From Sensor Data to Piracy Threat Classification for Merchant Shipping

K-G Stenborg, Maria Andersson, Jonas Allvar, Ronnie Johansson and Niclas Wadströmer
FOI - Swedish Defence Research Agency, Sweden
E-mail: {karl-goran.stenborg,maria.andersson.jonas.allvar,ronnie.johansson,niclas.wadstromer}@foi.se

***Abstract*—In the EU FP7 project IPATCH, we are researching components for an early piracy detection and avoidance system deployed on merchant ships. The system combines information from on-board sensors about the local situation with intelligence from other sources about the current situation in the region in order to give early warning about threatening pirates. One of the challenges in the project is how data from the on-board sensors should be derived and represented as motion indicators, that can be fused with text and numerical values from other sources, for threat classification and situation awareness. In this paper we describe our approach with Bayesian networks, which are used for fusing different types of indicators. Motion indicators are based on detection and tracking data from different sensors.**

I. Introduction

The start of the 21st century has seen a resurgence of piracy at sea. Regions in the Gulf of Aden, West Africa, South East Asia and South America have turned into dangerous places for commercial ships. Pirates operating from small but relatively fast skiffs can attack and board ships to steal cargo or take the crew and ship hostage. Just detecting skiffs is not enough since that type of boats are also commonly used by local fishermen. Therefore also the maneuvers of skiffs combined with general risk depending on area, time of day, weather and other factors are needed to generate more reliable risk information.

It is of utmost importance for ships in high risk areas to detect piracy threats as early as possible so that the ship master can initiate countermeasures while they are still effective. Countermeasures could for example be to change the course, call for assistance or bring the crew into the protected citadel. In the IPATCH project [1] we develop an on-board system for automatic early detection, classification and mitigation of piracy threats against commercial ships.

The IPATCH system will analyze and fuse information from all available sources (e.g. radar, AIS, IR- and visual cameras) as well as knowledge from intelligence and ship databases to detect and classify threats. In addition, the system will provide a decision support tool that supports the master of the ship in selecting countermeasures specific to the situation. The algorithms of the system can be classified into three basic steps:

1) Detection and tracking of objects
2) Situation awareness and threat classification
3) Decision support

In this paper we will present our selected approach for step 2 in the system.

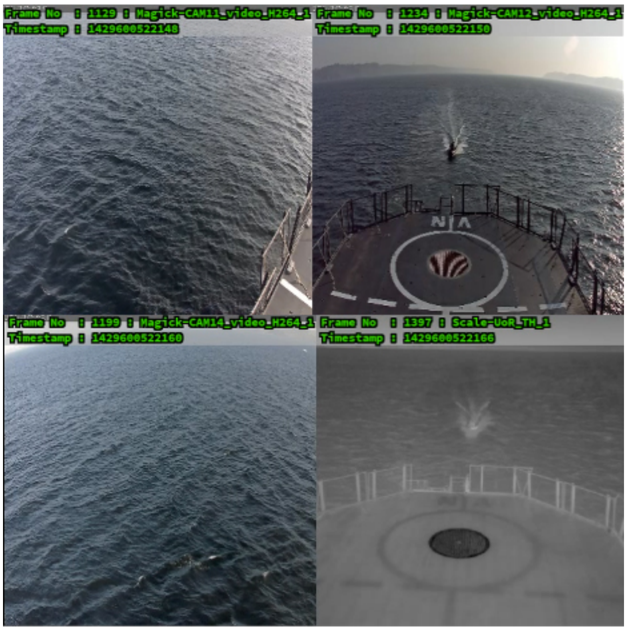
Frame No : 1129 : Magick-CAM11_video_H264_1
Timestamp : 1429600522148
Frame No : 1234 : Magick-CAM12_video_H264_1
Timestamp : 1429600522150
Frame No : 1199 : Magick-CAM14_video_H264_1
Timestamp : 1429600522160
Frame No : 1397 : Scale-UoR_TH_1
Timestamp : 1429600522166

Fig. 1. Three visual and one thermal sensor monitoring the area around the protected ship at the data collection in Brest.

II. Data collection

At the end of the IPATCH project the system will be demonstrated in a real-world scenario in the area around a ship. To prepare for this we have started to collect maritime data of small boats attacking a larger sensor bearing ship. We have used two different approaches for the data collection: field trials on the sea and production of synthetic maritime sensor data.

A. Field trial

In spring 2015 a data collection with different types of sensors on a ship was performed in the sea outside Brest [2]. The ship used AIS, GPS, radar and a number of IR- and visual sensors and for ground truth the smaller boats was equipped with GPS. The smaller boats preformed scenarios where they sometimes acted like fishermen and other times as pirates. The scenarios have different levels of threats depending on the movement of the smaller boats.

Part of the collected data have been made available by the PETS 2016 [3] workshop. An example of the collected data is given in Fig. 1.

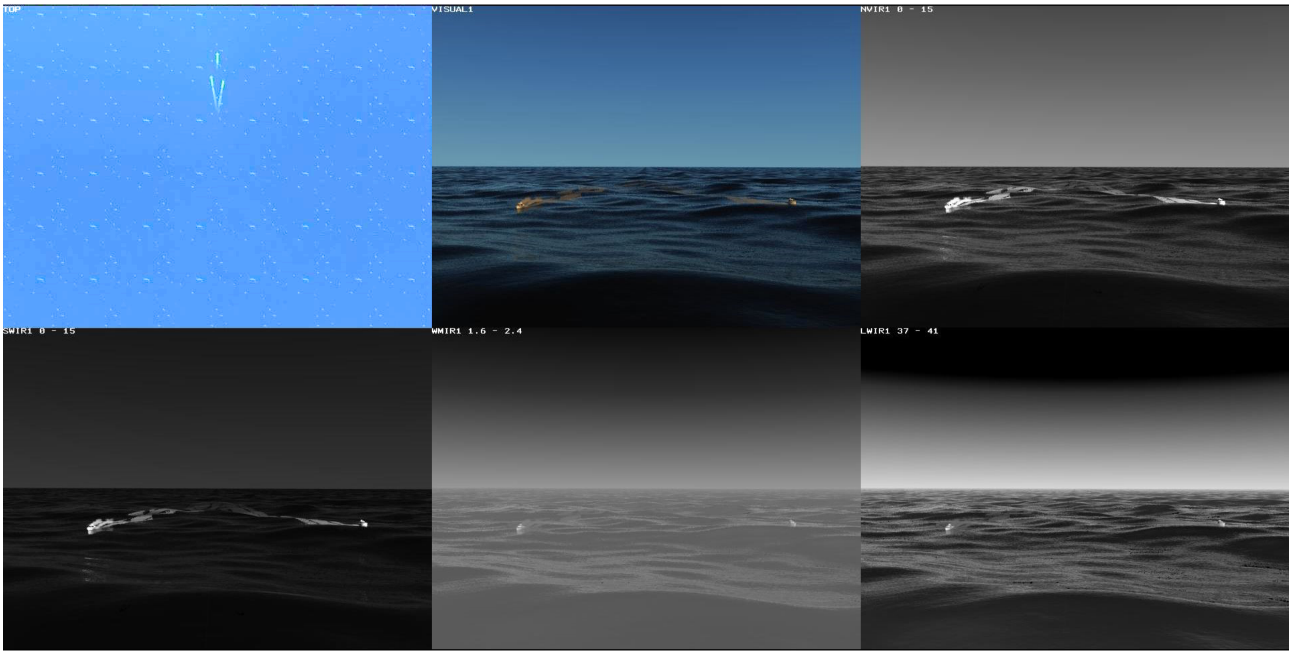

Fig. 2. Top row: Map view of our ship and two approaching boats from the aft, visible sensor data and NIR (Near-infrared) sensor data. Bottom row: SWIR (Short-wavelength infrared), MWIR (Mid-wavelength infrared) and LWIR (Long-wavelength infrared) sensor data.

B. *Synthetic data*

As a complement to the dataset collected in Brest a synthetic dataset has also been generated. This has some advantages compared to the other dataset, for example:

- Weather conditions can be controlled to be similar to, for example, the Horn of Africa. The same scenario can also be generated in different weather conditions to compare algorithm results for these given weathers.
- Many different sensors can be used. Different thermal sensors can be compared to establish which wavelength band provides the clearest contrast between boats and sea. It is easy to test sensors that in real life are very expensive and compare their results with those from lower-cost sensors.
- Exact position of the boats in the sensors are known (without manual annotation) and in both sensor and world coordinates.
- It is easy to change parameters and regenerate the simulated data when needed, while it is very costly to redo a live data collection if new or other data is needed.

The synthetic data is generated using 3D models and SE-Workbench [4]. SE-Workbench is a software designed to simulate the physical signature of terrain and objects for different types of sensors. In the Electro-Optics part of SE-Workbench the 3D models should be built by polygon surfaces. These surfaces should have their materials classified, which means that their characteristics are described for different wavelength bands. Both terrain (in our case sea) and objects (boats) should have all their polygons material classified correctly to give accurate physical properties. Weather data is based on observations from the Gulf of Aden taken on 2015-04-20 08:00 local time. Atmospheric parameters are modeled by the atmospheric transmission, radiance and flux model MODTRAN [5] and sea state was calculated using SWAN [6].

The sensors are fixed at three positions on the aft of the ship. Each position has five virtual sensors with the same heading, FOV, resolution and frequency. In Fig. 2 one frame for five such virtual sensors can be seen.

III. Algorithms

In this section we describe the suggested steps from tracking, through threat recognition to the decision support module that interacts with the crew of the ship and supports the crew in choosing suitable countermeasures, Fig. 3.

A. *From detection/tracks to higher level indicators*

In this paper we assume that the detections of boats are sufficient to give fused tracks (from different sensors of the same type and different types of sensors) so that the higher level algorithms will get an accurate situational description. Some of the detection/tracking work has been published in [7]. For the synthetic data we can also generate tracks from the ground truth for test purposes.

The sensor data will give a description of the current situation with all boats and their tracks as far back as known. This data is relevant to the classification of possible pirate movement and some threat recognition methods can use boat trajectories directly. As we will later see we have chosen Bayesian network for threat recognition and that means that the boat trajectories needs to be derived and represented in a way that the higher level algorithms can handle. Bayesian networks are used to describe how the indicators and other information about the situation relate to specific threats. Each threat is described by a Bayesian network and the current evidence

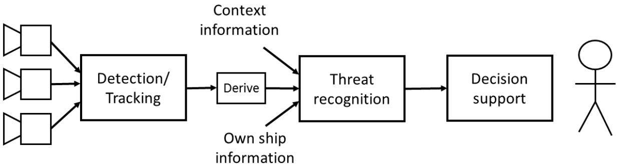

Fig. 3. The IPATCH system from sensor to human. The threat recognition is done with Bayesian networks and tracks are derived into suitable indicators for the network. Other information such as geographic location, time, season, weather, intelligence information and own ship status is also indicators to the network. From the decision support tool the ship crew will get alarms for threatening or suspicious behavior of boats and in critical situation suggestions on suitable countermeasures.

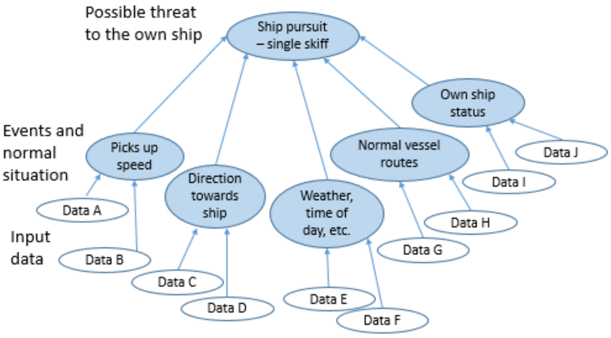

Fig. 4. Example of a model for threat detection.

from the indicators are used to calculate the probability of that threat. Some indicators are computed from the data of a single boat while other requires an updated statistical model of boats' movements to indicate if the current situation is statistically likely or not. One indicator use tracks of boats to determine common routes and then indicate if a specific boat follows any of the routes. The routes could both be geographically related or locally related to the protected ship. Another indicator shows if the movements of two boats are coordinated as when two skiffs launch a coordinated attack. Some basic indicators are for example *boat speed*, *boat speed change*, *boat direction*, *boat direction change*, *boat distance to ship* and relation events such as *meet* and *split* when two or more boats gets close or departs from one another. The closer the boats are to the ship the more correct these indicators will become, while early detection of possible threats are desirable, providing some difficulty to the creation of the system.

B. Prevouis work in threat recognition

Some of the previous work for the situation awareness and threat classification use methods such as Trajectory Clustering [8], [9], Rule based systems [10] and Markov logic networks [11]. Some ideas from these approaches was reused by us but in a format more suitable for the given architecture in the project.

C. Bayesian networks

Macro threat scenarios define general conditions that are likely to facilitate an attack. Micro threat scenarios define and simulate realistic behavioral patterns of the pirates during the attacks. In the IPATCH project we have derived and described a large set of macro and micro threat scenarios [12], which will be used as input data to the threat classification module. The nature of the macro and micro scenarios will also be useful in the creation of the threat classification module, or in our case, the structure of the Bayesian network. Macro scenarios can be seen as context information to a micro scenario. A specific micro scenario can have different meanings in different context, i.e. in different macro scenarios. For example, outside a certain coast at a certain time of the day and season, there is a lot of traffic with different types of boats that move in many different directions. Specific complex features are needed for recognizing threats. Outside another coast at the same time of day and season few small boats are normally present. Most probably less specific features are needed for that case to form an alarm in the threat classification module.

The reasoning above, concerning macro and micro scenarios, leads to the effect that it may be necessary to have several different threat classification modules. In any case, we need to correlate and combine information from different types of information sources, i.e. macro and micro scenarios. The different types of information sources are very different in nature concerning how they are represented, how often they are expected to change and how certain they are. We select the Bayesian network as our main approach to describe and categorize known pirate behaviors since it has the ability to combine information that are different in nature. In addition, Bayesian networks have also been selected earlier [13] for fusing context information with patterns.

A Bayesian network is a probabilistic graphical model that is represented as a directed acyclic graph, whose nodes are random variables in a certain domain (in this case maritime domain) and whose edges direct influence from one node to another [14]. The main application of Bayesian networks is to update the probabilities of variables of interest (e.g., threats), conditioned on other observed variables. In this application the Bayesian networks estimate threat levels by fusing information about related events and features. The estimated events and features are based on other algorithms such as tracking and boat behavior algorithms. Fig. 4 shows an example of a Bayesian threat model that divides a pirate attack into events, where each event gets data from different feature extraction models. The feature extraction models describe kinematic states of boats in the environment. Features can also be other types of information such as for the current area around the ship, i.e. information on weather, time and that there is a recognized fishing area close to the ship. Data about the ship, such as current speed, maximum speed and current freeboard, is also input data. As described earlier detection and tracking information about other boats need to be adapted to a format comprehensible for the Bayesian network.

D. Decision support

The output from the Bayesian network are descriptors that go into the decision support tool. In the Bayesian network indicators are used to detect, recognize and classify threats. The system will have a continuously updated description of the situation to assist the crew of the ship. The situational awareness will include descriptions of the normal situation and automatic detections of anomalies. The crew will be alerted when a threat is detected and recognized, but also when there is an unusual situation even if it is not recognized as a known threat. In such a case the crew has to determine if the situation is threatening and, if so, what action that should be taken. The system will have a database with countermeasures and descriptions of them to give information about alternative actions as well as possible consequences of using them. The results from the threat classification are important input data to the selection of countermeasures.

IV. Discussion

In this section we discuss two different topics concerning the system.

A. Technical challenges

There are still some problems that we need to solve for the threat recognition and the Bayesian network approach. We give a short description of them here:

- How to best represent dynamic events as a node in the Bayesian network.
- How to parameterize the Bayesian network in a suitable way. Is a learning system or a rule-based approach best.
- Should we use Dynamic Bayesian network as a node to the Bayesian network (e.g. a HMM).
- How should we handle old information (when has it become obsolete?) so it does not affect the Bayesian network.
- How to best handle data association (e.g. which groups of boats should we consider?).

Some of these problems might not be fully addressed within this project.

B. Additional usage of the system

We think that the IPATCH system can have other useful features, in addition to the piracy threat detection, for future maritime applications:

- Collision avoidance between ships.
- Sea rescue operations with support to detect and track boats and possible people in the water.
- For the piracy case the system might also be used to suggest when it is resource wise suitable to assign personnel for manual visual boat detection (monitoring with binoculars) for high risk situations and areas.

The applications and use of intelligent optical sensor systems in the maritime environment will probably increase in the coming years.

V. Conclusion

In this paper we have given an overview of the threat recognition tool of the IPATCH system for suspected piracy activity. The work is still ongoing and exact which algorithms will prove to be reliable remains to be seen. Our approach with Bayesian networks provides many advantages but we also see challenges ahead of us. To use and try to represent detection and tracking data in a suitable way for Bayesian networks has been exciting but also raised many questions.

Acknowledgment

The IPATCH project has received funding from the European Unions Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607567.

The coordinator of the project is BMT (UK). Partners are FOI (SE), Sagem (FR), University of Reading (UK), ITTI (PL), Termisk Systemteknik (SE), Universit Cattolica del Sacro Cuore (IT), University of Namur (BE) and Foinkas Shipping Company (GR).

References

[1] “IPATCH - Intelligent Piracy Avoidance using Threat detection and Countermeasure Heuristics,” http://www.ipatchproject.eu/, 2014 – 2017.

[2] T. Cane, “Data Collection Event held in Brest,” http://www.ipatchproject.eu/news/page-content/news-index/data-collection-event.aspx, 2015.

[3] “PETS 2016 - IEEE International Workshop on Performance Evaluation of Tracking and Surveillance,” http://pets2016.net/, 2016.

[4] T. E. Cathalaa, “The coupling of MATISSE and the SE-WORKBENCH: a new solution for simulating efficiently the atmospheric radiative transfer and the sea surface radiation,” in *Proceedings SPIE 7300, Infrared Imaging Systems: Design, Analysis, Modeling, and Testing*. SPIE, 2009.

[5] G. P. Anderson, “MODTRAN4: radiative transfer modeling for remote sensing,” in *Proceedings SPIE 3866 (2), Optics in Atmospheric Propagation and Adaptive Systems III , vol. 3866 (2)*. SPIE, 1999.

[6] “SWAN Scientific and Technical Documentation,” http://swanmodel.sourceforge.net/, Delft University of Technology, 2015.

[7] C. Osborne, T. Cane, T. Nawaz, and J. Ferryman, “Temporally stable feature clusters for maritime object tracking in visible and thermal imagery,” in *12th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. IEEE, 2015, August, pp. 1–6.

[8] A. Dahlbom and L. Niklasson, “Trajectory clustering for coastal surveillance,” in *10th International Conference on Information Fusion*. IEEE, 2007.

[9] F. Katsilieris, P. Braca, and S. Coraluppi, “Detection of malicious AIS position spoofing by exploiting radar information,” in *16th International Conference on Information Fusion*. IEEE, 2013.

[10] J. van Laere and M. Nilsson, “Evaluation of a workshop to capture knowledge from subject matter experts in maritime surveillance,” in *12th International Conference on Information Fusion*. IEEE, 2009.

[11] L. Snidaro, I. Visentini, and K. Bryan, “Fusing uncertain knowledge and evidence for maritime situational awareness via Markov Logic Networks,” *Information Fusion*, vol. 21, pp. 159–172, 2015.

[12] M. Dugato and G. Berlusconi, “Maritime piracy worldwide,” Transcrime Research in Brief, Universita degli Studi di Trento, Tech. Rep. 1/2015.

[13] V. J. J. Dabrowski, J. P., “A unified model for context-based behavioural modelling and classification,” *Expert Systems with Applications*, vol. 42, pp. 6738–6757, 2015.

[14] D. Koller and N. Friedman, *Probabilistic Graphical Models*. Cambridge, Massachusetts: The MIT Press, 2009.