Scientific Journals
of the Maritime University of Szczecin

Zeszyty Naukowe
Akademii Morskiej w Szczecinie

2015, 43 (115), 115–124
ISSN 1733-8670 (Printed)
ISSN 2392-0378 (Online)

Bi-objective maritime route planning in pirate-infested waters

Ondřej Vaňek, Ondřej Hrstka, Štěpán Kopřiva, Jan Faigl, Michal Pěchouček

Czech Technical University in Prague, Faculty of Electrical Engineering, Department of Computer Science
2 Technicka St., Praha 6, Czech Republic, e-mails: {vanek;hrstka;faigl;kopriva;pechoucek}@agents.fel.cvut.cz

Key words: maritime piracy, risk-aware planning, optimization, risk analysis, modeling, FTA

Abstract

Contemporary maritime shipping is subject to a large number of constraints given by tight shipping schedules and very low margins. Additionally, problematic areas with increased security needs dynamically changing in time, combined with seasonal oceanographic and meteorological conditions pose a challenging voyage planning problem. In this work we present a risk-aware voyage planner taking into account spatio-temporal environmental conditions. The planner is based on a graph-based search algorithm A*. We discretize the required area into a graph, we store various layers of information into the edges of the graph (such as risk and weather conditions) in a form of numeric weights and we define a bi-objective planning problem with a trade-off between security and duration of the voyage. The nature of the algorithm guarantees a complete and optimal solution in a form of an optimized voyage with respect to the criterion function composed of the two weighted components, i.e, duration and security of the voyage.

We demonstrate the approach on our area of interest: Indian Ocean. We use NATO piracy activity risk surface as the risk layer and we compute all transit voyages between relevant routing points in the area. Finally, thanks to the discretization of the problem, we are able to integrate corridors imposed by the shipping authorities and evaluate additional what-if scenarios with extended corridor systems. The resulting planner is exposed to the public using a web service with an easy interface requiring start time of the voyage and the origin and the destination point of voyage. Combined with an expressive visualization, this tool demonstrates the capabilities of the proposed solution.

Introduction

Contemporary maritime piracy presents a significant threat to global shipping industry, with annual costs estimated at up to US$7bn. To counter the threat, policymakers, shipping operators and navy commanders need new data-driven decision-support tools that will allow them to plan and execute counter-piracy operations most effectively. So far, the provision of such tools has been limited.

We focus on the problem of maritime routing under the risk imposed by the maritime piracy. Specifically, the captains need to decide which path to take through the dangerous area to minimize the length of the route and to minimize the risk. However, these two criteria are opposing each other thus, given different and complex risk maps for different days and conditions, the problem of optimal criteria weighting is non-trivial.

Currently, the problem is solved either by hand or neglected, minimizing the transit time through the area without the examination of the risk map. The high risk area is typically represented by a polygon and the risk inside the polygon is considered constant. This rough approximation can be significantly improved by considering fine-grained risk map and explicit criterion weighing.

We propose a planner based on a bi-objective function, weighing the risk taken along the route as well as the length of the route itself. It can take any kind of risk map on the input and produce a route through the dangerous area by optimizing the objective function. We utilize graph-based discretization of the area and A*-based planner to find the optimal route.

To access the planner we have created a website where the users can put in their coordinates and retrieve the optimal route. Also, the website allows computation of risk along a route defined by the user. The planner is also integrated into the AgentC platform, allowing modeling and execution of

complex scenarios containing merchant ships, pirates and counter-piracy forces.

Related work

In the maritime domain, applications of similar approach to solve routing problems are surprisingly scarce. If we look closer at existing maritime models, existing work either focuses on traffic in ports and national, coastal waters (Hasegawa et al., 2004) or uses high-level equation-based models (Bourdon, Gauthier & Greiss, 2007) unfit for capturing individual-level behavior and inter-vessel interactions essential for modeling maritime piracy. Furthermore, none of the above models is concerned with the security of maritime shipping lanes.

As far as the security angle on transportation systems is concerned, existing simulations focus on modeling activities in and around terminals rather than within transportation networks themselves. This is true both for airport security (Chawdhry, 2009) and port security (Koch, 2007). The spatial, network aspect of transportation security has been touched upon in the work on modeling critical infrastructures (Barton & Stamber, 2000), however, the emphasis there is mostly on other than transportation types of infrastructures. The problem of securing transportation infrastructures and logistical networks has only been studied in the military context (Sebbah, Ghanmi & Boukhtouta, 2011).

Focusing on the very phenomenon of maritime piracy, existing work is concentrated primarily in the fields of security studies, international relations and global policy (Onuoha, 2010). Only recently, initial attempts at applying computational modeling and optimization to maritime piracy have emerged but focus exclusively on military aspects of the problem: (Bruzzone et al., 2011) model piracy around the Gulf of Aden using the discrete-event simulator PANOPEA. The authors focus on evaluating the efficiency and effectiveness of different Command and Control models; only main actors in the Gulf of Aden are considered and the simulation is not scaled to the Indian Ocean where the merchant traffic model is significantly more complicated.

Tsilis (Tsilis, 2011) employs the MANA agent-based modeling framework (Lauren & Stephen, 2002) to identify key factors affecting the escort of vulnerable merchant vessels through the Gulf of Aden. The escorting scenario is modeled on a tactical level, focusing on positioning of individual ships and protection of one group of merchant vessels; this is different from our model which adopts a whole-system perspective and considers the security of maritime transportation system as a whole. The MANA framework is also used by (Decraene, Anderson & Low, 2010) to analyze requirements on non-lethal deterrents for defending large merchant vessels against pirate attacks; again, the focus is on the tactical level of modeling a single encounter in detail, rather than the system as a whole.

Wong and Yip (Wong & Yip, 2012) use binary choice models to estimate the success or failure of pirate attacks as a function of vessel type, flag, vessel operation, number of pirates, boarding methods, and arms type. They demonstrate that three major approaches for pirate attacks, with the different approaches being associated with different levels of violence and arms used and different targets. Their conclusions can be used to better estimate specific types of risks within an area, however, additional assessment is required to decide how to route a vessel.

Slootmaker (Slootmaker, 2011) describes *Next-generation Piracy Performance Surface* (*PPSN)* model which employs meteorological forecasts, intelligence reports and historical pirate incidents to predict areas conductive to pirate activity around the Horn of Africa.

Hansen et al. (Hansen et al., 2011) further improve the PPSN model by refining the environment model and adding a probabilistic behavioral pirate model, resulting into the *Pirate Attack Risk Surface* (*PARS*) model. Both PPSN and PARS models are numerical with only a minor simulation component and are limited to short-term forecasts (several days). They do not directly model real-world behavior and interactions of individual vessels; consequently, their applicability for what-if type of analysis is limited.

Domain background

Before diving into the description of the planner we describe the nature of pirate attacks using standard data analysis. Our piracy risk estimation method uses data about reported piracy incidents and data about long-haul shipping traffic in different regions and time periods. We first describe the data and then present the risk estimation framework itself and its integration into a web application for transit route risk assessment.

Piracy incident analysis

To our best knowledge, there are no publicly available sources of pirate vessel trajectories. Only information about reported pirate incidents is available. This section therefore provides an analysis of piracy incidents between from year 2005 to year 2010. We have applied data mining methods

on the piracy incident data to discover relationships between geographical, environmental and other factors affecting pirate activity. This analysis is similar to that provided in piracy reports from the IMB Piracy Reporting Centre (e.g. United Kingdom. ICC International Maritime Bureau, 2000), which are available for internal use, http://www.icc-ccs.org/home/piracy-reporting-centre.

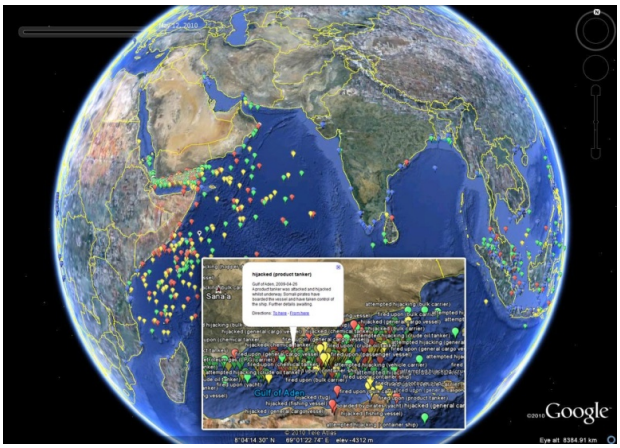


Figure 1. IMB piracy incident dataset 2005–2010 (global view and Gulf of Aden detail)

1) *Incident Data Description:* The data used for the analysis consists of the total of 1,671 records of pirate incidents from the years 2005 to 2010, which have been obtained from the IMB Piracy Reporting Centre website, http://www.icc-ccs.org/home/piracy-reporting-centre/ imb-live-piracy-map-2010. Each incident record has the following fields:

- *incident number* [*Integer*] – unique identifier of the event;
- *latitude*, *longitude* [*GPS*] – geographical coordinates of the event;
- *vessel type* [*String*] – type of vessel attacked;
- *location* [*String*] – verbal description of the location;
- *date* [*Date*,*time*] – date and time of the event;
- *attack type* [*Enum*] – category of the attack: attempted, boarded, hijacked, fired upon, suspicious.

2) *Incident Data Analysis:* We have analyzed the distance of attacks from the nearest shore in the area around east Africa, in the Gulf of Aden and in the Red Sea: most attacks take place near the shore, although some attacks take place very far from the coast, some up to 1500 nm from the Somali coast; furthermore, the average distance of attacks has been increasing in time. In 2005, pirates attacked mainly near the shore; in 2010 attacks happened more and more often far away from the shore. Further on, periods of increased frequency of attacks and periods of "silence" can be observed which are correlated with changing weather and sea conditions in different year seasons.

Additionally, we analyzed the effect of International Recommended Transit Corridor (IRTC) placed in the Gulf of Aden on the number of attacks. The pirates were able to adapt to new routing schemes and, after the introduction of the corridor, the pirates shifted their activity to attack ships sailing within the corridor.

Also a significant number of attacks took place in international waters and in Yemen's exclusive economic zone waters, which is because of the close proximity of IRTC to these areas.

3) *Geographical Shift of Pirate Activity:* Piracy incident records from years 2011–2014 (which can be found at the International Chamber of Commerce – Commercial Crime Services (ICC CSS) website, http://www.ice-ccs.org/) suggest that pirate activity is no longer focused on the Gulf of Aden. This is probably due to the success of international counter-piracy operations in the Gulf of Aden. Thanks to equipment upgrades, paid for mainly from the ransoms collected, pirates are now also able to attack vessels up to 1,500 nm from the Somali coast. Consequently, pirate activity has shifted into the Indian Ocean which is a much larger and consequently more difficult-to-protect area.

We have analyzed piracy incident reports from ICC CCS website. Incident densities in each year are depicted in Figure 2. Up until 2008, there is a noticeable increase in the number of incidents in the Gulf of Aden. Since 2009, the shift from Gulf of Aden to the Indian Ocean has been taking place. In 2010, the incidents are clearly scattered over the northern part of the Indian Ocean. On the contrary, the number of incidents in Gulf of Aden in 2010 has decreased compared to 2008. If the trend continues, more effective patrolling schemes will have to be employed to effectively battle the piracy threat in the open ocean. Additional information about changes in the areas of pirate activity can be found in McGuire, 2009.

The analysis shows an overall trend of maritime piracy in given years: the pirates are able to cover parts of the Indian Ocean almost reaching to the coast of India. Additionally, the pirates react to the introduction of countermeasures (such as the IRTC corridor).

Long-haul transportation traffic analysis

AIS data can be used to analyze traffic patterns of long-haul transportation vessels. Due to the very high cost of obtaining historical AIS data, our analysis is limited to a sample of global satellite

AIS data provided by ORBCOMM satellite data provider, http://www.orbcomm.com/services-ais.htm. The dataset contains AIS messages from all areas of the world for two days from 2010-01-28 00:00:00 to 2010-01-29 22:45:06. In total, 101,432 AIS messages about 15,350 vessels are provided. Each message carries information about current vessel position, speed, rate of turn and other information according to the AIS data specification, http://en.wikipedia.org/wiki/Automatic_Identification_System.

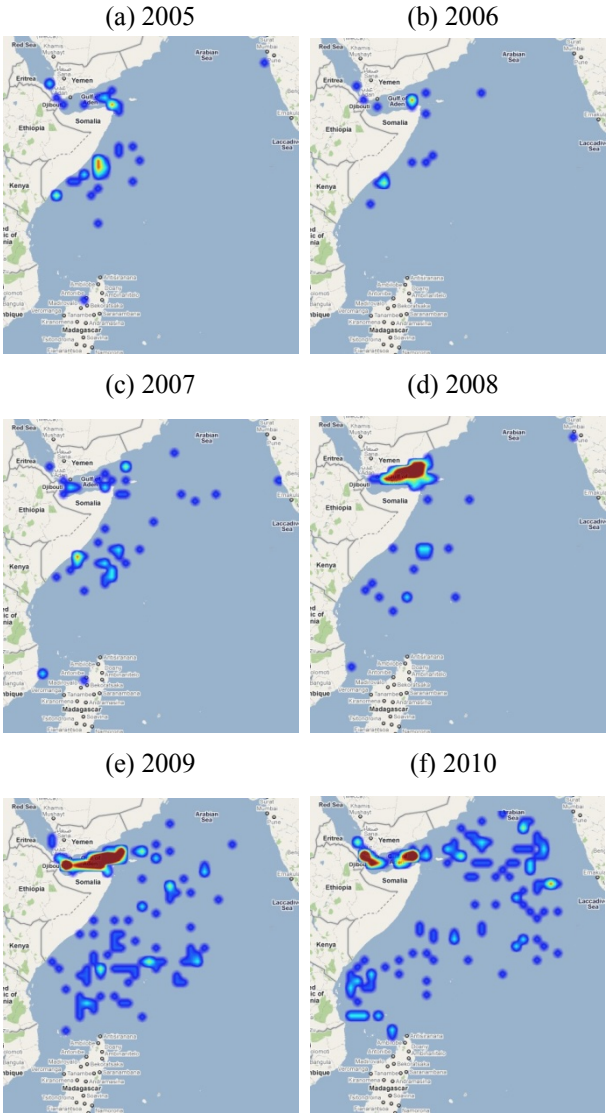


Figure 2. Densities of piracy incidents in the years 2005–2010. It can be observed how the piracy activities spread throughout the Indian Ocean as the time progressed

Unfortunately, the coverage of individual vessels varies greatly – for some vessels, a large number of messages is available; for most of the vessels, however, the coverage is relatively sparse and their trajectories thus cannot be reliably reconstructed. However, it is possible to observe the alignment of the traces with the IRTC in the Gulf of Aden (in a detailed window).

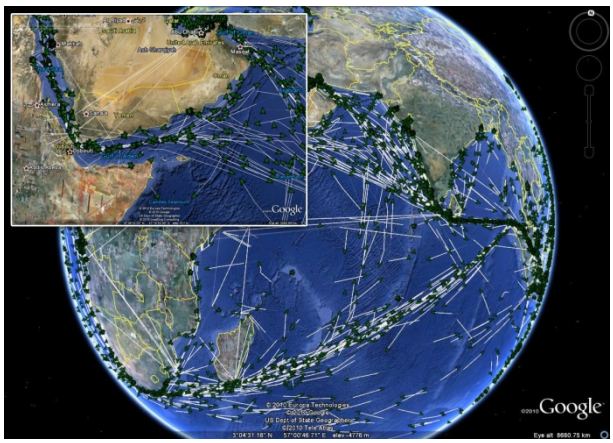


Figure 3. Ship trajectories from the ORBCOMM AIS data set (global view and Gulf of Aden detail)

From this analysis we can see, that direct utilization of AIS data is not possible, however, it is possible to extract some trends about long-haul traffic. These trends can be then used to validate generative models of long-haul traffic; the generative models can then be used to conduct a range of what-if analyses which is not possible to do with the AIS data.

Risk model

The ability to estimate the probability of pirate attack is essential in managing the risk of maritime transportation. When planning the vessel route, such an estimate can be used to find the desired compromise between the risk of attack and the length of the route. When deploying maritime patrols, the estimate can be used to schedule more frequent visits to locations with higher estimated probability of attack.

The most intuitive way to estimate the risk is to calculate the estimated number of incidents that happen in a particular geographical area during a specific time interval and divide it by the estimated total number of cargo vessels passing through the area in the same time interval. The resulting number corresponds to an estimate of the probability of pirate attack for the specific geographic area and specific time interval. For a vessel traversing multiple areas, the probability has to be correctly aggregated to estimate the probability of attack along the whole vessel's route. In this section, we first formalize the method described above.

We also show how to calculate the probability of attack for a specific vessel trajectory. Finally, we describe a prototype of a web application for assessing piracy risk along a specified route.

Abstract risk modeling framework

The proposed framework permits evaluation of the attack probability for a specified vessel trajectory. The framework uses historical data to create a risk map and to evaluate the probability of attack by employing curve integration along the vessel's route.

The main assumption of the framework is that observed traffic density and pirate attacks are realizations of probability distribution functions. We then look for aggregated estimates of these distributions. To do that, we first need to divide the area of interest $S \subset \mathrm{R}^2$ into n subareas a_i that satisfy:

$$\bigcup a_i = S \text{ and } \bigcap a_i = 0 \tag{1}$$

Let T_i be the estimated total time spent by vessels in area a_i; let I_i be the estimated number of incidents for area a_i during the same time interval. Then, the estimated number of incidents that would occur if a ship spends one time unit in area a_i can be expressed as:

$$N_i = \frac{I_i}{T_i} \tag{2}$$

The risk map is then defined as a function r: $\mathrm{R}^2 \to \mathrm{R}$:

$$r(x,y) = N_i \quad \text{if} \quad (x,y) \in a_i \tag{3}$$

The estimated number of incidents of a vessel that follows a trajectory T can then be calculated by the following curve integral:

$$N_T = \int_T \frac{r}{v} \mathrm{d}s \tag{4}$$

where $v(x, y)$ is the traveling speed of the vessel at location (x, y). For a constant vessel traveling speed, we can write:

$$N_T = \tau \int_T r \,\mathrm{d}s \tag{4}$$

where τ is the total travel time along T.

Finally, we can calculate the probability that a vessel will be attacked at least once along its trajectory T using the Poisson probability distribution function. Let

$$f(k,\lambda) = \frac{\lambda^k e^{-\lambda}}{k!} \tag{6}$$

be the probability that an event with the rate of occurrences λ occurs exactly k time in a given unit interval. We can then calculate the probability that a pirate attack happens exactly zero times as

$$P_T' = e^{-N_T} \tag{7}$$

which gives us:

$$P_T = 1 - e^{-N_T} \tag{8}$$

as the probability that the vessel will be attacked at least once along its trajectory T.

Risk-aware planner

A fundamental part of the merchant vessel operation is route planning.

Route planning is modeled as an optimization problem of finding an optimal route between *origin* and *destination* points on a sphere, given vessel-specific route optimality criterion, a set of constraints imposed by geographical obstacles and physical properties of the vessel, and a spatial piracy risk function (the latter only when voyage planning is performed for merchant vessels).

Optimization problem

In more formal view, the optimal route selection problem can be formalized as a bi-objective optimization problem in the following form:

$$\min \ \mathcal{L}(x), \mathcal{R}(x) \tag{9}$$

$$\text{s.t. } x \cap O = 0 \quad \forall O \in \mathcal{O} \tag{10}$$

where x is the sought route that does not intersect with any geographical obstacles represented as a set $\mathcal{O}$ of spherical polygons $O \in \mathcal{O}$, $\mathcal{L}(x)$ is length of the route and $\mathcal{R}(x)$ is risk along the route. We transform the criterion into a single function using an aggregation method (Hwang & Masud, 1979) with a single weight α, termed *risk aversion* coefficient (which can be set individually for each merchant vessel agent based, e.g., on the level of onboard security, vessel cruising speed or the value of its cargo):

$$\min \ (1-\alpha)\mathcal{L}(x) + \alpha \, \mathcal{R}(x) \tag{11}$$

The problem is hard to solve optimally in the continuous space, we thus discretize the region and formalize the problem as path-finding on a graph: we define a *risk area* as additional spherical polygon $O_{\mathcal{R}}$ which we divide into a rectangular grid graph with predefined cell widths for the Indian Ocean and the Gulf of Aden (see Figure 5a) to construct the navigation graph.

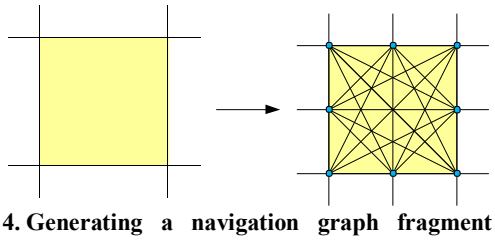
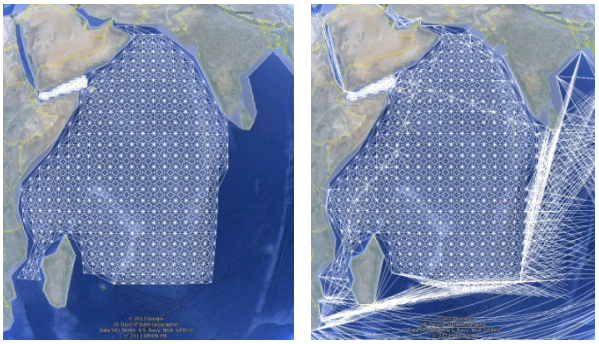


Figure 4. Generating a navigation graph fragment for a single grid cell

The process of generating a fragment of the rectangular grid graph corresponding to a single grid cell a_i is shown in Figure 4: each cell boundary is split into n segment and graph vertices are placed at the ends of these segments. A complete graph connecting these vertices is then created and topologically redundant edges are removed.



(a) (b)

Figure 5. (a) rectangular grid representing the risk area, (b) cell-grid connected to the visibility graph

We construct *spherical visibility graph* from the spherical polygons $\mathcal{O} \cup O_{\mathcal{R}}$ by adding an edge between any two polygon vertices connectible by a geodesic (the shortest path between two points on the surface of a sphere) which does not intersect any polygon (Figure 5b) and we connect the origin and destination points to this graph by edges that do not intersect any other edge already in the graph. The visibility graph is then connected to the rectangular grid graph forming a navigation graph $\mathcal{G}$.

Finally, to each edge in the grid in $O_{\mathcal{R}}$, we assign a risk value in the interval [0, 1] from a spatial risk function which is provided by, e.g., the NATO Shipping Centre (http://www.shipping. nato.int), synthetically generated as described above, or provided by the user. The risk value on the remaining edges outside of the risk area is set to 0.

Optimum vessel route in the navigation graph with respect to the criterion (11) is then computed using the A* algorithm (Russell et al., 2010) with orthodromic distance (the shortest distance between any two points on the surface of a sphere) heuristics and with the cost function equal to the criterion function.

Case studies

This section presents a set of case studies conducted with the PARS risk model to demonstrate the capabilities of the planner.

All routes

Figure 6 depicts a PARS map with all routes between all significant harbors around the Indian Ocean. The risk coefficient $\alpha = 0.5$ weighing the distance and the risk equally.

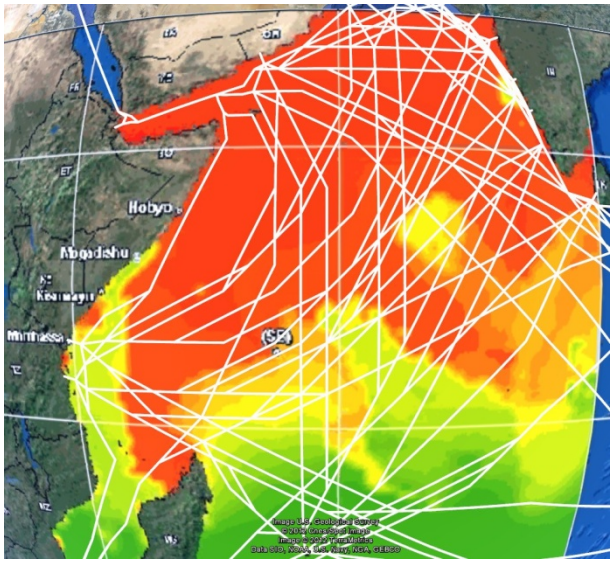
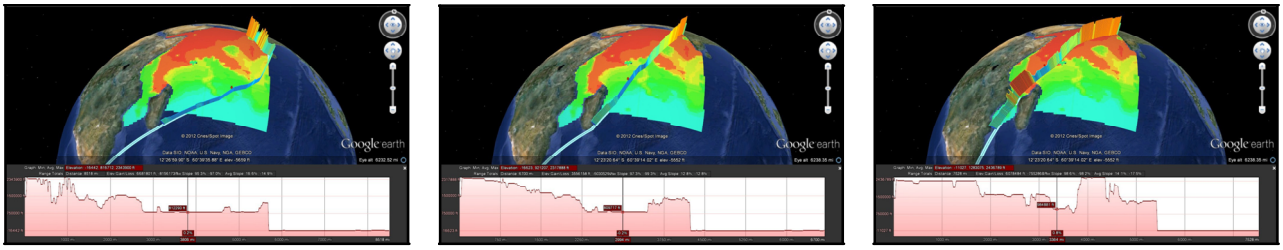


Figure 6. PARS model for October 1st, 2011, provided by NATO Shipping centre – green, yellow, red colors correspond to low, medium and high risk of attack respectively; plans are generated for each significant harbor close to the Indian Ocean; the risk aversion coefficient is set to $\alpha = 0.5$

Single route case study

We evaluate the planner on a number of specific routes crossing the area of the Indian Ocean. Here we demonstrate its capabilities on a route from Mumbai to Cape Town.



(a) (b) (c)

Figure 7. The figures depict three routes from Mumbai to Cape Town. The first case on the left figure minimizes the route's length, the middle case balances the length of the route and the risk along the route, the third figure presents a case with a route minimizing the risk

Figure 7 shows three variants of routes with risks along the route depicted below each route. Figure 7a shows a shortest route measuring 4,790 nautical miles. Figure 7b shows a route with a coefficient 0.5 weighing risk and length equally. The route is 4,891 nautical miles long. The longest route with the lowest risk is depicted in Figure 7c. The path is 5,599 nautical miles long and the risk is the lowest possible given the origin and the destination.

Case study on the AgentC framework

We have applied the developed planner to several real-world cases, based in part on discussions with maritime domain stakeholders. Here we present one particular case study focusing on analyzing the possibility of introducing transit corridor system in the Indian Ocean.

The existing International Recommended Transit Corridor (IRTC), established in 2009, has proven – in combination with the deployment of navy vessels – a very effective tool in reducing the number of successful pirate attacks in the Gulf of Aden. The maritime security community has been discussing the possibility of establishing additional corridors in the Indian Ocean, where most pirate activity takes place following pirates' displacement from the Gulf of Aden. In contrast to the Gulf of Aden, which is an elongated, narrow area with a simple bidirectional traffic flow, the Indian Ocean is much larger and criss-crossed, in all directions, by a multitude of traffic flows. This makes the design of an effective corridor system a complicated task.

We have utilized the AgentC framework to evaluate the case study (see section *AgentC framework* for a brief description of the framework). We have extended the framework to include the risk-based planner and the graph was extended for corridors to allow the vessels to sail within the corridors. The risk in corridors was set to 0 to simulate the strong recommendation of transiting the area through the corridor. The risk in the areas outside of the corridor was taken from the PARS risk map (see Figure 6).

Scenarios

We studied the effect of two possible layouts of Indian Ocean corridor systems: (1) single west-east corridor channeling the large amount of west- and east-bound traffic (denoted as Single-IO), and (2) a more extensive multi-corridor system covering all the main traffic flows in the Indian Ocean (denoted as Multi-IO). See Figure 8 for a scheme of corridor layouts. We compared the results with the current setup where no corridors are used in the Indian Ocean (denoted as None-IO). The existing IRTC corridor was considered in all three configurations.

In addition to the corridor layout, we were interested in assessing synergies between corridors and other counter-measures, specifically in assessing employing group transit schemes within the corridors and deploying of navy vessels alongside the corridors. In addition to the corridor layout, we therefore included the number of deployed navy warships ($\#N = \{20,30,40,50,60,80,100\}$ and the use of group transit ($group\text{-}transit = \{YES, NO\}$) as additional study parameters. In order to make the assessment more robust with respect to the variation of future pirate activity, we also included the number of active pirates ($\#P = \{1,2,3,4\}$) as a study parameter.

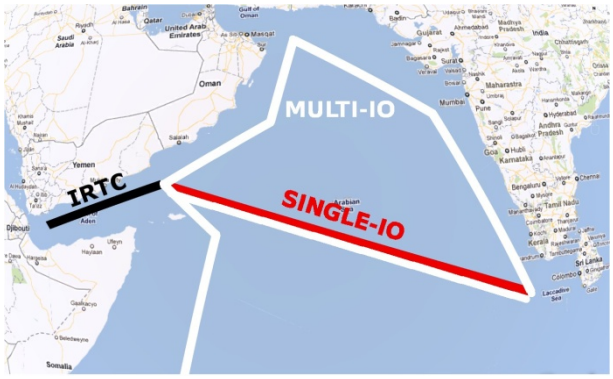


Figure 8. Corridor layouts for the Indian Ocean corridor system. The Single-IO layout only uses IRTC with the red east-west corridor; the Multi-IO layout utilizes all depicted corridors

Results

The results given are for one year of simulated maritime traffic. Due to probabilistic nature of part of the model, we simulated each configuration for 50 runs and present average values together with standard errors.

The values of the average transit distance (in nautical miles) and average transit duration (in hours) only depend on the layout of the corridor system and amounted to 2153 nm / 141 h for the None-IO setup with no corridors in the Indian Ocean, 2162 nm / 142 h for the Single-IO and 2213 nm / 145 h for the Multi-IO corridor setups. The small difference between different corridor settings is due to the positioning of corridors copying main natural shipping lanes. The traffic is not re-routed significantly by the introduction of the corridors.

Figure 9a captures the dependency of the number of hijacks on the number of navy vessels

for each corridor system, averaged over different numbers of pirates. As expected, increasing the number of navy vessels decreases the number of both attempted and successful attacks. The reduction in attempted attacks is caused by a denser navy presence, which causes the pirates not to launch attacks when a navy vessel is nearby. The reduction in successful attacks is then caused, additionally, by more frequent attack disruption allowed by the higher density of navy vessels – this can be seen in Figure 9b which depicts a detailed breakdown of attack outcomes for the Multi-IO corridor system. When the number of navy vessels is increased to a certain level, most of the attacks are successfully disrupted.

What is more interesting is the finding that in order to have positive impact on reducing hijacks, the extended corridor systems (Single-IO and Multi-IO) have to be patrolled by a high number of navy vessels (approximately 70 and more). For fewer than 40 navy vessels, the introduction of the corridors in the Indian Ocean actually worsens transit security (keep in mind that, as suggested in the validation section, quantitative results are only indicative).

This is because the better predictability and higher concentration of merchant traffic inside the extended corridors systems makes targeting vessels easier for pirates. This can be seen in Figure 9c – the number of attempted attacks for the Multi-IO remains higher than for the None-IO setup even for very high numbers of navy vessels. The ratio of disrupted attacks to the number of all attacks (depicted in Figure 9d) can be seen as navy vessel efficiency. This efficiency rises with increasing the number of deployed navy vessels. More inter-

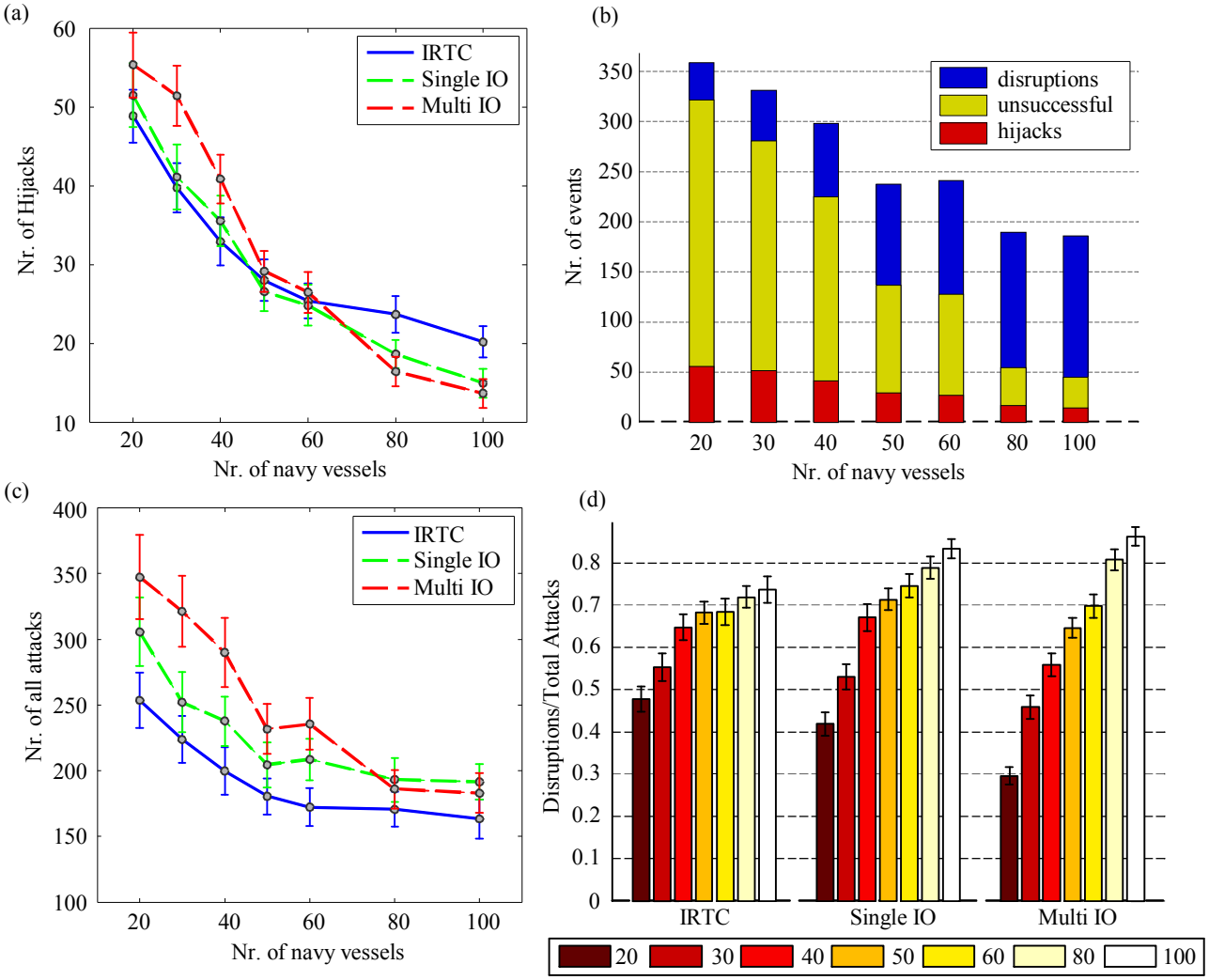


Figure 9. Results of the Corridor system study. (a) Dependency of the number of hijacks on the corridor system and the number of navy vessels (lower is better). (b) Breakdown of the different attack types for Multi-IO corridor system. (c) Dependency of the number of all attacks on the corridor system (lower is better). (d) Dependency of the ratio of intercepted attacks on the number navy vessels – we can observe boost of navy vessel efficiency by the introduction of extended corridor systems, when enough navy vessels are available (higher is better)

estingly, the Single-IO and Multi-IO systems lead to higher navy vessel efficiency (though this increase is not enough to counter the increase of attempted attacks). The use/not use of group transit has an insignificant effect in the current model – this may change if more sophisticated patrolling strategies which coordinate navy vessels with transit groups are employed.

Overall, the results suggest that the positive effect of transit corridors is not directly transferable from the small and narrow Gulf of Aden into the vast Indian Ocean. This is not surprising given the complex nature of the inter-dependencies in the maritime transportation system; it is exactly the kind of conclusions that is difficult to reach without in-depth simulation modeling (e.g., by employing data analysis techniques only).

A key limitation of the study lies in the simple static deployment of navy vessels. More elaborated patrolling and convoy formation strategies could be more effective and allow the extended corridor systems to be successfully patrolled with fewer vessels. The agent-based design and implementation of the simulator makes introduction of such strategies into the model straightforward.

AgentC framework

AgentC framework is a data-driven agent-based simulation model of maritime activity in piracy-affected waters. The model aims to help decision makers reduce uncertainty about the effects of their operational control and regulatory interventions. The model incorporates a wide range of real-world data and, to our best knowledge, is the first computational model that simulates deep sea shipping down to the level of individual vessels. This is crucial for accurately capturing emergent, collective effects arising from the context-dependent interactions of merchant, pirate and navy vessels.

More information is accessible on the project website (http://agents.felk.cvut.cz/projects/agentc) or described in (Vaněk, 2013).

Web application risk modeling

To facilitate access to our risk assessment method, we have integrated the piracy risk estimation method into a web application. The application allows the user to specify its planned transit route using a Google Map-based web interface. It then outputs the overall risk and also annotates individual route segments with their associated risk. See a screenshot of the application in Figure 10.

The planner is not currently exposed to the public, however, it is integrated within the AgentC framework to provide more realistic behavior of the simulated vessels.

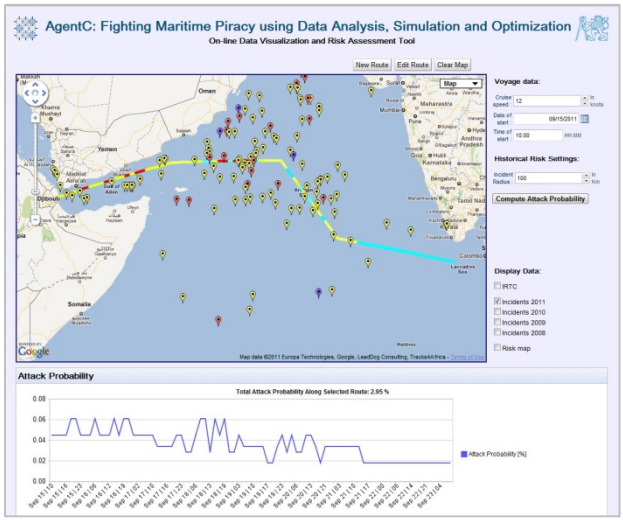


Figure 10. A prototype of a web application for route piracy risk analysis. A map-based view of the route with a risk along the route depicted below

Conclusions

Facing the various security threats on the high seas, the ship-masters need effective decision support tools to be able to navigate dangerous waters. We have developed a route planner able to weigh security risks and the length of the route. The planner takes into account a risk model which can be provided by a third party. The risk is mapped onto a graph which represents the space over which the route is planned. We then utilize standard A* algorithm to find optimal route with respect to the pre-selected risk aversion coefficient.

We have applied our approach to the case of maritime piracy where we demonstrate its capabilities. We show a simple model of maritime activity in piracy-affected waters. The model aims to help decision makers reduce uncertainty cases of planning between two points on the globe as well as more advanced scenarios taking into account all relevant harbors around the Indian Ocean. Finally, we integrate the planner into the AgentC framework which we use to evaluate a set of scenarios integrating different corridor systems into the transit system.

Acknowledgments

The research presented in this paper was supported by the Office of Naval Research grant No. N000140910537, by the Office of Naval Research grant No. N62909-14-1-N231 and by the Czech Science Foundation (GAČR) under research project No. 13-18316P.

References

1. BARTON, D.C. & STAMBER, K.L. (2000) *An agent-based microsimulation of critical infrastructure systems*. Technical report. Sandia National Labs., Albuquerque, NM (US); Sandia National Labs., Livermore, CA (US).
2. BOURDON, S., GAUTHIER, Y. & GREISS, J. (2007) *MATRICS: A maritime traffic simulation*. Technical report. Defence R&D Canada.
3. BRUZZONE, A.G., MASSEI, M., MADEO, F., TARONE, F. & GUNAL M.M. (2011) Simulating marine asymmetric scenarios for testing different C2 maturity levels. In: *Proceedings of the 16th International Command and Control Researh and Technology Symposium*. pp. 12–23.
4. CHAWDHRY, P.K. (2009) Risk modeling and simulation of airport passenger departures process. In: *Proceedings of the 2009 Winter Simulation Conference*. Austin, TX, 13–16 Dec. 2009. IEEE. pp. 2820–2831.
5. DECRAENE, J., ANDERSON, M. & LOW, M.Y.H. (2010) Maritime counter-piracy study using agent-based simulations. In: *Proceedings of the 2010 Spring Simulation Multiconference*. New York: ACM. pp. 82–89.
6. HANSEN, J., JACOBS, G., HSU, L., DYKES, J., DASTUGUE, J., ALLARD, R., BARRON, C., LALEJINI, D., ABRAMSON, M., RUSSELL, S. & MITTU, R. (2011) Information domination: Dynamically coupling METOC and INTEL for improved guidance for piracy interdiction. *NRL Review*. pp. 110–115.
7. HASEGAWA, K., HATA, K., SHIOJI, M., NIWA, K., MORI, S. & FUKUDA, H. (2004) Maritime traffic simulation in congested waterways and its applications. In: *4th Conference for New Ship and Marine Technology*. Chine, pp. 195–199.
8. HWANG, CH.-L. & MASUD, A.S. (1979) *Multiple objective decision making: methods and applications*. Berlin: Springer-Verlag.
9. KOCH, D.B. (2007) PortSim – a port security simulation and visualization tool. In: *Proceedings of 41st Annual IEEE International Carnahan Conference on Security Technology*. IEEE. pp. 109–116.
10. LAUREN, M. & STEPHEN, R. (2002) Map-aware non-uniform automata (MANA)-a New Zealand approach to scenario modelling. *Journal of Battlefield Technology*. 5. pp. 27–31.
11. MCGUIRE. G. (2009) Combined Maritime Forces (CMF) – who we are and wider military counter piracy update. Brief presented at the MARLO Maritime Conference, Dubai, UAE. December 2009. Availabe from: http://www.cusnc.navy.mil/marlo/Events/DEC09-MARLO-DubaiConference.htm
12. ONUOHA, F.C. (2010) Piracy and maritime security off the Horn of Africa: Connections, causes, and concerns. *African Security*. 3(4). pp. 191–215.
13. RUSSELL, S.J., NORVIG, P., DAVIS, E., RUSSELL, S.J. & RUSSELL, S.J. (2010) *Artificial intelligence: a modern approach*. New Jork: Prentice Hall.
14. SEBBAH, S., GHANMI, A. & BOUKHTOUTA, A. (2011) Modeling and simulation of military tactical logistics distribution. In: *Proceedings of the 2011 Winter Simulation Conference*. Phoenix, AZ, 11–14 Dec. 2011. IEEE. pp. 2507–2518.
15. SLOOTMAKER, L.A. (2011) *Countering piracy with the next-generation piracy performance surface model* (master thesis). Technical report, Naval Postgraduate School. Monterey California.
16. TSILIS, T. (2011) *Counter-piracy escort operations in the Gulf of Aden* (master thesis). Technical report, Naval Postgraduate School, Monterey California.
17. United Kingdom. ICC International Maritime Bureau (2000) *Piracy and armed robbery against ships*. Technical report. London: Cinnabar Wharf, 24 Wapping High Street.
18. VANĚK, O., JAKOB, M., HRSTKA, O. & PĚCHOUČEK, M. (2013) Agent-based model of maritime traffic in piracy-affected waters. *Transportation research part C: emerging technologies*. 36. pp. 157–176.
19. WONG, M.CH. & YIP, T.L. (2012) Maritime piracy: an analysis of attacks and violence. *International Journal of Shipping and Transport Logistics*. 4(4). pp. 306–322.