Data fusion challenges for AIS anti-piracy measures

Loic Salmon, Pedro Merino Laso, Christophe Claramunt, Dominique Follut, Nicolas Pelissero

Data fusion challenges for AIS anti-piracy measures

1st Loïc Salmon
Naval Academy Research Institute, LabISEN
Ecole navale, ISEN Yncrea Ouest
Brest, France
loic.salmon@isen-ouest.yncrea.fr

2nd Pedro Merino Laso
Naval Academy Research Institute
French Maritime Academy (ENSM)
Nantes, France
pedro.merino-laso@supmaritime.fr

3rd Christophe Claramunt
Naval Academy Research Institute
Ecole navale
Brest, France
chistophe.claramunt@ecole-navale.fr

4rd Dominique Follut
Naval Academy Research Institute
French Maritime Academy (ENSM)
Nantes, France
dominique.follut@supmaritime.fr

5st Nicolas Pelissero
Chair of Naval Cyber Defense
Ecole navale
Brest, France
nicolas.pelissero@ecole-navale.fr

***Abstract*—Cruise operators offer a big amount on services in high quality onboard amenities. Cruise vessels has became a target for pirates because its potential value. These attackers use more and more sophisticated tools and strategies to perform successful attacks. In consequence, detection systems need to evolve to take in account these new threats. No system are able to cover all detection requirements, so proposed solution will operate with complementary sub-systems as AIS, radar and cameras.**

The aim of this position paper is to introduce current threats and challenges specifically related to Automatic Identification System (AIS) anti-piracy measures and how it can be useful in fusion detection methods. We also introduce ISOLA system as a complete detection and decision aid support against, among other threats, piracy attacks.

***Index Terms*—Anti-piracy, maritime security, AIS, data fusion**

I. Introduction

Cruise operators are challenged to develop competitive cruise packages for potential clients through developing new itineraries, high-quality onboard amenities, as well as shore-based excursions giving access to various cultural sites and activities in the countries where the ships dock. Despite the large numbers of people on board, crime reporting on cruise ships is so far relatively low. While the ship itself faces security threats, activities on board and on shore nowadays provide many opportunities for targets and security flaws to be exploited by individuals or groups with motivation to do so. For instance one of the main issues concerns organized groups that intentionally plan to attack vessels at sea, usually piracy or terrorism acts [1]. Therefore, cruise companies take security threats more and more seriously, with the objective of designing and implementing the most appropriate strategies and solutions to provide passengers the best security policies and ensure the cruise and its activities are not endangered by any security threats.

The research leading to these results is part of the ISOLA project that has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement No 883302.

Nowadays, piracy detection is mainly carried out from the collected information by navigation systems as AIS and radar. This works is executed manually by the crew assisted by ECDIS tools. Threat detection need to evolve to make automatic identification and alerts. Also, its important that the system will provide pertinent information to improve Security Situational Awareness.

This paper introduces current threats and challenges specifically related to Automatic Identification System (AIS) anti-piracy measures. The rest of the paper is organised as follows. We will first survey current existing protocol and solutions closely associated to AIS anti-piracy measures, as well as the range of suspicious activities, hijacks, boarding events and full-blown attacks that provide many different threats on board. In Section III, works concerning combining multiple data sources are discussed and a generic framework is proposed. Afterwards, in Section IV, we present a realistic scenario where proposed ISOLA solution is used to attack detection. Finally, we present and discuss our conclusions in Section V.

This work is part of the European project ISOLA (Innovative and Integrated Security System on Board Covering the Life Cycle of a Passenger Ships Voyage) developed as par to the Horizon2020 program.

II. AIS limitations and challenges for anti-piracy measures

While maritime monitoring capabilities have been largely extended over the past few years, AIS malicious actions are still possible and range from falsification of transmitted data to disappearance of AIS tracks [2].

The detection of deliberate piracy actions clearly requires the implementation of a vessel monitoring system whose objective will be to identify anomalies and abnormal behaviours potentially. In [3], the authors addressed and discussed computational issues associated to the integration of large maritime data flows in order to identify and visualize some phenomena of interest such as regular and abnormal behaviours. Within

the scope of the Datacron project [4], and in order to real-time monitor maritime data, ontologies provide appropriate mechanisms to generate data summaries and further event-based analysis [5].

However, there is still a need to develop and implement some specific real-time algorithms for tracking and categorize the large extent of vessel trajectories anomalies [6] as depicted in Figure 1 and those that can reveal some piracy threats.

Amongst the potential behaviours that can denote some anomalies and then potential piracy acts that happen at sea let us mention change of position, usurpation of identity (or AIS Spoofing) [2] [8], boats that no longer transmit their positions during a given time intentionally (or Going Dark) and necessitate some specific detection algorithms [9] [10].

In order to address all these issues in a timely manner, not only a sound analysis of AIS data should be provided as most of the above approaches do, but also integration of additional sensor-based capabilities provided by Unmanned Aerial Vehicle (UAVs), semi-autonomous or more conventional systems (radars, human observations etc.).

III. Towards maritime data fusion

Considering AIS limitations, different heterogeneous data integration solutions have been so far developed for a sound monitoring of vessel trajectories. For instance, in [11] authors use radar-based data and AIS signals to detect MMSI spoofing. Other approaches as Hidden Markov models have been applied to radar-based data and AIS signals to detect suspicious activities [12]

Novel operational systems are appearing in maritime as USVs (Unmanned Surface Vehicles) and AUVs (Aerial Unmanned Vehicle). These systems can be used separately or combined in different manners: sharing information or being deployed together [13]. Some platforms as Sea4M proposes a complete solution of attack detection thanks to the fusion of radar and AIS data and verifying and responding thanks to heterogeneous USVs [14]. Others suggest to combine AUV videos with AIS data [15], [16].

Despite the interest of these approaches the main limitation is that they mainly combined two specific sources of data and cannot cover for example the large range of sensors potentially available, this being specifically the case for large vessels such as cruising ships or very large cargos.

Under the scope of the H2020 ISOLA funded project, the system to be implemented should integrate a series of state-of-the-art technological achievements from multidisciplinary fields, namely sensors, Internet of Things as well as additional processing mechanisms such as semantic reasoning, high-level analytics, decision support systems, crisis management and situational awareness focusing on passenger's ship security sector and beyond. Figure 2 depicts the objective of the ISOLA monitoring system composed by legacy system of the boat (AIS/GPS and Radar) completed by a fleet of unmanned UxVs, IoT and cameras streams as part of an interoperable modalities to detect, assess, evaluate and locate threat actions within existing ships.

The interest of the ISOLA approach is that it allows to fuse data from different sources, this providing a sound approach to detect abnormal situations. For instance when a vessel changes its MMSI or switch off intentionally its signal, this could be detected by comparing AIS data with other data sources such as UAVs videos or radar.

IV. Use case

In this section, we introduce a realistic scenario where a group of pirates attacks a cruise vessel with limited but not negligible means. The attack is performed with a mother ship that can deploy multiple skiffs. The attackers will take advantage of weather conditions to hide their position and goals to the last moment.

A. Description

A cruise vessel is sailing in high seas within a High Risk Area in the Mediterranean Sea (Greece – Cyprus - Israel) and 200 nm close to recent piracy hot spots, as per latest security intelligence report. Five hours ago sea state gradually changed from level 6 to 2 of Douglas Sea Scale. Additionally, visibility decreased from 12 to 6 nm. This conditions are favorable for pirates because they can navigate safely with little skiffs while they can hide their position.

Initially cruise vessels radar detects a low speed target at a distance of 16 nm. The target continuously closing distance towards the cruise vessel starboard side. An experienced bridge officer categorizes the track as "suspicious target".

What happens in real is that the pirates mother ship launched two skiffs in close distance (less than 5nm) to cruise vessel almost undetectable due to low visibility and the high detection range scale in ship's radar. Despite the deter verbal and other visual warnings the skiffs entered vessel's security perimeter (3nm). Now the skiffs are upgraded to "attackers" since the three persons on each one of them are obvious equipped with weapons and climbing means.

Skiffs separated from each other at a distance of 1nm and both dared an attack starboard side and port side simultaneously. Pirates of one skiff appeared determined and one of the pirates managed to board, however, fell down wounded on main deck. Other pirates deterred and sailed away. One Crew Member of the Bridge Element accidentally wounded and fell down in the Bridge (didn't manage to reach the safe room). The aforementioned case was scripted based on real piracy attacks that took place across several years.

B. Limitations of existing detection solutions

As we can appreciate with this scenario, no system could be able to detect skiffs before they were too close, less than 1nm. Furthermore, there were no way to identify the suspicious mother ship that were detected in the firs time.

Attackers usually disconnect AIS transmitter to hide their position or they spoof their identity. Because of this, AIS data are often not interesting to detect piracy attacks. Nevertheless, this system can be useful to detect anomalies as when a ship

Fig. 1. Statistics concerning AIS frauds realised by Windward [7].

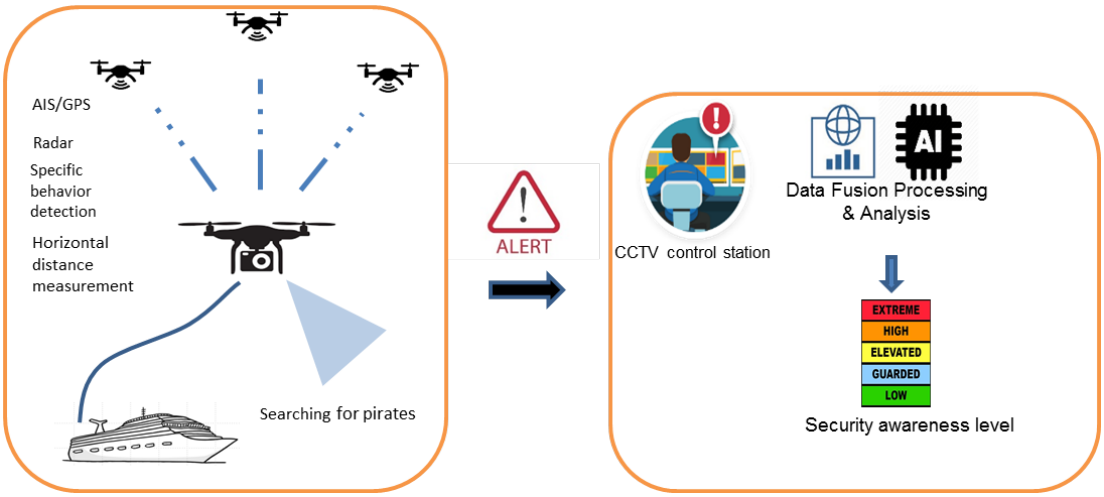

Fig. 2. ISOLA piracy detection process.

"goes dark" or to verify is shared information is coherent with other information sources i.e. cameras or radar.

Radar system is useful for detect medium-size vessels but it is not appropriate for detecting skiffs, boats that rarely measures more than 20 feet (about 6 meters) and usually used by pirates. Skiffs are also not detected because their height are comparable with swell and waves. Also, the scale used by the radar is usually adapted to navigation and not for piracy detection.

On-board cameras are useful to detect near targets These cameras can improve the visibility of the crew thanks to UHD (Ultra High Definition) sensors and zoom capabilities. Nevertheless, they are limited to visibility distance that can be significantly decreased by the weather. Because of this, pirates can take advantage easily of this limitation. Same way, IR cameras are useful for night scenarios but their action are also limited to a limited distance.

C. ISOLA's proposed solution

ISOLA is a complex system that take advantage of each subsystem in particular conditions. It embarks multiple subsystems, as shown in Figure 2. Collected data is presented to the watch personnel. In parallel, data is fused, processed and analyzed by adapted algorithms. Some of them make good use of Artificial Intelligence tools. These algorithms are able to improve Security Awareness Level thanks to automation and decision-aid capabilities.

In case the cruise ship of the presented scenario was equipped with ISOLA, a tethered drone carrying as payload a Smart Cameras System (one day/night HD fish-eye and one day/night UHD Zoom camera) and AI (Artificial intelligence) algorithms for skiffs distant detection and distinction from the sea waves noise would have been be deployed above the main mast of the vessel to maximize the covered area. This subsystem would have been covering on a permanent basis an

estimated surrounding distance of more than 6nm in favorable weather conditions.

AI algorithms for targets' horizontal distance measurement, localization and specific behaviour detection provides the security watch with a relevant alarm and the supportive information for preparing the response. The timely and accurate situation evaluation, the early threat recognition supports, the gradual application of Deter Measures against the attack and consequently the RUF (Rules for the Use of Force) are facilitated. In specific the main elements as suspicious activity criteria and threat estimation, compliance with SOP (Standard Operating Procedures) Counter Piracy Reaction Table, RUF, safety precautions to be taken, compliance with lines of authority and command, communication flow chart, decision making etc. were in place early enough to avoid any delay that could lead to a pirates embarkation if not close up.

ISOLA would also provide suggestions for announcements, messaging and reporting asking for help but also guidance to the crew by the PCASP (Privately Contracted Armed Security Personnel) and level of cooperation among them. Tethered drone's use, provided adequate data that fused verified and validated with other tracks in the surrounding area data, acquired by vessel's existing systems (ECDIS/ARPA, AIS, GPS and other) enhancing the human cognitive and raising early enough the Situational Awareness. As an option, AI algorithms could provide an automated "distress mode" service operation as an option for flawless unmanned operation.

V. Conclusion and future directions

This paper has presented different challenges for piracy attack detection due mainly to AIS limitations as well as meteorological conditions. Some works have been initiated to use one another source to correlate the position given by AIS, however merging of multiple sensors has not been addressed yet. In this paper, we have defined the main principles of a system for multiple sensor data fusion developed in the context of ISOLA project for safety of cruising ships. A lot of different data sources as drone images, AIS data or radar are available and necessitate mechanisms for data fusion. The main idea is the formalization and the development of an ontology for piracy attack detection. However, there is still a large range of issues from the development of appropriate sensing architectures at large, to data fusion algorithms for piracy detection and threats classification at sea, as well as visualization interfaces still to be developed for both maritime authorities and crew members.

ISOLA will contribute to the Enforcement of PMSC's SOPs and RUF, Captain's standing orders and Company's policies and regulations aboard the ship. It will deliver the required warning signals and suggestions to the ship's key personnel and the Private Contracted Armed or Unarmed Security Personnel Team Leader (the initial evaluator and first responder) regarding the gradual implementation of pirates preventive actions, in terms of effective early warning, detection, situation evaluation, decision making and emergency responding, not allowing the situation escalation and preserving the security and safety of people on-board and vessel's operations continuity.

Acknowledgment

The authors would like to thank to the other participants of the ISOLA project for their work and dedication.

References

[1] B. Møller, "Piracy, maritime terrorism and naval strategy," Copenhagen, DIIS Report 2009:02, 2009. [Online]. Available: http://hdl.handle.net/10419/59849

[2] C. Ray, C. Iphar, A. Napoli, R. Gallen, and A. Bouju, "Deais project: Detection of ais spoofing and resulting risks," *OCEANS 2015 - Genova*, pp. 1–6, 2015.

[3] C. Claramunt and C. Ray et al, "Maritime data integration and analysis: recent progress and research challenges," in *Proceedings of the 20th International Conference on Extending Database Technology, EDBT 2017, Venice, Italy, March 21-24, 2017*. OpenProceedings.org, 2017, pp. 192–197. [Online]. Available: https://doi.org/10.5441/002/edbt.2017.18

[4] G. A. Vouros and G. L. Andrienko et al, *Big Data Analytics for Time-Critical Mobility Forecasting, From Raw Data to Trajectory-Oriented Mobility Analytics in the Aviation and Maritime Domains*. Springer, 2020. [Online]. Available: https://doi.org/10.1007/978-3-030-45164-6

[5] L. Salmon and C. Ray, "Design principles of a stream-based framework for mobility analysis," *GeoInformatica*, vol. 21, no. 2, pp. 237–261, 2017. [Online]. Available: https://doi.org/10.1007/s10707-016-0256-z

[6] M. Riveiro, G. Pallotta, and M. Vespe, "Maritime anomaly detection: A review," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 8, 2018.

[7] Windward, "Windward,ais data on the high seas : An analysis of the magnitude andimplications of growing data manipulation at sea," Windward, Tech. Rep., 2014.

[8] I. Kontopoulos, G. Spiliopoulos, D. Zissis, K. Chatzikokolakis, and A. Artikis, "Countering real-time stream poisoning: An architecture for detecting vessel spoofing in streams of ais data," in *2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, 2018, pp. 981–986.

[9] I. Kontopoulos, K. Chatzikokolakis, D. Zissis, K. Tserpes, and G. Spiliopoulos, "Real-time maritime anomaly detection: detecting intentional AIS switch-off," *Int. J. Big Data Intell.*, vol. 7, no. 2, pp. 85–96, 2020. [Online]. Available: https://doi.org/10.1504/IJBDI.2020.107375

[10] L. Salmon, C. Ray, and C. Claramunt, "Continuous detection of black holes for moving objects at sea," in *Proceedings of the 7th ACM SIGSPATIAL International Workshop on GeoStreaming, IWGS@SIGSPATIAL 2016, Burlingame, California, USA, October 31 - November 3, 2016*, F. B. Kashani, C. Zhang, and A. M. Hendawi, Eds. ACM, 2016, pp. 2:1–2:10. [Online]. Available: https://doi.org/10.1145/3003421.3003423

[11] T. Zhang, S. Zhao, B. Cheng, and J. Chen, "Detection of ais closing behavior and mmsi spoofing behavior of ships based on spatiotemporal data," *Remote Sensing*, vol. 12, no. 4, 2020. [Online]. Available: https://www.mdpi.com/2072-4292/12/4/702

[12] M. Andersson and R. Johansson, "Multiple sensor fusion for effective abnormal behaviour detection in counter-piracy operations," in *2010 International WaterSide Security Conference*, 2010, pp. 1–7.

[13] G. Shao, Y. Ma, R. Malekian, X. Yan, and Z. Li, "A novel cooperative platform design for coupled usv–uav systems," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 4913–4922, 2019.

[14] P. M. Laso, D. Brosset, and M.-A. Giraud, "Monitor and control human-computer interface for unmanned surface vehicle fleets," in *OCEANS 2019-Marseille*. IEEE, 2019, pp. 1–5.

[15] F. Zhou, S. Pan, and J. Jiang, "Verification of ais data by using video images taken by a uav," *Journal of Navigation*, vol. 72, no. 6, p. 1345–1358, 2019.

[16] S. Xiu, Y. Wen, H. Yuan, C. Xiao, W. Zhan, X. Zou, C. Zhou, and S. C. Shah, "A multi-feature and multi-level matching algorithm using aerial image and ais for vessel identification," *Sensors*, vol. 19, no. 6, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/6/1317