Using Multi-agent Simulation to Improve the Security of Maritime Transit

Ondřej Vaněk, Michal Jakob, Ondřej Hrstka, and Michal Pěchouček

Agent Technology Center, Dept. of Cybernetics,
Faculty of Electrical Engineering, Czech Technical University,
Technická 2, Praha 6, Czech Republic
{vanek,jakob,hrstka,pechoucek}@agents.fel.cvut.cz
http://agents.fel.cvut.cz

Abstract. Despite their use for modeling traffic in ports and regional waters, multi-agent simulations have not yet been applied to model maritime traffic on a global scale. We therefore propose a fully agent-based, data-driven model of global maritime traffic, focusing primarily on modeling transit through piracy-affected waters. The model employs finite state machines to represent the behavior of several classes of vessels and can accurately replicate global shipping patterns and approximate real-world distribution of pirate attacks. We apply the model to the problem of optimizing the Gulf of Aden group transit. The results demonstrate the usefulness of agent-based modeling for evaluating and improving operational counter-piracy policies and measures.

Due to its inherent dynamism, distribution and complexity of dependencies, traffic and transportation is a domain particularly suitable for the application of multi-agent techniques. This has been reflected in the number of multi-agent simulations developed in the field of air traffic (e.g. [18]) and ground transportation [2,14]. The key motivation behind these models is to better understand the behavior of transportation systems and to evaluate novel mechanisms for improving it.

In the maritime domain, existing models focus on traffic in ports and regional, near shore waters [3,15,10]. High-level equation-based models are typically used, which have difficulties capturing vessel interactions and more complex dynamics of maritime traffic. In contrast, our proposed model focuses on modeling global maritime traffic and employs a fully agent-based, microsimulation approach. Such a model is pivotal in the development of measures for countering the complex problem of maritime piracy, which presents a growing threat to global shipping industry and consequently international trade. In 2010 alone, 53 merchant vessels were hijacked and 1181 crew members held hostage [11] and the numbers continued to rise in the first half of 2011.

The proposed simulation model is the first agent-based model focusing on maritime traffic and piracy. It models the operation of all key actors in piracy scenarios, i.e., the long-range merchant vessels, pirate vessels and navy patrols. Although the simulation is geared towards maritime piracy, it is rather general

D. Villatoro, J. Sabater-Mir, and J.S. Sichman (Eds.): MABS 2011, LNAI 7124, pp. 44–58, 2012.

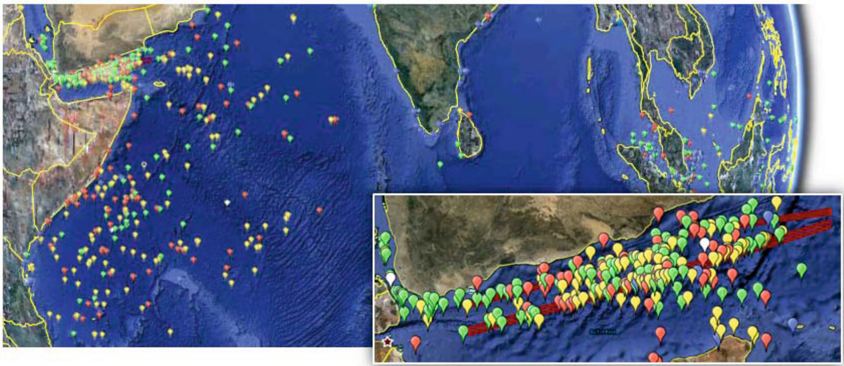


Fig. 1. Locations of pirate incidents over the last 5 years

and applicable to other problems in maritime transportation. As an illustrative application, we apply the simulation to optimize the group transit scheme established to improve the security of transit through the notorious Gulf of Aden.

Section 1 provides a brief introduction to the domain and reviews current anti-piracy measures. Sections 2.1, 2.2 and 2.3 describe agent-based models of three main classes of vessels. Section 3 describes implementation aspects of the proposed models and Section 4 discusses model validation. Finally, Section 5 describes the application to group transit scheme optimization.

1 Domain Background

In this section, we briefly describe existing anti-piracy measures and domain facts that are incorporated in the proposed model.

1.1 Piracy Around the Horn of Africa

Over the last years, waters around the Horn of Africa have experienced a steep rise in piracy. For approximately 20 thousand vessels[1] that annually transit the area, insurance rates have increased more than tenfold and the total cost of piracy was estimated at up to US$16 billion in 2008. Although attacks and hijackings used to be concentrated in the Gulf of Aden, in the last two years the pirates have been expanding further from the coast and attacking vessels on the main shipping lanes in the Indian Ocean, more than 1500 nm from the Somali coast (see Figure 1).

1.2 Existing Antipiracy Measures

In order to counter the rising piracy threat, a number of measures have been put into effect in the Horn of Africa area, which encompasses the Gulf of Aden

[1] about 40% of the world fleet.

Table 1. IRTC group transit schedule – entry times for vessels travelling at different speeds

Speed	Entry point A – time	Entry point B – time
10 kts	04:00 GMT+3	18:00 GMT+3
12 kts	08:30 GMT+3	00:01 GMT+3
14 kts	11:30 GMT+3	04:00 GMT+3
16 kts	14:00 GMT+3	08:30 GMT+3
18 kts	16:00 GMT+3	10:00 GMT+3

and the West Indian Ocean. Since 2008, transit through the Gulf of Aden itself has been organized – transiting vessels are grouped according to their speed and directed through a narrow transit corridor patrolled by international naval forces.

International Recommended Transit Corridor. Initially introduced in 2008, the *International Recommended Transit Corridor (IRTC)* was amended in 2009 to reflect the revised analysis of piracy in the Gulf of Aden and to incorporate shipping industry feedback. The new corridor has been positioned further from established fishing areas, resulting in a reduction of false piracy alerts[2].

Navy Patrols. Several naval task forces from various countries and allied forces[3] operate in the Gulf of Aden (see [13] for details) to protect the transit corridor and prevent attacks on transiting vessels. Detailed information about the strategy of navy vessels is classified. On a high-level, their coordination is based on a *4W Grid* on which areas of responsibility are assigned [5].

Group Transit Scheme. In August 2010, the *Group Transit Scheme* was introduced to further reduce the risk of pirate attacks on vessels transiting the Gulf of Aden [17]. *Group transits* are designed to group ships into several speed groups in order to leverage additional protection and assurance of traveling in a group. Each transit follows a recommended route through the IRTC at a published speed and schedule, designed to avoid the highest-risk areas and time periods. There is one transit per day for each speed group (see Table 1).

2 Model Description

We employ the agent-based modeling approach – each vessel is implemented as an autonomous agent with its specific behavior, capable of interacting with other

[2] MSCHOA, The Maritime Security Centre, Horn of Africa, strongly recommends transiting vessels to follow the corridor to benefit from the protection provided by naval forces.

[3] NATO, Combined Maritime Forces including Japan, China, India, Korea and others.

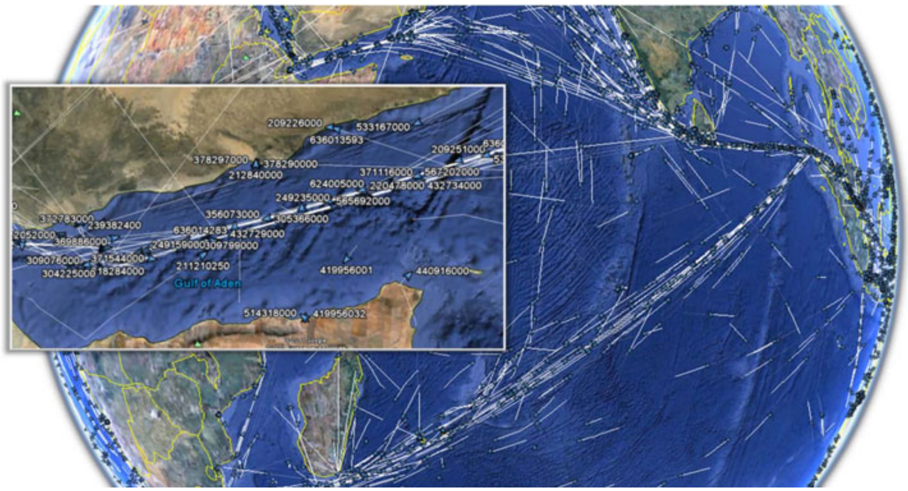


Fig. 2. Merchant vessel traces obtained from satellite AIS data

vessels and the simulated maritime environment. Three categories of vessels are modeled: (1) long-haul merchant vessels, (2) pirate vessels and (3) navy vessels. Each behavior model is based on real-world data. Below, we describe the model for each vessel category.

2.1 Merchant Vessel Model

Merchant vessels, traveling repeatedly between the world's large ports, form the bulk of international maritime traffic. Our agent-based model aims to achieve the same spatio-temporal distribution as the real traffic. We do not simulate physical vessel dynamics and do not yet take into account environmental conditions such as weather or sea currents.

Data Used. Data from the *Automatic Identification System (AIS)* – the most widely used vessel position tracking system – are publicly available[4] and contain time-stamped records of vessel GPS positions along their routes. However, even though it is easy to simply replay the traces, it is not possible to test various hypothetical scenarios (the main reason for the development of the simulation), not to mention low spatial resolution in crucial areas. We thus use AIS data to reconstruct main shipping lanes and traffic density. Furthermore, we use data about geography, including locations of ports, straits, channels or capes through which vessels have to pass while avoiding land, islands and shallow waters.

[4] Large databases are available on `http://www.vesseltracker.com` or `http://www.aislive.com`.

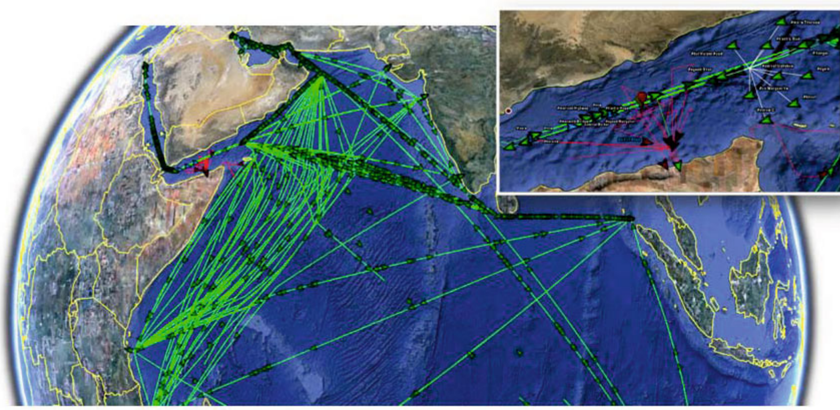


Fig. 3. Simulated traffic – merchant vessels (green) and pirate vessels (red)

AIS Data-based Replicating Traffic Model. In the simplest traffic model, each simulated vessel follows an assigned AIS trace. This way, we are able to replay real traffic from recorded AIS data (see Figure 2). While easy to implement, this approach has several drawbacks: (1) the AIS data have very low sampling frequencies in crucial areas, such as in the Gulf of Aden; (2) the scalability is limited and the number of agents is limited by the number of available traces; (3) experimentation with alternative shipping routes is not possible; (4) the data may be obsolete and not yet reflect the recent shifts in maritime shipping lanes due to increased pirate activity.

Merchant Vessel Model. To eliminate the above issues, we combined simple AIS replication with route planning algorithms in order to generate realistic merchant vessel traffic. As long as it is safe, vessels follow shortest paths between desired locations, avoiding obstacles. Transit through high-risk areas is handled separately to reflect vessel's tendency to avoid such areas or to use special tactics to make such transit more secure.

To approximate global properties of the real-world merchant vessel traffic, origin-destination matrices are used for trip generation. The simulated vessels plan their routes between ports using the combination of the following planners:

Shortest Path Planning. The shortest route planner is based on the A^* algorithm in a spherical environment with polygonal obstacles. The algorithm employs a pre-calculated visibility graph to speed up search and is guaranteed to find the shortest path [16].

Risk-aware Route Planning. The risk-aware planner is invoked for planning routes through high-risk areas. The planner searches for a route which minimizes a weighted sum of route length and the piracy risk along the route. To quantify the risk along a route, we use a spatio-temporal incident density map representing the number of piracy incidents in a given area over a given period of time. By integrating incident density along a vessel route, we obtain the estimate of the number of incidents N that can be expected when following the route. Using the Poisson probability distribution, we then estimate the probability of at least one attack as $1 - e^{-N}$ (for details, see [13]).

Strategic Route Planning. In contrast to the previous two route planners, which reflect practices currently used in the field, the strategic route planning provides an experimental technique for further reducing piracy risk. This game-theoretic route planner explicitly accounts for pirate adaptability and ability to reason about merchant vessel routes and produces routes in an optimally randomized manner, which minimizes the chance of a successful pirate attack (similar to work done by Jain et al. [12]). See [20] for a detailed description of the algorithms.

Group Transit Model. Vessel trajectories are not modified when participating in the group transit scheme and so the generated route does not need to be modified. However, the vessel has to be present at the beginning of the IRTC corridor at a prescribed time (according to the schedule 1) and then continue through the corridor at a prescribed speed. See Section 1.2 for the description of the currently employed group transit schedules and Section 5 for the design of optimal group transit schedules. The implemented group transit model accurately reflects the current state.

2.2 Pirate Vessel Model

Due to the lack of data on real-world pirate vessel movement, an indirect approach is used in modeling pirate behavior.

Data Used. The primary source of information for pirate vessel model are reported descriptions of typical pirate strategies (found e.g. in [8]) which we have translated into executable behavior models (see below). These are then used in conjunction with additional data about real-world pirate activity. Specifically, we use a public dataset [7] of places on the Somali coast known to serve as pirate hubs or ransom anchorages. We also use piracy incident records published since 2005 by the IMB Piracy Reporting Centre[5]. Each record contains the incident location in GPS format, the type of attacked vessel, incident date and the type of attack (see Figure 1 for the visualization of a sample of the dataset). These data are partially used for calibration and partially for validation of the pirate behavior model (see Section 4.2).

Pirate Behavior Model. In order to capture the diversity of real-world pirate strategies (see e.g. [8]) we implemented four different pirate vessel models: (1) *Simple pirate* with a small boat without any means of vessel detection except the direct line of sight (5 nm), (2) *Radar pirate* with a radar extending the

[5] `http://www.icc-ccs.org/home/piracy-reporting-centre`

vessel detection range to 20-50 nm, (3) *AIS pirate* with an AIS interception device monitoring AIS broadcasts and (4) *Mothership pirate* with a medium-size vessel and several boats able to attack vessels up 1500 nm from the Somali coast. The last type can be combined with the radar or AIS interception device to achieve more complex behavior. Additionally, for specific needs of testing game-theoretic routing strategies, we designed an adaptive pirate based on the multi-armed bandit problem [19]. Through trial and error, the adaptive pirate is capable of discovering and exploiting potential vulnerabilities of employed routing and patrolling strategies.

Each pirate agent is initialized in its home port and based on the position of the port, it is assigned its operational zone (Gulf of Aden, Northern or Southern part of Indian Ocean). The pirate operates in cycles, starting and finishing in its home port. Before each cycle, the pirate chooses a position to sail. In the case of the adaptive pirate, this decision is based on the exploration/exploitation algorithm; otherwise the position is chosen randomly from the assigned operational area. Based on the type of vessel used, the pirate has different total amount of time it can spend on the open sea, ranging from a single day in the case of small boats to weeks in the case of motherships.

2.3 Naval Vessel Model

The lack of data and large variation of patrolling strategies – which can vary from active search for pirates to protecting transiting groups of merchant vessels – makes proper modeling of navy vessel agents very difficult. We have thus proposed a minimal model based on the information available. However, as a potential improvement to current practices, we have also proposed a game-theoretic policy for patrolling (see [4] for details).

Data Used. The *4W Grid* [5], dividing the Gulf of Aden into square sectors, is used for coordination of anti-piracy operations. Data about combined task forces CTF-150 and CTF-151 are used for approximating the number and capabilities of deployed naval assets.

Patrolling Behavior. We have implemented several of patrolling strategies, ranging from stationary reactive patrols to deliberative agents evaluating the situation in the assigned area and pro-actively deciding where to patrol and which vessels to protect. Naval vessel agents are controlled by a hierarchical structure of authority agents, reflecting the real-world chain-of-command. A central *Navy Authority* agent controls a set of *Task forces* (i.e. group of agents), each controlling a number of agents representing Naval vessels with on-board helicopters able to patrol the area and respond to attacks. More details can be found in [13].

3 Model Implementation

We have implemented the proposed multi-agent model in Java, employing selected components of the A-lite[6] simulation platform and using Google Earth for geo-referenced visualization. Scripts written in Groovy are used for scenario description. Below we describe the implementation of behavior models – see [13] for a detailed description of the (rest of) implementation.

The performance of the simulation is directly dependent on the number of agents (the most demanding are the pirate models). With approximately thousand vessels and one simulation step equal to 1 minute, our platform is able to simulate a month of real-world traffic in approximately one minute on a standard desktop computer (2.4Ghz, 4GB RAM, single-core use).

Agent Behavior Implementation. Behavior model implementation needs to be computationally efficient to allow simulation of thousands of vessel agents and expressive enough to model complex behavior and interactions between vessels. The agents should be able to execute multi-step plans while handling possible interruptions. Different vessels models share some behaviors – such as trajectory planning or basic pirate attack cycle – therefore re-usability should be supported. Moreover, to effectively implement adaptive pirates, we want to support learning directly in the behavior model implementation.

Extended finite state machines (FSM) fit the above requirements well. Individual states correspond to the principal mental states of the vessel agent (such as move, attack, hijacked, patrol etc.). Transitions between the states are defined by unconditional state transitions (a pair $\{s_{from}, s_{to}\}$, e.g. $\{wait, move\}$) or by conditional transitions triggered by external events (a tuple $\{s_{from}, event, s_{to}\}$, e.g. $\{move, shipSpottted, attack\}$). Each state stores its context when deactivated so that when reactivated, the context can be restored to continue the previously interrupted plan. Transitions between states can be internally or externally triggered, thus allowing interruption of plans or actions. FSMs are easily extensible and state implementations can be easily reused. It is possible to create abstract skeletons of various FSM and then enrich them with specific behaviors. The ability to learn can be implemented using internal state variables.

The problem of incorporating time into FSMs is solved by allocating the agent each turn a time quantum which the agent uses for performing the activity associated with its current state. Concurrent actions are not supported by our FSM implementation but this is not required for the level of modeling used.

Agent Interaction. The agents can interact in two ways: (1) by exchanging messages (cooperative interaction) or (2) by forcing the other agent to transit between states by triggering an external environmental event. The first option is used for communication between merchant vessels transiting in a group or between task-forces (i.e. exchange of information); the latter is used for non-voluntary interactions, e.g. when a pirate hijacks a merchant vessel or when a helicopter disables a pirate vessel and prevents it from attacking.

[6] `http://agents.felk.cvut.cz/projects/#alite`

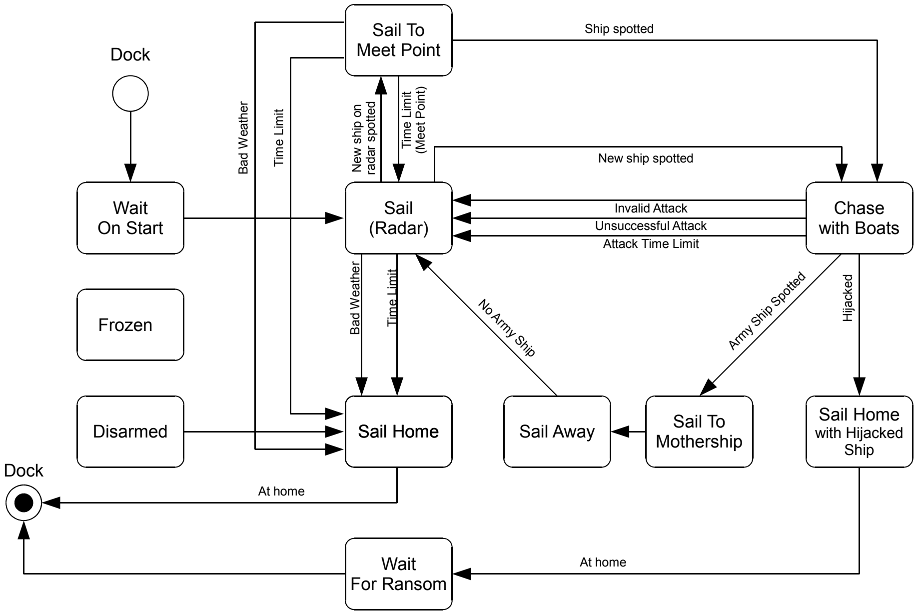


Fig. 4. FSM implementing the behavior of a pirate with a mothership and a radar

Pirate FSM Example. Figure 4 depicts a FSM of a pirate equipped with a radar and a mothership. The pirate waits an arbitrary amount of time in its home port and then sails into the open sea, scanning with the radar for a potential target. If it detects a merchant vessel, it approaches it and launches attack. If the attack is successful and the pirate vessel hijacks the vessel, it gains full control over the vessel and forces it to go to its home port and wait for the payment of ransom.

There are several external events that can disrupt this cycle: the pirate has limited resources, thus the amount of time to spend at sea – when this amount is depleted, the pirate has to return back to its home port. If a naval vessel is spotted, the agent interrupts its chase and moves away from the naval vessel. The forced state transition can be triggered by the naval vessel when it intercepts pirate attack. First, the pirate is *disabled* by a helicopter and later *disarmed* by a warship. The unconditioned state transition ($\{disarmed, sailHome\}$) then returns the control to the pirate agent, which then sails to its home port.

4 Model Validation

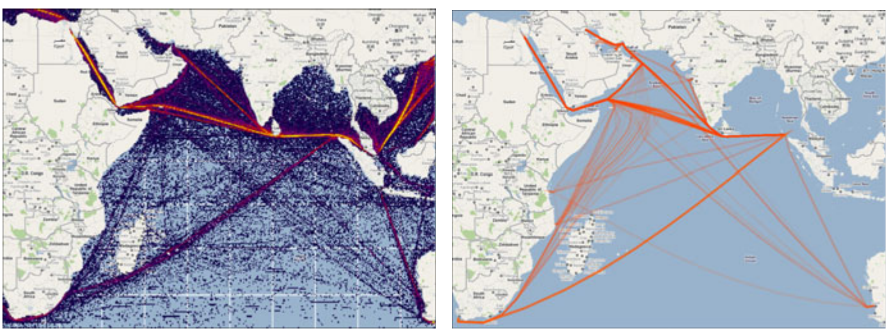
To validate the proposed model, we compare simulation output with real-world data. We first validate the model of merchant vessels alone and then look at the full model. We only employ visual comparison at the moment; formal statistical comparison will be part of our future work.

4.1 Long-Range Shipping Traffic Model Validation

To verify the accuracy of merchant traffic, we compare the traces of simulated merchant vessels with the aggregated AIS-based maritime shipping density map [9] (gathered from 2005 till the beginning of 2008, see Figure 5a). A few differences are visible (see Figure 5). (1) Main corridors are narrower in the simulation. This difference could be removed by adding perturbations to simulated vessel routes. (2) The simulated traces do not exactly correspond to the corridors near the Socotra island. This difference is caused by the introduction of the IRTC corridor which is not yet reflected in the density map (our traces are more up-to-date). (3) The routes along the Somali coast extend farther from the coast in the simulated data. Again, the routing in these waters underwent major changes in the last years and the density map does not yet fully reflects the tendency of vessels to stay farther from the dangerous Somali coast. Our model uses a risk-based planner which takes this factor into consideration.

The reference data [9] also contain samples of trajectories of vessels not considered in our simulation, such as fishing vessels, maritime-research vessels or private vessels. These samples account for the irregular traffic outside the main corridors.

Overall the agreement between the real and simulated traffic is very good. In the future, we aim to introduce and evaluate a formal measure of model accuracy.

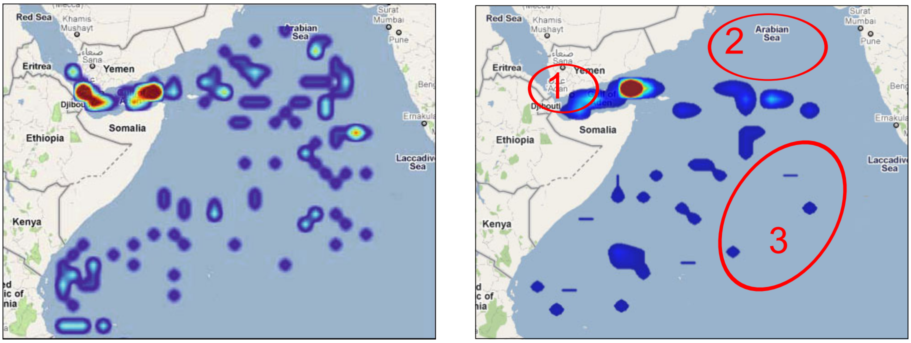


(a) Real-world ship density (2005-2008). **(b)** Simulated merchant vessel traffic.

Fig. 5. Comparison of the real-world shipping density (left) and simulated merchant vessel traffic (right)

4.2 Piracy Model Validation

Due to the lack of real-world pirate movement data, we are not able to directly validate pirate behavior models. Instead we compare the pirate attack density, as produced by the pirate models in conjunction with the models of merchant and navy vessels, and compare this density with the data provided by IMB Piracy Reporting Centre (see Section 2.2).



(a) Real pirate attack density for 2010. **(b)** Simulated attack density for a 1-year period.

Fig. 6. Comparison of real and simulated attack densities for a 1-year period

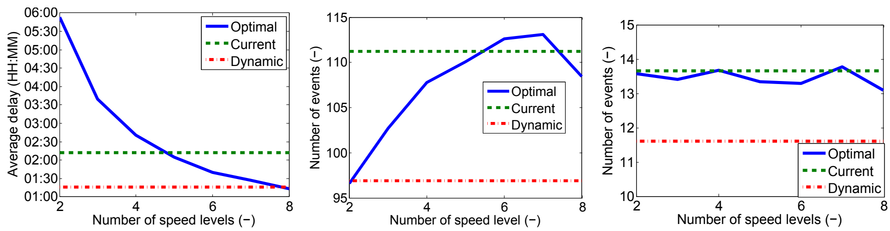
For comparison, we have simulated one year of merchant vessel traffic through the region with realistic traffic density (approximately 60 vessels a day in IRTC). We do not have any estimates of real-world density of pirates in the area. We have therefore set their number so that the overall number of incidents corresponds to the number observed in the real-world. We have simulated 15 pirates – 5 simple, 5 radar equipped pirates and 5 pirates with a mothership and a radar. Finally, we have placed 3 naval task forces, each equipped with 2 warships and a helicopter, into the IRTC according to the 4W grid.

Figure 6 shows the comparison of the real and simulated density of pirate attacks. The red circles denote main differences in incident distribution. (1) Simulated pirates do not attack vessels in the Red Sea; this is because the current configuration focuses on the IRTC corridor. (2) There are no attacks in the Arabian Sea in the simulation. This is because the simulated pirates which sail far from the coast are equipped with a radar, and are thus almost always able to detect and attack vessels sailing in the shipping lane from the Gulf of Aden to Malaysia. (3) The density of attacks in the central Indian Ocean is lower; this is because of the lower density of the simulated merchant vessel traffic itself.

Overall, the agreement between the real-world and simulated pirate attack density is satisfactory, especially considering the random fluctuations in the real-world attack density and the fact that the simulated attack density is the result of the interaction of three types of vessels: merchant vessels, pirates and patrols. Each deviation in the behavior model is amplified through these interactions and can have a disproportional effect on the resulting incident density. After fixing the specific issues mentioned, the agreement between the model and reality should be further improved.

5 Group Transit Schedule Optimization

As an example application of the developed model, we use it to optimize the Gulf of Aden group transit scheme (introduced in Section 1.2). The current



(a) Average delays. **(b)** Number of attacks. **(c)** Number of hijacks.

Fig. 7. Evaluation of different group transit schemes

group transit scheme uses fixed transit schedules designed to divide transiting vessels into five groups travelling at different speeds uniformly spaced between 10 and 18 knots. Our motivation is to explore whether the number of attacks and the transit delay caused by participating in group transit can be reduced by (1) proposing a different set of speed levels for the fixed-schedule scheme and (2) employing a dynamic grouping scheme, which takes into account not only the speeds of transiting vessels but their time of arrival too.

Optimal Fixed Schedule Group Transit. The real-world distribution of merchant vessel speeds is approximated by a histogram (see Figure 8) with bins of a fixed width (can be set e.g. to 0.1, 0.5 or 1 knot). The optimization problem can be formulated as partitioning the histogram into N groups, corresponding to group transit speeds, which minimize the average transit delay (i.e. the delay caused by traveling at a group speed which might be lower than the vessel's normal cruising speed).

Dynamic Group Transit. Instead of assigning vessels to groups according to predefined schedules and speed levels, dynamic grouping forms groups on the fly. This allows to form groups that better reflect actual arrival times and speed distribution of incoming vessels, at the expense of a more complex coordination scheme required. Our current implementation uses a greedy technique which assigns incoming vessels with similar speeds to the same group (see [13] for details).

Evaluation. We have used the simulation to evaluate the average transit delay (Figure 7a), the average number of transit groups and the number of total and successful pirate attacks for different grouping schemes. Figure 8 shows the optimal speed levels for the fixed-schedule group transit with 5 speed levels. Note that in contrast to the current scheme, new speed levels are not distributed uniformly and are concentrated around the mean vessel speed. As shown in Table 2, new speed levels result in shorter transit times and a lower average number of transit groups, thus potentially saving millions of US dollars.

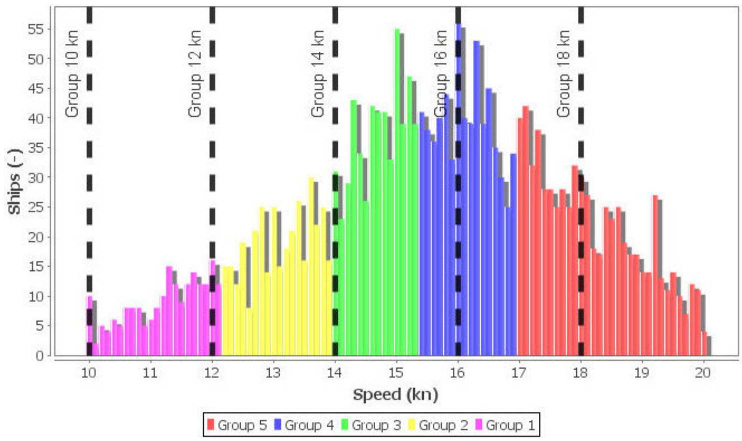


Fig. 8. Vessel speed histogram and its optimum partitioning into 5 speed groups

Table 2. Time savings and average number of transit groups for selected grouping schemes. ΔT is the average transit time reduction compared to the current scheme (per one transit and aggregated for all transits in one year). The overall savings are computed as $(\Delta T/year) \cdot \$30000$ (according to [6]).

Scheme	Schedule	ΔT/ship	ΔT/year	Avg. groups	Savings
current	$\{10, 12, 14, 16, 18\}$	0 min	0 days	10.73	-
opt. 5	$\{10, 12.2, 14, 15.4, 17\}$	7 min	97 days	9.16	2.9m USD
opt. 6	$\{10, 11.7, 13.3, 14.6, 16, 17.6\}$	31 min	430 days	9.88	12.9m USD
dynamic	-	56 min	778 days	12.14	23.4m USD

The grouping for 6 speed levels further reduces group transit delay and saves over a year of total vessel travel time. The number of pirate incidents does not significantly vary with the increasing number of speed levels (see Figures 7b, 7c), because even though there are potentially more groups to attack, the speed of the groups is higher on average. The dynamic scheme is by far the most efficient in reducing transit delay although at the expense of higher number of groups (i.e. smaller average group size).

6 Conclusion

Multi-agent simulations have a great potential for designing and evaluating solutions to a range of issues in international shipping, including the threat of contemporary maritime piracy. To this end, we have developed a first fully agent-based model of global traffic that accounts for the effects of maritime piracy on global shipping. The model is based on a range of real-world datasets and represents the operation of three types of vessels and their interactions. Despite the lack of hard data on some phenomena related to maritime piracy, the implemented model shows good correspondence in areas where validation data are available. As an example of potential applications of the developed model, we have shown how it can be used to optimize the current Gulf of Aden group transit scheme.

Overall, the implemented model demonstrates the viability of agent-based modeling in the maritime domain and opens a number of promising research directions.

As the immediate next step, we plan to improve the validation of our proposed model by employing statistical measures of model error and by considering the model dynamics too, in particular the ability to properly capture the co-evolution of merchant and pirate strategies over time. In a longer term, we aim to leverage some of the recent economic studies of piracy (e.g. [1]) in order to endogenize selected parameters of the model (in particular the intensity of pirate attacks) by calculating what economic incentives, survival risks and alternative livelihoods pirates face.

Acknowledgments. Funded by the Office of Naval Research (grant no. N000140 910537), by the American Science Information Center AMVIS (grant no. LH11051), and by the Czech Ministry of Education, Youth and Sports under grant "Decision Making and Control for Manufacturing III" (grant no. MSM 6840770038).

References

1. The economics of piracy – pirate ransoms and livelihoods off the coast of Somalia. Technical report, GeoPolicity (2011), `http://www.geopolicity.com/upload/content/pub_1305229189_regular.pdf`
2. Bernhardt, K.: Agent-based modeling in transportation. Artificial Intelligence in Transportation E-C113, 72–80 (2007)
3. Bourdon, S., Gauthier, Y., Greiss, J.: MATRICS: A Maritime Traffic Simulation. Technical report, Defence R&D Canada (2007)
4. Bošanský, B., Lisý, V., Jakob, M., Pěchouček, M.: Computing time-dependent policies for patrolling games with mobile targets. In: Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (2011)
5. CAPT George McGuire, R.: Combined maritime forces (cmf) - who we are and wider military counter piracy update, 12 (2009), `http://www.cusnc.navy.mil/marlo/Events/DEC-MARLO-DubaiConference_files-2009/CAPT%20McGuire.ppt`
6. Elbeck, M., Tirtiroglu, E.: The threat of piracy on maritime transportation. International Journal of Society Systems Science 2(2), 125–133 (2010)
7. Expedition. Somalia pirate attacks, 4 (2008), `http://bbs.keyhole.com/ubb/ubbthreads.php?ubb=showflat&Number=1242871&site_id=1`
8. Gilpin, R.: Counting the Costs of Somali Piracy. Technical report, US Institute of Peace (2009)
9. Halpern, B.S., Walbridge, S., Selkoe, K.A., Kappel, C.V., Micheli, F., D'Agrosa, C., Bruno, J.F., Casey, K.S., Ebert, C., Fox, H.E.: A global map of human impact on marine ecosystems. Science 319(5865), 948 (2008)

10. Hasegawa, K., Hata, K., Shioji, M., Niwa, K., Mori, S., Fukuda, H.: Maritime Traffic Simulation in Congested Waterways and Its Applications. In: Proceedings of the 4th Conference for New Ship and Marine Technology (New S-Tech 2004), Chine, pp. 195–199 (2004)
11. ICC Commercial Crime Services. Hostage-taking at sea rises to record levels, says IMB (2010), `http://www.icc-ccs.org/news/429-hostage-taking-at-sea-rises-to-record-levels-says-imb`
12. Jain, M., Kardes, E., Kiekintveld, C., Ordonez, F., Tambe, M.: Security Games with Arbitrary Schedules: A Branch and Price Approach. In: Proceedings of the Conference on Artificial Intelligence (2010)
13. Jakob, M., Vaněk, O., Bošanský, B., Hrstka, O., Pěchouček, M.: Adversarial modeling and reasoning in the maritime domain year 2 report. Technical report, ATG, CTU, Prague (2010)
14. Krajzewicz, D., Hertkorn, G., Rössel, C., Wagner, P.: Sumo (simulation of urban mobility) – an open-source traffic simulation. In: MESM 2002 (2002)
15. Köse, E., Basar, E., Demirci, E., Güneroglu, A., Erkebay, S.: Simulation of marine traffic in istanbul strait. Simulation Modelling Practice and Theory 11(7-8), 597–608 (2003)
16. Lozano-Perez, T., Wesley, M.A.: An algorithm for planning collision-free paths among polyhedral obstacles. Communication of the ACM (1979)
17. MSCHOA. Gulf of aden internationally recommended transit corridor and group transit explanation (August 2010), `http://www.shipping.nato.int/GroupTrans1/file/_WFS/GroupTransit12aug2010.pdf`
18. Pěchouček, M., Šišlák, D.: Agent-based approach to free-flight planning, control, and simulation. IEEE Intelligent Systems 24(1), 14–17 (2009)
19. Sundaram, R.K.: Studies in Choice and Welfare. Springer, Heidelberg (2005)
20. Vaněk, O., Jakob, M., Lisý, V., Bošanský, B., Pěchouček, M.: Iterative game-theoretic route selection for hostile area transit and patrolling. In: Proccedings of the International Conference on Autonomous Agents and Multiagent Systems (2011)