The IPATCH System for Maritime Surveillance and Piracy Threat Classification

M. Andersson[a], R. Johansson[b], K-G. Stenborg[a],
R. Forsgren[a]

[a]Dept. of C4ISR
[b]Dept. of Defence and Security, Systems and Technology
Swedish Defence Research Agency, Stockholm, Sweden
maria.andersson@foi.se, ronnie.johansson@foi.se, karl-goran.stenborg@foi.se, robert.forsgren@foi.se

T. Cane[c], G. Taberski[d], L. Patino[e], J. Ferryman[e]
[c]BMT Group Ltd, Teddington, UK
[d]ITTI, Poznan, Poland
[e]Computational Vision Group, Univ. of Reading, UK
tcane@bmtmail.com, grzegorz.taberski@itti.com.pl,
j.l.patinovilchis@reading.ac.uk,
j.m.ferryman@reading.ac.uk

Abstract—In the EU FP7 project IPATCH, we are researching components for a maritime piracy early detection and avoidance system for deployment on merchant vessels. The system combines information from on-board sensors with intelligence from external sources in order to give early warnings about piracy threats. In this paper we present the ongoing work with the development of an integrated system fusing heterogeneous data.

Keywords—threat detection, information fusion, Bayesian network, semantic model

I. INTRODUCTION

After a resurgence at the beginning of the 21st century, maritime piracy continues to place a huge economic and human cost on commercial shipping around the world [1]. Regions in the Gulf of Aden, West Africa, South East Asia and South America have turned into dangerous places for merchant vessels. It is of utmost importance for vessels in high-risk areas to detect piracy threats as early as possible so that the shipmaster can initiate countermeasures while they are still effective.

The poster proposes a maritime surveillance system that is developed in the EU FP7 project IPATCH (Intelligent Piracy Avoidance using Threat Detection and Countermeasure Heuristics) [2]. The aim is to automatically detect potential pirate attacks towards the vessel under protection. The outcome will be an improved understanding of the current situation for the vessel's crew, including a threat level estimation.

II. THE IPATCH ON-BOARD SYSTEM CONCEPT

The IPATCH on-board system is based on three modules: early detection, threat classification and decision support. The early detection module performs detection and tracking, based on input from on-board sensors. The threat classification module detects piracy threats by performing maritime situation assessment. The objects and their behaviours are analysed in context by looking at their trajectories (provided by the early detection module) and other situation parameters such as location, time of day and environmental conditions. Methods that are developed for the threat classification include expert-based event detection, semantic models for behaviour analysis and a Bayesian network (BN) model.

The BN model is used to fuse the information from events, behaviours and other situation parameters. It is based on the division of the threat concept into intent, capability and opportunity according to [3].

Results from the threat classification are input to the decision support module, which displays the current situation to the vessel crew via a decision support tool and user interface. In addition, the decision support module suggests appropriate countermeasures on the basis of potential and emerging threats, as derived from the threat classification module.

The whole system is underpinned by a common data model which is developed to support the end-to-end processing from per-sensor signal analysis to threat detection.

A data collection campaign took place in 2015 where a number of threat scenarios were recorded. Part of the dataset is available via PETS 2016 [4].

III. FUTURE WORK

Future work will be to test and evaluate the whole system using the collected data, and to connect the outcome from the threat classification to the choice of countermeasures.

REFERENCES

[1] Oceans Beyond Piracy, The State of Maritime Piracy 2014 (Denver, CO: One Earth Future Foundation), 2014.

[2] EU FP7 IPATCH (Intelligent Piracy Avoidance using Threat Detection and Countermeasure Heuristics), http://www.ipatchproject.eu/.

[3] Merriam-Webster (n.d.), Retrieved 04 26, 2012, from http://www.merriam-webster.com/dictionary/threat.

[4] PETS 2016, IEEE International Workshop on Performance Evaluation of Tracking and Surveillance, www.pets2016.net

IEEE computer society