=1}^{n} \tau_{ij}^{(k)} (\bar{a}_j - \mu_i^{(k+1)})(\bar{a}_j - \mu_i^{(k+1)})^T}{\sum_{j=1}^{n} \tau_{ij}^{(k)}}. \tag{13}$$

The E- and M-steps are alternated repeatedly until convergence. The EM algorithm converges when $\log \mathcal{L}_c(\psi^{(k+1)}) - \log \mathcal{L}_c(\psi^{(k)}) < \epsilon$, where ϵ is a small arbitrary value [65].

5.2. Model Likelihood

The likelihood function is defined according to a set of observations originating from a distribution with parameters ψ [65]. A likelihood function is to be formed that describes the likelihood of the real-world pirate dataset with respect to the simulated pirate dataset. This likelihood function may be described according to the observations from the real-world dataset and the parameters of the simulated dataset. The parameters of the simulated dataset are the GMM model parameters ψ, described in (5). Let $\bar{b} = (b_1^T, ..., b_n^T)^T$ describe the a vector of the pirate attack locations of the 2011 dataset. The log-likelihood function of the real-world dataset with respect to the simulated dataset is given as follows:

$$\log \mathcal{L}(\psi) = \sum_{j=1}^{n} \log q(\bar{b}_j; \psi). \tag{14}$$

The function $q(\bar{b}_j; \psi)$ is the GMM of the simulated dataset evaluated at the locations given by $\bar{b}_j$, $j = 1...n$.

The results of (14) provide a means for model optimisation and evaluation.

5.3. Model Configuration for Simulation

A set of simulations are run for the purpose of optimisation and evaluation of the proposed model. A set of ports, points-of-interest and via points are fixed on the map of the Gulf of Aden. The particular assignment of simulated routes of transport vessels and the pirate attack zones is critical. The assignments are delineated according to known shipping lanes and the 2011 pirate attack data. Three pirate ports are initialized; Bosaso, Harardhere and Mogadishu. The pirate port locations are selected based on locations of ransom payments and reported hijacked vessel anchorage locations [66].

A set of N vessels are sampled from a Poisson distribution and initialized on the map. The Poisson distribution is modelled with a mean of $\lambda = 40$. The C variable is sampled from a distribution that describes the probability of sampling each class. The pirate class is sampled with a probability of 0.05. The transport vessel is sampled with a probability of 0.7. A fishing vessel is sampled with a probability of 0.25.

The JP variable is sampled from a uniform distribution of ports, pirate zones and fishing zones. Ports, pirate zones and vessel paths for transport and pirate vessels are illustrated in Figure 5.

The EP variable plate contains a single variable that describes the sailing conditions. This variable combines information such as season, time-of-day and ocean conditions. As an example, a poor sailing condition for a pirate vessel occurs during daytime in a monsoon season.

The model is configured such that vessels follow a constant velocity model. The x_t, y_t^m and u_t variables are implemented as described by (1), (2) and (3). The y_t^m variable is configured to contain the longitudinal and latitudinal coordinates of the vessel. The OW variable is modelled as a random process.

The control function $f(x_t)$ calculates the control vector u_t such that the vessel sails along a designated path. The control function includes a random Markov process that is modelled by a white noise distribution. This process adds a variance to the vessel paths.

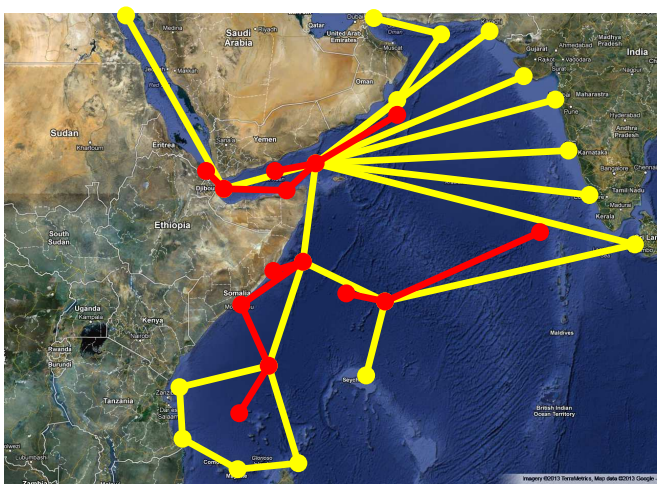


Figure 5: Map of the Gulf of Aden with vessel routes. Yellow routes are routes for transport and pirate vessels. Red routes are routes that extend from pirate ports and pirate zone centres.

5.4. Model Optimisation and Evaluation

The optimal model is the model that produces the most likely results. The likelihood is described in section 5.2. For model optimisation, the model parameters may be varied. Parameters associated with the transport routes and pirate zones may be considered. Parameters include the transport vessel paths, the number of pirate zones, pirate zone locations, pirate zone sizes and pirate zone probabilities. In this study, only the pirate zone size shall be considered. This shall serve a demonstration of the optimisation procedure.

A set of six pirate zones are selected as illustrated in Figure 6. The locations and relative sizes of the pirate zones are selected according to the 2011 attack data. The probability of a pirate zone is determined by the number of attacks in the pirate zone and the size of pirate zone. The probability of a pirate zone is the probability that the pirate zone will be selected by a pirate. The pirate zones are represented by bivariate Gaussian distributions. The mean value of the Gaussian distribution defines the location of the pirate zone. The covariance of the Gaussian distribution determines the size of the pirate zone.

The covariance of the Gaussian distributions are varied for the purpose of model optimisation. Each Gaussian distribution has a preselected covariance. The covariance of all the Gaussian distributions are scaled by a single scaling factor, σ. The scaling factor is considered over the set of values $\sigma = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. A simulation is performed for each value of σ. The simulated pirate attacks for $\sigma = 1$ is illustrated in Figure 7. This result illustrates condensed clusters of pirate attacks. For comparison, the pirate attack locations of 2011 are illustrated in Figure 8. The results in Figure 7 seem to demonstrate little correlation with the real-world data. The simulated pirate attacks for $\sigma = 6$ is illustrated in Figure 9. The results seem to demonstrate a higher correlation with the 2011 pirate

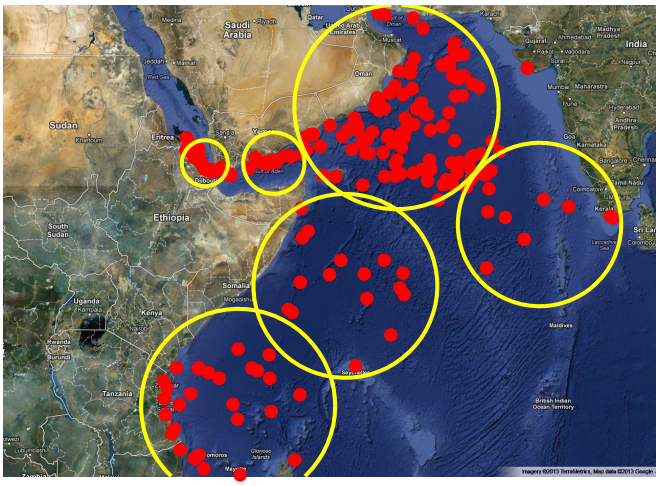


Figure 6: Selected pirate zones. Each pirate zone is represented by a Gaussian distribution. The yellow rings describe the standard deviation of the Gaussian distributions. The 2011 pirate attack locations are plotted as red markers.

attack data. The simulated pirate attacks for $\sigma = 9$ is illustrated in Figure 10. The results demonstrate a more uniform distribution of pirate attacks.

A set of GMMs are fitted to each of the nine simulation results. The EM algorithm described in section 5.1 is applied for fitting the GMMs. The EM-algorithm requires initial parameters for the GMM. The number of Gaussians in the GMM was set as $g = 6$. This corresponds to the number of preselected pirate zones. The initial mean values were set as the preselected pirate zone Gaussian distribution means. The covariance matrices were initialized as diagonal matrices. The diagonal elements were set as the variance of the real-world pirate attack data. The initial weights were set uniformly. The resulting GMM probability density function for $\sigma = 6$ is illustrated in Figure 11.

The model is optimised by considering the likelihood described by (14). The likelihood results for the set of σ values is presented in Table 1. The optimum value is demonstrated to be $\sigma = 6$. The model with $\sigma = 6$ is considered to be the optimum model.

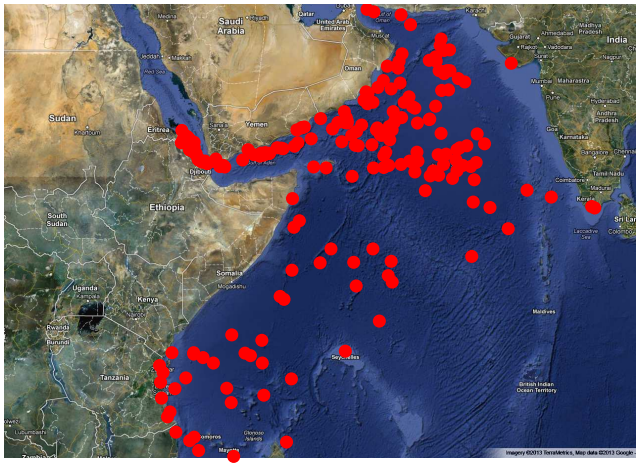


Figure 8: Pirate attack locations of 2011 [2]

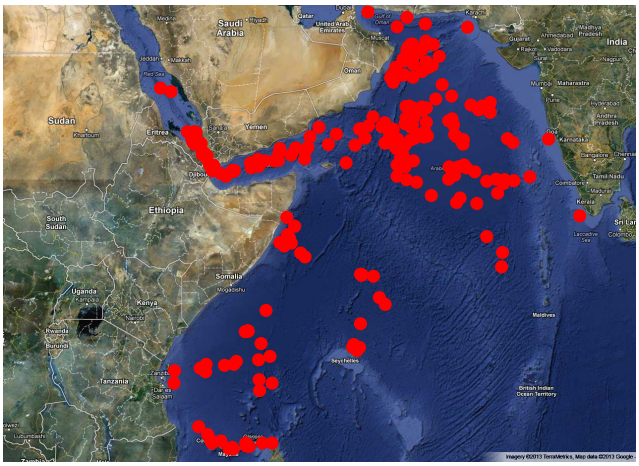


Figure 9: Simulated pirate attacks for $\sigma = 6$. This value produces the optimum results.

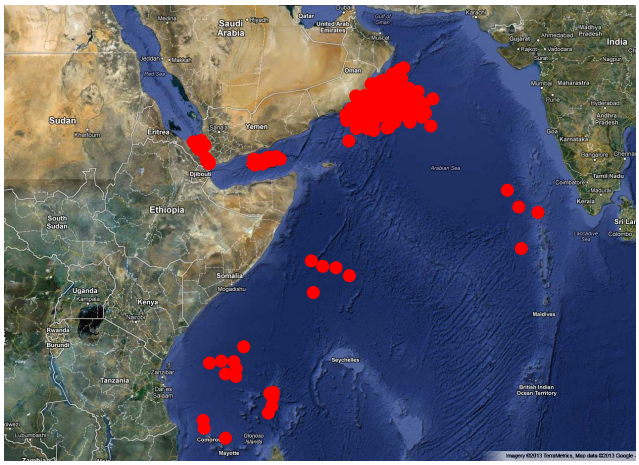


Figure 7: Simulated pirate attacks for $\sigma = 1$

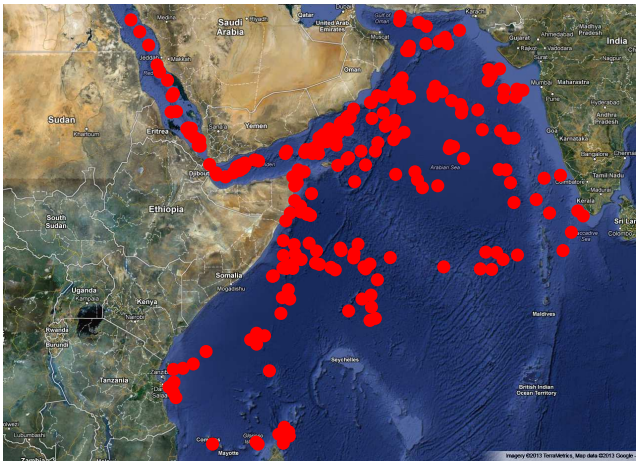


Figure 10: Simulated pirate attacks for $\sigma = 1$

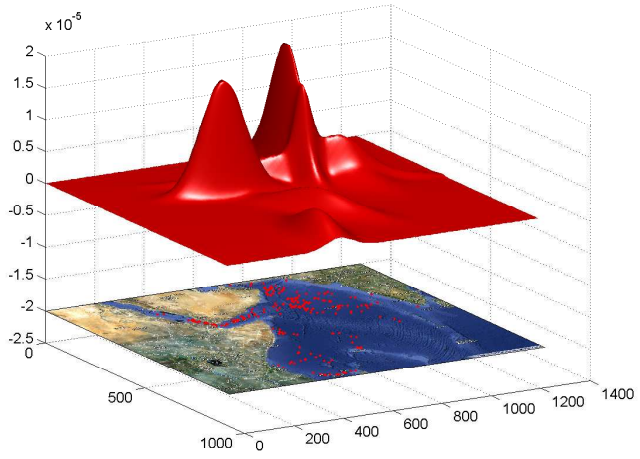


Figure 11: GMM for the simulated pirate attack data for $\sigma = 6$. The surface illustrates the GMM probability density function above the map of the region considered.

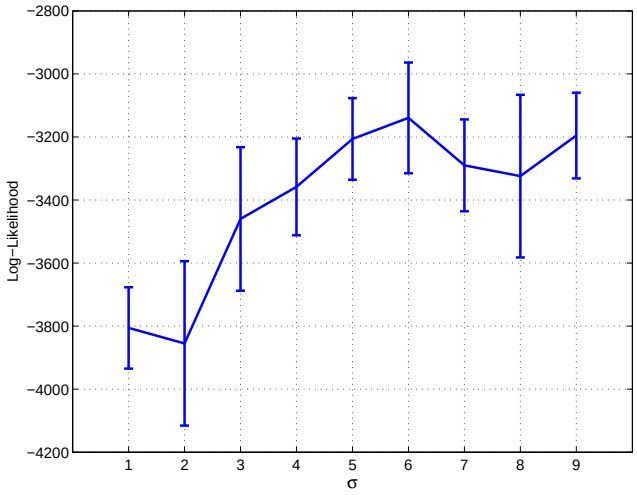


Figure 12: An error-bar plot for a set of four simulations over the set $\sigma = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. The mean value for each σ value is plotted as a line. The error bars describe the standard deviation of the results for each σ value.

5.5. Results Validation

The simulations described in section 5.4 were repeated. Four simulations were run over the set $\sigma = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. A considerable amount of time is required to perform a set of simulations. This limited the number of simulations performed. The error-bar plot of the simulation results is illustrated in Figure 12. The line plot and associated error bars represent the mean values and standard deviations respectively of the log-likelihood results over four simulations for each of the σ values considered. The trend provides a confirmation that the maximum likelihood occurs for $\sigma = 6$.

It may noted that the likelihood does not seem to decrease as σ increases beyond $\sigma = 6$. A cause of this is the structure of the transport vessel routes. A large covariance of a pirate zone will result in larger area considered by the pirate. Pirate attacks will however not occur in regions where no transport vessels sail. The distribution of pirate attacks is thus constrained to the regions in which transport vessels sail. The results illustrated in Figure 10 demonstrate this. Pirate zones with high covariance are simulated. A structure in the simulated pirate attack location distribution is maintained. With reference to Figure 5, the transport routes define the maintained distribution structure. Increasing the pirate zone variance beyond the constraint will not cause a change in the variance of the simulated attacks. The likelihood results will not vary significantly over large values of σ.

Table 1: Log-likelihood values for the pirate attack data of 2011 given the simulation data. The log-likelihood is provided for each of the simulations over the set $\sigma = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. The row containing the maximum likelihood is presented in bold font.

σ	$\log \mathcal{L}(\psi)$
1	-3983
2	-4172
3	-3781
4	-3232
5	-3173
6	**-2987**
7	-3161
8	-3138
9	-3112

5.6. Model Effectiveness

The effectiveness of an information fusion system may be described according to robustness, quality and information gain [67]. Robustness measures the consistency of the model. Quality measures the performance of the model. Information gain measures the ability of the model to provide improvement.

5.6.1. Model Robustness

The robustness of the model may be described by ability of the model to generalise the data. A model that is not able to generalise data is not considered to be robust. The simulated pirate attack locations are not required to be identical to real-world attack locations. A robust model will maintain the form of the spatial distribution while providing a level of uncertainty on the attack locations. A robust model is able to generalise the data.

The results illustrated in Figure 12 provide an indication of the robustness of the model. The standard deviation of the model for each σ is described by the error bars. The log-likelihood seems to vary more over the the σ parameter values than over different simulation instances with the same σ value. This is particularly true for $\sigma \leq 5$. This implies that the model is more strongly affected by the parameter selection than model uncertainty. Furthermore, the standard deviation values remain similar between the various model parameters.

5.6.2. Model Quality

The quality of the model may be described by the similarity between the simulated data and the real-world data. The like-

lihood results discussed in section 5.4 provide an indication of the quality of the model. The maximum likelihood value indicates the model with highest quality. The Bhattacharyya distance may be considered as a simpler and more intuitive measure than the likelihood. The Bhattacharyya distance is however a less rigorous measure.

The Bhattacharyya coefficient between two discrete distributions p_1 and p_2 is defined as [68, 69]:

$$\rho(p_1, p_2) = \sum_x \sqrt{p_1(x)p_2(x)}. \tag{15}$$

The Bhattacharyya coefficient may be explained as the cosine of the angle between the unit vectors formed with p_1 and p_2.

The Bhattacharyya distance between discrete distributions p_1 and p_2 may be calculated as [68, 69]:

$$D_B(p_1, p_2) = \sqrt{1 - \rho(p_1, p_2)}. \tag{16}$$

The discrete distributions of the pirate attack locations are determined using two dimensional histograms. The maps are divided into square cells to form the histogram bins. The distribution p_1 is the histogram determined from the simulated data. The distribution p_2 is histogram determined from the 2011 pirate attack data. Results of distances between the spatial distributions for various histogram bin sizes are provided in Table 2. For small histogram bin sizes, the distributions appear unrelated. For large histogram bin sizes, the distributions are more similar. The results describe the scale at which the model performance becomes acceptable. The model performance becomes acceptable around the 250kmx250km region.

5.6.3. Information Gain (Kullback-Leibler Divergence)

The information gain may be considered as the required information to be gained for the simulated distribution to match the real-world data distribution. The Kullback-Leibler divergence describes information gain. Let $p_1(y)$ describe the distribution for the simulated dataset. Let $p_2(y;\theta)$ describe the distribution of the real-world dataset. This distribution is parametrised by θ. The Kullback-Leibler divergence (D_{KL}) between distributions $p_1(y)$ and $p_2(y;\theta)$ is given as [70, 71]:

$$\begin{aligned} D_{KL}(p_1(y), p_2(y;\theta)) &= \int p_1(y) \log\left(\frac{p_1(y)}{p_2(y;\theta)}\right) dy \\ &= \int p_1(y) \log\left(p_1(y)\right) dy \\ &\quad - \int p_1(y) \log\left(p_2(y;\theta)\right) dy. \end{aligned} \tag{17}$$

The average log likelihood is given by:

$$\mathbb{E}[\log \mathcal{L}(\theta)] = \frac{1}{n} \sum_{i=1}^{n} \log\left(p_2(y_i;\theta)\right). \tag{18}$$

The average log likelihood may be used in approximating (17). Given the law of large numbers, the approximation is given by [70]:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \log\left(p_2(y_i;\theta)\right) = \int p_1(y) \log\left(p_2(y;\theta)\right) dy. \tag{19}$$

The D_{KL} value may be approximated using the GMM, the 2011 pirate attack data and the simulation results. These elements are described in sections 5.1 and 5.2. The approximation of D_{KL} is given by:

$$\begin{aligned} D_{KL}(\bar{b}\|\bar{a}) \approx &\frac{1}{n} \sum_{i=1}^{n} \log\left(q(\bar{a}_i, \psi)\right) \\ &- \frac{1}{n} \sum_{i=1}^{n} \log\left(q(\bar{b}_i, \psi)\right). \end{aligned} \tag{20}$$

The distribution q is the GMM model of the simulated dataset. The variable $\bar{a}$ describes the simulated dataset. The variable $\bar{b}$ describes the real-world dataset.

The D_{KL} values for the various simulation parameters is presented in table 3. The simulation parameters are described in section 5.4. The D_{KL} values are displayed in nats. The minimum D_{KL} value corresponds to the covariance for $\sigma = 6$. This result agrees with the maximum likelihood value displayed in table 1. The minimum D_{KL} value indicates that the corresponding simulation parameters provide the highest information gain.

Table 2: Pirate attack location spatial distribution comparisons between the simulated results and the 2011 attacks. The Bhattacharyya distance and the Bhattacharyya coefficient are provided for various histogram bin sizes in kilometres. The bin sizes are discretised in pixels and converted to approximated distance measures. As a frame of reference, the dimensions of the map are approximately 6400km x 4600km.

Bin Size (pixels)	$\rho(p_1, p_2)$	$D_B(p_1, p_2)$
25kmx25km	0.0358	0.9819
100kmx100km	0.2702	0.8543
250kmx250km	0.6684	0.5758
400kmx400km	0.7988	0.4485
500kmx500km	0.8632	0.3699

6. Future Research and Applications

The implementation of the model is to be refined using real world data and statistics. The EP variable may be expanded to include parameters such as wave hight, wind speed, wind direction, cloud cover and air temperature. Additional parameters may be varied in the optimisation of the model as discussed in section 5.4.

The proposed model is developed for the purpose of simulation and data generation. The data generated by this model shall be utilized for the purpose of developing and testing maritime pirate detection algorithms. Research is being conducted on using a DBN for classification of vessels in the maritime

Table 3: Kullback-Leibler divergence (in nats) the set of simulations over various values of σ.

σ	$D_{KL}(\bar{b}\|\|\bar{a})$
1	6.54
2	7.17
3	5.31
4	2.27
5	1.27
6	**0.27**
7	1.19
8	0.82
9	0.56

environment using the generated data. The DBN classifier is a generalised variation of the proposed model where the class variable is inferred.

The data generated by the proposed model may be utilised in various other applications. For example, the proposed model may be used for multi-sensor simulation. The proposed model contains a plate of sensor variables. The sensor variables could be used in modelling a set of particular sensors. The data generated by the sensors could be used for testing and evaluating multi-sensor information fusion methods. The model is not limited to the maritime piracy application. The variables in the proposed model can be adapted to be applied to other applications such as land or air based applications.

The authors intend to integrate the proposed model into the ICODE-MDA open source tool for maritime domain awareness [72].

7. Summary and Conclusion

A multi-agent generative model is proposed for the purpose of simulating a maritime piracy situation. The model comprises of a SLDS represented in the form of a DBN. The DBN describes a Markovian state based model that determines the behaviour and motion of the modelled vessel. The states of the model are determined by a set of higher level variables whose probability distributions may be inferred from data. The proposed DBN thus provides a versatile model that unifies physical, graphical and probabilistic attributes to model behaviour.

The proposed model is modelled and evaluated with respect to the attack locations of 2011. Optimisation and evaluation is conducted based on likelihood computations of the real-world pirate attack data with respect to the simulated data. The model effectiveness is measured according to quality, robustness and information gain. The Kullback-Leibler divergence is utilised to describe the information gain. The likelihood and Bhattacharyya distance is used to describe the quality. The robustness of the model is measured by the consistency of the model. The proposed model is able to produce unique and varying results while maintaining the structural integrity of the general spatial distributions. The produced spatial distributions correlates well with the real-world data. The evaluation and optimisation methodology may be applied to other behavioural modelling applications.

The data generated by the model may be utilised for various applications. The intended use of the data is for training, testing and evaluating threat assessment methods. Machine learning methods may require training data. Statistical methods may require prior information. In general, most algorithms and methods will require testing and evaluation. The model is able to produce unique and varying results while maintaining the structure of a spatial distribution. This quality is desirable for producing realistic results and for generating suitable data for training, testing and evaluation.

Acknowledgement

This work was supported by the Advanced Sensors and Electronics Defence (ASED) Centre of KACST through the Council for Scientific and Industrial Research (CSIR).

The maps used in the illustrations presented in this work are obtained from Google Maps [73] under the fair use principle.

References

[1] M. Jakob, O. Vaněk, M. Pěchouček, Using agents to improve international maritime transport security, Intelligent Systems, IEEE 26 (2011) 90–96.

[2] ICC-IMB, ICC-IMB Piracy and Armed Robbery Against Ships Report - Annual Report 2011, Annual Report, ICC International Maritime Bureau, 2012.

[3] M. Wooldridge, An Introduction to Multiagent Systems, John Wiley and Sons, Ltd, 2008.

[4] Y. Shoham, K. Leyton-Brown, Multiagent Systems: Algorithmic, Game Theoretic and Logical Foundations, Cambridge University Press, 2009.

[5] C. M. Macal, M. J. North, Tutorial on agent-based modeling and simulation, in: Proceedings of the 37th conference on Winter simulation, WSC '05, Winter Simulation Conference, 2005, pp. 2–15.

[6] G. Weiss, Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence, Intelligent Robotics and Autonomous Agents Series, The MIT Press, 1999.

[7] T. Cioppa, T. Lucas, S. Sanchez, Military applications of agent-based simulations, in: Simulation Conference, 2004. Proceedings of the 2004 Winter, volume 1, 2004, pp. –180. doi:10.1109/WSC.2004.1371314.

[8] S. M. Sanchez, T. W. Lucas, Exploring the world of agent-based simulations: simple models, complex analyses, in: Proceedings of the 34th conference on Winter simulation: exploring new frontiers, WSC '02, Winter Simulation Conference, 2002, pp. 116–126.

[9] T. Dean, K. Kanazawa, A model for reasoning about persistence and causation, Computational Intelligence 5 (1989) 142–150.

[10] J. Pearl, Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference, Representation and Reasoning Series, Morgan Kaufman, 1988.

[11] Y. Luo, T.-D. Wu, J.-N. Hwang, Object-based analysis and interpretation of human motion in sports video sequences by dynamic bayesian networks, Computer Vision and Image Understanding 92 (2003) 196 – 216. Special Issue on Video Retrieval and Summarization.

[12] P. Wiggers, B. Mertens, L. Rothkrantz, Dynamic bayesian networks for situational awareness in the presence of noisy data, in: Proceedings of the 12th International Conference on Computer Systems and Technologies, CompSysTech '11, ACM, New York, NY, USA, 2011, pp. 411–416. doi:10.1145/2023607.2023676.

[13] A. Petrovskaya, S. Thrun, Model based vehicle detection and tracking for autonomous urban driving, Autonomous Robots 26 (2009) 123–139.

[14] S. Das, High-Level Data Fusion, Artech House electronic warfare library, Artech House, Incorporated, 2008.

[15] J. Poropudas, K. Virtanen, Influence diagrams in analysis of discrete event simulation data, in: Winter Simulation Conference, WSC '09, Winter Simulation Conference, 2009, pp. 696–708.

[16] J. Poropudas, K. Virtanen, Simulation metamodeling in continuous time using dynamic bayesian networks, in: Proceedings of the Winter Simulation Conference, WSC '10, Winter Simulation Conference, 2010, pp. 935–946.

[17] J. Poropudas, K. Virtanen, Simulation metamodeling with dynamic bayesian networks, European Journal of Operational Research 214 (2011) 644 – 655.

[18] Y. Bar-Shalom, X. Li, Estimation and Tracking: Principles, Techniques, and Software, The Artech House radar library, Artech House, Incorporated, 1993.

[19] K. P. Murphy, Dynamic Bayesian Networks: Representation, Inference and Learning, Ph.D. thesis, University of California, Berkeley, 2002.

[20] D. Barber, Bayesian Reasoning and Machine Learning, Cambridge University Press, 2012.

[21] V. Pavlovic, J. Rehg, T.-J. Cham, K. Murphy, A dynamic bayesian network approach to figure tracking using learned dynamic models, in: Computer Vision, 1999. The Proceedings of the Seventh IEEE International Conference on, volume 1, 1999, pp. 94–101 vol.1. doi:10.1109/ICCV.1999.791203.

[22] C.-J. Kim, Dynamic linear models with markov-switching, Journal of Econometrics 60 (1994) 1 – 22.

[23] B. Mesot, D. Barber, Switching linear dynamical systems for noise robust speech recognition, Audio, Speech, and Language Processing, IEEE Transactions on 15 (2007) 1850–1858.

[24] H. Wehn, R. Yates, P. Valin, A. Guitouni, E. Bosse, A. Dlugan, H. Zwick, A distributed information fusion testbed for coastal surveillance, in: Information Fusion, 2007 10th International Conference on, 2007, pp. 1–7. doi:10.1109/ICIF.2007.4408089.

[25] M. Kruger, L. Ziegler, K. Heller, A generic bayesian network for identification and assessment of objects in maritime surveillance, in: Information Fusion (FUSION), 2012 15th International Conference on, 2012, pp. 2309–2316.

[26] F. Fooladvandi, C. Brax, P. Gustavsson, M. Fredin, Signature-based activity detection based on bayesian networks acquired from expert knowledge, in: Information Fusion, 2009. FUSION '09. 12th International Conference on, 2009, pp. 436–443.

[27] P. C. G. Costa, K. B. Laskey, K.-C. Chang, W. Sun, C. Y. Park, , S. Matsumoto, High-level information fusion with bayesian semantics, in: UAI 9th Bayesian Modeling Applications Workshop, Catalina Island, CA, 2012, pp. –. Held at the Conference of Uncertainty in Artificial Intelligence (BMAW UAI 2012).

[28] R. Carvalho, R. Haberlin, P. Costa, K. Laskey, K. Chang, Modeling a probabilistic ontology for maritime domain awareness, in: Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on, 2011, pp. 1–8.

[29] Y. Zhang, Q. Ji, Active and dynamic information fusion for multisensor systems with dynamic bayesian networks, Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on 36 (2006) 467–472.

[30] G. Yang, Y. Lin, P. Bhattacharya, A driver fatigue recognition model based on information fusion and dynamic bayesian network, Information Sciences 180 (2010) 1942 – 1954. Special Issue on Intelligent Distributed Information Systems.

[31] V. I. Pavlovic, Dynamic Bayesian Networks for information fusion with applications to human-computer interfaces, Ph.D. thesis, University of Illinois at Urbana-Champaign, 1999.

[32] T. Strang, C. Linnhoff-Popien, A context modeling survey, in: In: Workshop on Advanced Context Modelling, Reasoning and Management, UbiComp 2004 - The Sixth International Conference on Ubiquitous Computing, Nottingham/England, 2004, pp. –.

[33] C. Bettini, O. Brdiczka, K. Henricksen, J. Indulska, D. Nicklas, A. Ranganathan, D. Riboni, A survey of context modelling and reasoning techniques, Pervasive and Mobile Computing 6 (2010) 161 – 180. Context Modelling, Reasoning and Management.

[34] L. S. Kennedy, S.-F. Chang, A reranking approach for context-based concept fusion in video indexing and retrieval, in: Proceedings of the 6th ACM international conference on Image and video retrieval, CIVR '07, ACM, New York, NY, USA, 2007, pp. 333–340. doi:10.1145/1282280.1282331.

[35] J. Gómez-Romero, M. A. Serrano, M. A. Patricio, J. García, J. M. Molina, Context-based scene recognition from visual data in smart homes: an information fusion approach, Personal and Ubiquitous Computing 16 (2012) 835–857.

[36] A. Steinberg, G. Rogova, Situation and context in data fusion and natural language understanding, in: Information Fusion, 2008 11th International Conference on, 2008, pp. 1–8.

[37] J. Garcia, J. Gomez-Romero, M. Patricio, J. Molina, G. Rogova, On the representation and exploitation of context knowledge in a harbor surveillance scenario, in: Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on, 2011, pp. 1–8.

[38] R. Hegde, J. Kurniawan, B. Rao, On the design and prototype implementation of a multimodal situation aware system, Multimedia, IEEE Transactions on 11 (2009) 645–657.

[39] J. George, J. Crassidis, T. Singh, Threat assessment using context-based tracking in a maritime environment, in: Information Fusion, 2009. FUSION '09. 12th International Conference on, 2009, pp. 187–194.

[40] O. Sekkas, S. Hadjiefthymiades, E. Zervas, Enhancing location estimation through data fusion, in: Personal, Indoor and Mobile Radio Communications, 2006 IEEE 17th International Symposium on, 2006, pp. 1–5. doi:10.1109/PIMRC.2006.254053.

[41] O. Sekkas, C. B. Anagnostopoulos, S. Hadjiefthymiades, Context fusion through imprecise reasoning, in: Pervasive Services, IEEE International Conference on, 2007, pp. 88–91. doi:10.1109/PERSER.2007.4283896.

[42] C. Anagnostopoulos, O. Sekkas, S. Hadjiefthymiades, Context fusion: Dealing with sensor reliability, in: Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on, 2007, pp. 1–6. doi:10.1109/MOBHOC.2007.4428752.

[43] O. Vaněk, M. Jakob, O. Hrstka, B. Bošanský, M. Pěchouček, Agentc: Fighting maritime piracy using data analysis, simulation and optimization, 2013. URL: http://agentc-project.appspot.com/.

[44] European Commission: Joint Research Centre., Blue hub - integrating maritime surveillance data, 2013. URL: https://bluehub.jrc.ec.europa.eu/.

[45] R. Middleton, Piracy in somalia: Threatening global trade, feeding local wars, Chatham House, 2008. Briefing Paper.

[46] C. Bueger, J. Stockbruegger, S. Werthes, Pirates, fishermen and peacebuilding: Options for counter-piracy strategy in somalia, Contemporary Security Policy 32 (2011) 356–381.

[47] M. Heger, J. Oberg, M. Dumiak, S. Moore, P. Patel-Predd, Technology vs. pirates, Spectrum, IEEE 46 (2009) 9–10.

[48] O. Vaněk, B. Bošanský, M. Jakob, M. Pěchouček, Transiting areas patrolled by a mobile adversary, in: Computational Intelligence and Games (CIG), 2010 IEEE Symposium on, 2010, pp. 9–16. doi:10.1109/ITW.2010.5593377.

[49] O. Vaněk, M. Jakob, V. Lisý, B. Bošanský, M. Pěchouček, Iterative game-theoretic route selection for hostile area transit and patrolling, in: The 10th International Conference on Autonomous Agents and Multiagent Systems - Volume 3, AAMAS '11, International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC, 2011, pp. 1273–1274.

[50] C. D. Marsh, Counter Piracy: A Repeated Game with Asymmetric Information, Master's thesis, Naval Postgraduate School, 2009.

[51] J. C. Sevillano, D. Rios Insua, J. Rios, Adversarial risk analysis: The somali pirates case, Decision Analysis 9 (2012) 86–95.

[52] H. Liwang, J. W. Ringsberg, M. Norsell, Quantitative risk analysis: Ship security analysis for effective risk control options, Safety Science 58 (2013) 98 – 112.

[53] G. Baldini, D. Shaw, F. Dimc, A communication monitoring system to support maritime security, in: ELMAR, 2010 PROCEEDINGS, 2010, pp. 243–246.

[54] M. Teutsch, W. Kruger, Classification of small boats in infrared images for maritime surveillance, in: Waterside Security Conference (WSS), 2010 International, 2010, pp. 1–7. doi:10.1109/WSSC.2010.5730289.

[55] J. G. Sanderson, M. K. Teal, T. Ellis, Characterisation of a complex maritime scene using fourier space analysis to identify small craft, in: Image Processing and Its Applications, 1999. Seventh International Conference on (Conf. Publ. No. 465), volume 2, 1999, pp. 803–807 vol.2.

doi:10.1049/cp:19990435.

[56] L. Esher, S. Hall, E. Regnier, P. Sanchez, J. Hansen, D. Singham, Simulating pirate behavior to exploit environmental information, in: Simulation Conference (WSC), Proceedings of the 2010 Winter, 2010, pp. 1330–1335. doi:10.1109/WSC.2010.5679060.

[57] D. Koller, N. Friedman, Probabilistic Graphical Models: Principles and Techniques, Adaptive Computation and Machine Learning, MIT Press, 2009.

[58] J. F. Verner, T. D. Nielsen, Bayesian Networks and Decision Graphs, Information Science and Statistics, Springer, 2007.

[59] S. Thrun, W. Burgard, D. Fox, Probabilistic Robotics, Intelligent robotics and autonomous agents series, first ed., MIT Press, United States of America, 2006.

[60] K. Murphy, Switching kalman filters, Technical Report, Dept. of Computer Science, University of California, Berkeley, 1998.

[61] AAPA, The american association of port authorities (aapa) website, 2013. URL: http://www.aapa-ports.org/.

[62] R. Lane, D. Nevell, S. Hayward, T. Beaney, Maritime anomaly detection and threat assessment, in: Information Fusion (FUSION), 2010 13th Conference on, 2010, pp. 1–8.

[63] B. White, K. Wydajewski, Commercial ship self defense against piracy and maritime terrorism, in: OCEANS '02 MTS/IEEE, volume 2, 2002, pp. 1164–1171 vol.2. doi:10.1109/OCEANS.2002.1192131.

[64] S. Percy, A. Shortland, The business of piracy in somalia, Journal of Strategic Studies 0 (0) 1–38.

[65] G. McLachlan, D. Peel, Finite Mixture Models, John Wiley and Sons, inc, Canada, 2000.

[66] Expedition, Somalia pirate activity areas, 2013. URL: http://productforums.google.com/forum/m/#!msg/gec-current-events/x0_XPmUe8HA/x5deCf5gtQ0J.

[67] E. Blasch, P. Valin, E. Bosse, Measures of effectiveness for high-level fusion, in: Information Fusion (FUSION), 2010 13th Conference on, 2010, pp. 1–8.

[68] D. Comaniciu, V. Ramesh, P. Meer, Real-time tracking of non-rigid objects using mean shift, in: Computer Vision and Pattern Recognition, 2000. Proceedings. IEEE Conference on, volume 2, 2000, pp. 142–149 vol.2. doi:10.1109/CVPR.2000.854761.

[69] A. Bhattacharyya, On a measure of divergence between two statistical populations defined by their probability distributions, Bulletin of the Calcutta Mathematical Society 35 (1943) 99–109.

[70] H. Akaike, A new look at the statistical model identification, Automatic Control, IEEE Transactions on 19 (1974) 716–723.

[71] J. Hershey, P. Olsen, Approximating the kullback leibler divergence between gaussian mixture models, in: Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on, volume 4, 2007, pp. IV–317–IV–320. doi:10.1109/ICASSP.2007.366913.

[72] ICODE-MDA, icode-mda website, 2013. URL: https://code.google.com/p/icode-mda/.

[73] Google Inc., Google maps, 2013. URL: maps.google.com.