Enhancing Resilience of Critical Maritime Infrastructure through Modeling and Simulation of Sensors Configuration

Marcos Julien Alexopoulos, Arto Niemi, Bartosz Skobiej, Frank Sill Torres
Institute for the Protection of Maritime Infrastructures
German Aerospace Center (DLR), Bremerhaven, Germany
Email: marcos.alexopoulos@dlr.de

***Abstract*—Critical Maritime Infrastructure (CMI) such as ports, underwater pipelines, and offshore platforms are essential for the security of supply of a state. However, growing reliance on CMI brings security risks from potential attacks. This paper reviews recent academic approaches for security threat analysis, which utilize methodologies for the development of scenarios and quantification of outcome likelihood. Building on these works, a framework is proposed to optimize surveillance and improve situational awareness for CMI with emphasis in offshore infrastructures. The methodology offers the option of enabling Modeling and Simulation (M&S) tools to simulate threat scenarios and test sensor configurations. Specific criteria that an M&S tool must satisfy are outlined, including Monte Carlo analysis, comprehensive databases, customizability, and environmental modeling. M&S could enable relevant authorities to visualize vulnerabilities, strategically position sensors, and enhance CMI resilience against diverse man-made threats. The proposed framework offers a practical, cost-effective solution for maximizing domain awareness and mitigating emerging security risks to vital maritime assets and activities.**

***Index Terms*—Critical Maritime Infrastructure, Modeling and simulation, Situational awareness, Security, Resilience**

I. Introduction

Critical infrastructure is crucial for states to deliver essential services and ensure public safety, security, health and economic functioning. Its definition is varying depending on the source of information. The European Union defines critical infrastructure as "any asset, facility, system or part thereof that is necessary for the provision of essential services." [1]. These services are ingrained within 11 sectors in the Directive on the Resilience of Critical Entities (2023) [1], addressing energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, and production, processing and distribution of food. Within the maritime sector, critical infrastructure is broadly classified into five key areas, according to the framework described by Bueger and Liebetrau (2023): transport, energy, communications, fisheries, and ecosystems [2]. Each area represents aspects of critical infrastructure that exist on, in, or connected to the sea. Transport encompasses ports, vessels, operators of vessel traffic services, as well as the supporting infrastructure needed to facilitate maritime trade and the movement of goods. Energy incorporates offshore wind farms, oil and gas rigs, pipelines, and other equipment vital for energy production and distribution. Communications infrastructure consists of submarine cables for transmitting data and digital communications. For fisheries it involves fishing ports and the systems supporting commercial fishing activities. Ecosystems infrastructure refers to the natural environment and resources that maritime industries and coastal communities depend upon.

The importance of Critical Maritime Infrastructure (CMI) is expected to grow in the coming years. This is evident in the energy sector, which is forecasted to see significant expansion. Currently under construction globally are approximately 68,000 km of pipelines, with an additional 129,644 km in the planning phase, as of 2024 [3]. Europe in particular is taking steps to strengthen its energy security and reduce dependence on Russian imports. By 2025, the region is projected to expand its Liquid Natural Gas pipeline network by over 21,333 km [3]. On a country level, Germany has unveiled plans to develop new CMI for its energy transition. In November 2023, the german government announced a proposed hydrogen pipeline artery, totaling 9,700 km in length [4], part of which extends in the Baltic Sea.

Another sector of CMI poised for growth is renewable energy. In Europe, offshore wind energy capacity is predicted to see expansion over the next six years, as the region works to meet its climate targets. In 2020, the EU increased its 2030 greenhouse gas emission reduction goal from 40% to 55% [5]. To help achieve this, on the 14th of July 2021 the European Commission proposed the 'Fit-for-55' legislative package [6]. This revises the Renewable Energy Directive [7], and sets a higher renewables target that is expected to drive additional demand for offshore wind farms. Specifically, the EU states it will require over 500 GW of total wind power capacity by 2030 [7]. To reach this level, approximately 23 GW of offshore capacity needs to be added per year, between 2024 and 2028 [8].

The increasing investment and reliance of states in CMI creates a security vulnerability. This kind of infrastructure is not heavily surveilled and is exposed to potential attacks. According to the Global Terrorism Database, there were 120 cases of maritime terrorism during 2015-2020 [9]. Commercial and tanker ships have been frequent targets for terrorist groups. For example, in March 2017, assailants hijacked a cargo ship off the Philippines, abducting crew members [10]. In

November 2020, an explosive device detonated on an oil tanker off Saudi Arabia [11], and in October 2020, a bomb exploded on an oil tanker in Yemen [12]. Underwater pipelines are also at risk, especially during times of conflict. Besides the well-known Nord Stream 1 and 2 attacks in September 2022, another attack occurred on the Finland-Estonia gas pipeline in October 2023 [13]. Operations estimate it will take approximately six months to restore functionality. Also, offshore oil rigs have occasionally been a target. While most oil rigs are onshore, as of 2023 there are 240 offshore operational oil rigs [17]. They have been common targets for looting, such as between May-August 2022 when three platforms were raided in the Bay of Campeche [18].

The value of offshore assets is increasing and becoming more vital for economic well-being. Therefore, there is a greater need to emphasize the prevention and response to attacks on critical marine infrastructure, as well as assets within that infrastructure that ensure performance and reliability. In the literature, for the protection of CMI, several frameworks have been proposed that align with the principles of resilience, as laid down by Article 2 of Directive (EU) 2022/2557 [1]. In addition, technology offers an increasing number of options for the surveillance of critical entities, which can be used in accordance with subletter (a) of paragraph 1 [1]. A short overview of this technology is presented below, according to the classification provided by Soldi et al. (2023) [19].

- Coastal radars: S-band or X-band pulse radar sensors installed along the coastline provide information on surface vessels, but their coverage area and maximum range are limited by line-of-sight propagation.
- High-Frequency Surface-Wave (HFSW) radars: These sensors can detect targets at Over-The-Horizon (OTH) distances. They overcome the limitations of coastal radars and provide continuous-time coverage of large sea areas.
- Automatic Identification System (AIS): An anti-collision broadcast system of transponders that automatically exchanges ship traffic information.
- Synthetic Aperture Radar (SAR): A high-resolution imaging system employed on board satellites or aircraft. It is capable of detecting and tracking vessels at sea independently of their compliance with AIS. Also it is not dependant on weather conditions or sunlight illumination.
- Multi-spectral (MSP) and Hyper-spectral (HSP) sensors: Optical sensors covering the optical region. They provide imagery at higher spatial and spectral resolutions than SAR, which allows for accurate classification and analysis of surface features.
- Underwater sensors: Active/passive sonars, cameras, and other sensors installed on the UCIs or equipped on Unmanned Underwater Vehicles (UUVs) for undersea monitoring.
- Distributed Acoustic Sensing (DAS): A technology that allows for continuous acoustic monitoring of underwater cables and pipelines, detecting potential threats and anomalies.

An important question is presenting itself: how can this state-of-the-art gear can be configured in order to optimize the identification of suspicious patterns and maximizing response time in the domain of CMIs. One way to address this is with the implementation of Modeling and Simulation (M&S) tools. NATO and similar organizations employ this software in order to derive insights for case studies and perform analysis of defence scenarios. Besides warfare units, this type of software allows the implementation of sensor technology, and enables the modeler to customize sensor technical parameters. The reader can find a selection of this software here [14]–[16]. Thus, M&S tools can provide a cost-effective representation of the physical environment. They allow for easy exploration of different scenarios and configurations, enabling the identification of the most effective sensor placement strategies under various conditions. It can be applied to large-scale critical marine infrastructure systems, which would be infeasible to analyze in the real world. Since research is lacking on using M&S to determine optimal sensor configurations, we propose criteria that an M&S tool must meet, in order to achieve target objectives. Furthermore, we test a simple experiment within an M&S tool for a case study in Germany, in order to verify whether it can provide quantifiable information for sensor placement.

II. Background

Security threat analysis has become increasingly complex due to the variety of potential threats and the sophistication of potential attackers. Recent academic work in this field has focused on the development of methodologies to analyze and prioritize security threats. Lichte et al. (2020) present a comprehensive hazard analysis methodology, using transmission systems as an example of a target [20]. The approach begins by defining the solution space through high-level category selection and characterization, leveraging expert knowledge from transmission system operators and security experts. As a second step, a consistency check of scenarios is performed with the implementation of a consistency matrix, alongside the clustering of assets to differentiate criticality. As a last step, risk factors are estimated for both the scenarios and assets, culminating in a security hazard risk matrix that aids in prioritizing scenarios for further examination. In a similar vein, Schneider et al. approach the security threats posed by civilian drones through a detailed scenario analysis [21]. The process starts with determining the scenario space, with sub-categories informed by literature reviews and expert interviews. An influence analysis using a matrix leads to the identification of key factors, which are then assessed for consistency using Cross-Impact Balance analysis. Similarly, Johansen's work is based on scenario modelling with morphological analysis, which is then subjected to cross-consistency assessment [22].

Another paper written by Witte et al. also employs a systematic identification of the problem space, but introduces a Bayesian network for the assessment of threat scenarios [23]. The methodology hinges on defining threat descriptors, setting up a Bayesian network to represent dependencies, and quantifying these through expert judgement. The result is a computation of probabilities for each scenario, which is then used to rank the most significant threats, providing a structured

approach to threat analysis. Lastly, Witte et al. delve into the impact of epistemic uncertainty on security risk analysis [24]. Their methodology features a morphological threat analysis, with the addition of a spatial analysis of security systems to derive potential attack paths. This is coupled with a vulnerability model and Bayesian network model to calculate scenario vulnerabilities and likelihoods. The aggregation of scenario-specific risks, weighted by these likelihoods, offers an overall risk measure.

III. Methodology

Within this context, we propose a framework where we make use of software available on the market, in order to perform a constructive simulation of relevant threat scenarios. The main idea is to define a scenario within an M&S tool, and through hundreds of iterations that account for aleatory uncertainty, derive optimal positions of a given sensor configuration in a study area.

The chosen M&S tool must meet a series of requirements to ensure it is fit for the purpose of optimizing sensor placement and configuration for the protection of CMI. The efficacy of an M&S software for our research hinges on several capabilities, which we have identified as essential for the accurate simulation of security scenarios involving CMI. The list below summarizes the criteria that the M&S tool must satisfy:

- Monte Carlo analysis – Essential for probabilistic risk assessment and understanding the variability in threat outcomes.
- Comprehensive offender vehicle and drone database – To accurately simulate potential threats, including aircraft, submarines, land vehicles, and unmanned vehicles.
- Sensor database – Up-to-date information on sonar, radar, and optical sensors to simulate detection capabilities.
- Bathymetric data – For subsurface operations and sensor performance simulations.
- High resolution terrain – To simulate sensor line-of-sight and signal propagation constraints.
- Weather and environmental effects – To assess the impact of various conditions on sensor performance and surveillance efficacy, and account for effect on the trajectory of offensive vehicles.
- Scenario retrieval – Capability to save, retrieve, and rerun scenarios for refinement and traceability.
- Customizability of sensor Parameters – To simulate different sensor configurations accurately, and inserting properties which are not available commercially.
- Consideration of physical variables – Realistic representation of the marine environment and sea state, for example temperature, salinity and currents.

Each of our proposed requirements is justified based on the need to simulate complex and dynamic security scenarios that involve a multitude of variables. Monte Carlo analysis is useful for assessing risks in a probabilistic manner, and introduces the uncertainties introduced by the physical system. An up-to-date database ensures that the simulated assets and threats are reflective of current capabilities and technologies. Including bathymetric and detailed terrain data is necessary for accurate simulation of sensor effectiveness, especially when considering the impact of environmental features and obstructions on detection ranges and signal clarity. The inclusion of weather and environmental effects has similar importance, as adverse conditions can negatively impact the performance of surveillance systems. The ability to retrieve and rerun scenarios is important for iterative analysis and allowing the scenario to be traceable for the modeler. Customizability is a key feature that allows for the exploration of a wide range of sensor configurations, while target and environmental modeling ensure that simulations provide a realistic representation of potential threats and environmental conditions.

IV. Case Study

As a test, we conduct a trial simulation within the Ternion software platform [14]. This platform supports the development of complex, realistic scenarios by integrating features like collaborative entity editing, improved multithreading, and realistic 3D environments through its Unreal Engine option. This makes it suitable for detailed and large-scale simulations.

Our selected study area is a part of the port in Brake in the northwest Germany. The port is situated on the west bank of the Weser between cities of Bremen and Bremerhaven. We perform the simulation on a 3 km by 3 km area north from the port. Within this area, we position a radar sensor at an elevation of approximately 60 m (Fig. 1). We implement a radar sensor, with the antenna height set to 2 meters from ground level; otherwise its detection capacity will be hindered.

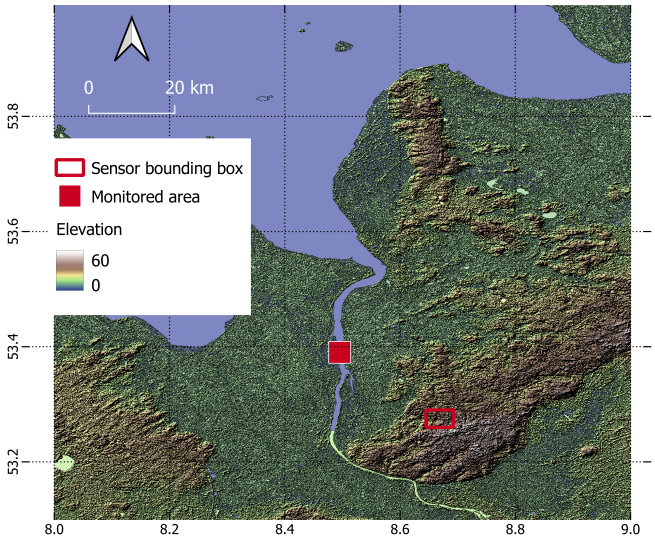

Fig. 1. Study area encompassing Brake and depiction of radar placement and monitored quadrants.

The primary objective of this exercise is to conduct iterations within a defined sensor quadrant in a parameter sweep fashion. For each iteration, we sample a different position for the radar within the box using a uniform distribution, ensuring that each sensor position is unique. The ultimate goal is to calculate the time required for the radar to detect a ship

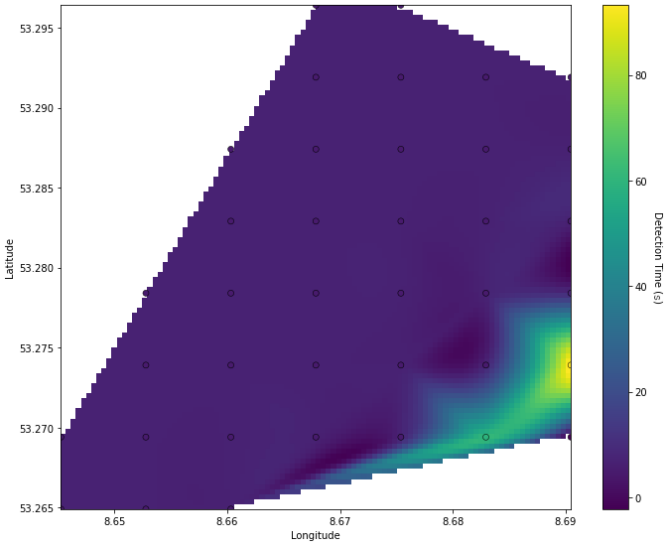

Fig. 2. Gradient plot depicting detection times per iteration.

when it enters the monitored area. We perform 100 iterations, each with a different radar position within the bounding box. For each iteration, we simulate a ship entering the monitored area, and record the time it takes for the radar to detect the vessel. The vessel trajectory remains constant across iteration for consistency. The exercise's results are presented in Fig. 2. The gradient depicts the change in detection time, according to the set of coordinates at the time of the iteration. Not all 100 runs yield results, as in some positions, radar ranges are obstructed. Sixty-three sampled sets of coordinates are rendered useless during this exercise. Conversely, only 37 of these trials provide estimates. This is probably due to the effect of partial obstruction based on the elevation of the radar position. In these cases the radar does not capture the monitored area due to its location.

V. Conclusion

In this publication we address the increasing reliance of states on offshore CMIs, and how their security becomes a growing need in years to come. The subject of physical security is a topic that is slowly gaining popularity in academic literature [25]–[27]; therefore a review of proposed frameworks for scenario development and quantification of likelihood has been presented. At the time of writing there are proposed frameworks for the increase of situational awareness and optimization of surveillance of offshore CMIs [28]–[31]. Within this context, we propose a practical and cost-effective solution for identifying the most effective implementation of sensors, which could increase domain awareness at a place of interest. Moreover, we present a case study utilizing an M&S simulation platform to evaluate sensor positioning for areas of interest within CMI. Our simple demonstration using a part of the port of Brake, Niedersachsen illustrates the potential of such tools in optimizing radar placement for enhanced maritime surveillance. We suggest that sensor placement can be optimized according to their ability to reach their target. In addition, radar positioning can impact detection times, however, with minor differences. While this trial is insightful, it is merely a starting point. Future work will incorporate more complex scenarios, multiple sensor types, and will provide the foundation for a more sophisticated framework. The ability to perform robust simulations could enable authorities and relevant stakeholders to not only visualize and understand potential vulnerabilities within their maritime assets, but also to strategically optimize sensor placements and configurations. By addressing these needs, the proposed M&S tool could serve as an instrument for enhancing resilience and security of CMI against a diverse range of threats. Thus, safeguarding vital socioeconomic activities and environmental resources tied to the maritime domain.

References

[1] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, *Official Journal of the European Union*, vol. L 333, pp. 164-240, 2022. [Online]. Available: https://www.official-documents.eu/en/browse.

[2] C. Bueger and T. Liebetrau, "Critical maritime infrastructure protection: What's the trouble?," *Marine Policy*, vol. 155, pp. 105772, 2023. doi:10.1016/j.marpol.2023.105772. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0308597X23003056.

[3] M. Reed, "Global Pipeline Construction Outlook 2024: New LNG Terminals Sound Beckon Call for More Pipelines," *Pipeline and Gas Journal*, vol. 251, no. 1, 2024.

[4] L. Collins, "German hydrogen pipeline network will begin transporting H2 in 2025, with 9,700km in place by 2032, says government," Nov. 14, 2023. [Online]. Available: https://www.hydrogeninsight.com/policy/german-hydrogen-pipeline-network-will-begin-transporting-h2-in-2025-with-9-700km-in-place-by-2032-says-government/2-1-1554455. [Accessed: Jan. 15, 2024].

[5] European Commission, "European Green Deal: Commission proposes transformation of EU economy and society to meet climate ambitions," Jul. 14, 2021. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3541.

[6] European Parliament and of the Council, "Directive 2009/28/EC of the European Parliament and of the Council of 23 April 2009 on the promotion of the use of energy from renewable sources and amending and subsequently repealing Directives 2001/77/EC and 2003/30/EC," 2009, apr. [Online]. Available: http://data.europa.eu/eli/dir/2009/28/oj, Issuer: Official Journal of the European Union.

[7] European Commission, "Commission sets out immediate actions to support the European wind power industry," Oct. 24, 2023.

[8] IEA, "Renewables 2023," 2024, Paris: IEA. [Online]. Available: https://www.iea.org/reports/renewables-2023. Note: Licence: CC BY 4.0.

[9] Global Terrorism Database, National Consortium for the Study of Terrorism and Responses to Terrorism (START), 2022. [Online]. Available: https://www.start.umd.edu/gtd.

[10] E. dela Cruz and C. Schmollinger, "Philippine troops rescue ship captain kidnapped by militants," Reuters, 25-Mar-2017. [Online]. Available: https://www.reuters.com/article/us-philippines-militants-idUSKBN16W06O/.

[11] J. Saul and L. Barrington, "Oil tanker hit by blast at Saudi terminal, Saudi Arabia confirms," Reuters, 25-Nov-2020. [Online]. Available: https://www.reuters.com/article/saudi-security-tanker/oil-tanker-hit-by-blast-at-saudi-terminal-saudi-arabia-confirms-idUSKBN28520B/.

[12] The Maritime Executive, "Crude Tanker Damaged by Floating Mines Near Yemeni Oil Terminal" The Maritime Executive, 09-Oct-2020. [Online]. Available: https://www.maritime-executive.com/article/crude-tanker-damaged-by-floating-mines-near-yemeni-oil-terminal?rand=17996.

[13] A. Kauranen and T. Solsvik, "Finland says 'outside activity' likely damaged gas pipeline, telecoms cable," Reuters, 11-Oct-2022. [Online]. Available: https://www.reuters.com/markets/commodities/finnish-government-hold-news-conference-suspected-pipeline-leak-media-2023-10-10/.

[14] "FLAMES Simulation Framework," FLAMES Simulation Framework, [Online]. Available: https://flamesframework.com/

[15] "JCATS — Joint Conflict and Tactical Simulation," Computing - Lawrence Livermore National Laboratory, [Online]. Available: https://computing.llnl.gov/projects/jcats
[16] "Command: Modern Operations," Matrix Games, [Online]. Available: https://command.matrixgames.com/
[17] Statista, "Number of land and offshore oil rigs worldwide at the end of each year from 2010 to 2023" Statista, 2023. [Online]. Available: https://www.statista.com/statistics/1128408/number-of-global-oil-rigs-by-type/
[18] Offshore magazine, "GoM continues to see threat from maritime crime, piracy," Offshore, 20-Mar-2023. [Online]. Available: https://www.offshore-mag.com/regional-reports/us-gulf-of-mexico/article/14291254/gom-continues-to-see-threat-from-maritime-crime-piracy
[19] G. Soldi, D. Gaglione, S. Raponi, N. Forti, E. d'Afflisio, P. Kowalski, L. M. Millefiori, D. Zissis, P. Braca, P. Willett, A. Maguer, S. Carniel, G. Sembenini, and C. Warner, "Monitoring of Critical Undersea Infrastructures: the Nord Stream and Other Recent Case Studies," *IEEE Aerospace and Electronic Systems Magazine*, doi: 10.1109/MAES.2023.3285075, 2023.
[20] Schneider, Moritz and Lichte, Daniel and Witte, Dustin and Gimbel, Stephan and Brucherseifer, Eva. "Scenario Analysis of Threats Posed to Critical Infrastructures by Civilian Drones." In 31st European Safety and Reliability Conference, ESREL 2021, 520-527. Angers, France: Research Publishing Services, 2021. Available at: https://elib.dlr.de/147231/. DOI: 10.3850/978-981-18-2016-8_4-cd.
[21] Lichte, Daniel and Witte, Dustin and Wolf, Kai-Dietrich. "Comprehensive Security Hazard Analysis for Transmission Systems." 2020, May. Available at: https://elib.dlr.de/xxxxxx.
[22] Iver Johansen, "Scenario modelling with morphological analysis", Technological Forecasting and Social Change, vol. 126, 2018, pp. 116-125. doi:https://doi.org/10.1016/j.techfore.2017.05.016. Available at: https://www.sciencedirect.com/science/article/pii/S004016251730656X.
[23] Witte, Dustin and Lichte, Daniel and Wolf, Kai-Dietrich. "Threat Analysis: Scenarios and Their Likelihoods." In 30th European Safety and Reliability Conference, ESREL 2020 and 15th Probabilistic Safety Assessment and Management Conference, PSAM15 2020, 4589-4595, 2020. Available at: https://elib.dlr.de/147230/.
[24] Witte, Dustin and Lichte, Daniel and Wolf, Kai-Dietrich. "On the Impact of Epistemic Uncertainty in Scenario Likelihood on Security Risk Analysis." In 33rd European Safety and Reliability Conference (ESREL 2023), 3260-3267, September 2023, Southampton, United Kingdom. Research Publishing, Singapore, Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023). doi:10.3850/978-981-18-8071-1_P603-cd. Available at: https://elib.dlr.de/202008/.
[25] Bowen, Zou and Jian, Liu and Wenlin, Wang and Zhenyu, Yan and Gaojun, Liu and Jun, Yang and Ming, Yang. "Development of an Interaction Simulator for the Scenario Analysis of Physical Protection Systems." IEEE Access 7 (2019): 91509-91517.
[26] Argyroudis, Sotirios A and Mitoulis, Stergios A and Hofer, Lorenzo and Zanini, Mariano Angelo and Tubaldi, Enrico and Frangopol, Dan M. "Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets." Science of The Total Environment 714 (2020): 136854.
[27] Khalil, YF. "A novel probabilistically timed dynamic model for physical security attack scenarios on critical infrastructures." Process Safety and Environmental Protection 102 (2016): 473-484.
[28] Gopinath, M.P., Tamizharasi, G.S., Kavisankar, L. et al. "A secure cloud-based solution for real-time monitoring and management of Internet of underwater things (IOUT)." Neural Computing & Applications 31 (Suppl 1), 293–308 (2019). https://doi.org/10.1007/s00521-018-3774-9.
[29] Jin, Guanghao, Fan Liu, Hao Wu, and Qingzeng Song. "Deep learning-based framework for expansion, recognition and classification of underwater acoustic signal." Journal of Experimental & Theoretical Artificial Intelligence 32, no. 2 (2020): 205-218. DOI: 10.1080/0952813X.2019.1647560.
[30] Eleftherakis, Dimitrios and Vicen-Bueno, Raul. "Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors." Sensors 20, no. 3 (2020): 737. https://www.mdpi.com/1424-8220/20/3/737. PubMedID: 32013207. DOI: 10.3390/s20030737.
[31] Liu, Linfeng, Yaoze Zhou, Zhiyuan Xi, Jiagao Wu, and Jia Xu. "Defense against underwater spy-robots: A distributed anti-theft topology control mechanism for insecure UASN." Computers & Security 129 (2023): 103214. https://doi.org/10.1016/j.cose.2023.103214.