Towards Semantic Modeling and Simulation of Cybersecurity on the Internet of Underwater Things

Stavros Stavrinos, Konstantinos Kotis, Christos Kalloniatis

Towards Semantic Modeling and Simulation of Cybersecurity on the Internet of Underwater Things

Stavros Stavrinos[1], Konstantinos Kotis[1][0000-0001-7838-9691], Christos Kalloniatis[1][0000-0002-8844-2596]

[1]Dept. of Cultural Technology and Communication, University of the Aegean, Mytilene, 83100 Greece
cti21010@ct.aegean.gr, kotis@aegean.gr, chkallon@aegean.gr

Abstract. As maritime and military missions become more and more complex over the years, there has been a high interest in the research and development of Unmanned Underwater Vehicles (UUVs). Latest efforts concern the modeling and simulation of UUVs collaboration within formations of vehicles (swarms), towards obtaining deeper insights related to critical issues related to cybersecurity and interoperability. The research issues which are constantly emerging in this domain are closely related to the communication, interoperability, and secure operation of trustworthy UUVs, as well as to the volume, velocity, variety, and veracity of data transmitted in low bitrate due to the medium i.e., the water. This paper focuses on such issues in the domain of UUVs, emphasizing interoperability and cybersecurity in swarms of trustworthy UUVs in a military/search-and-rescue (SAR) setting. The aim of this paper is to present preliminary work on a semantic modeling and simulation approach that aims to facilitate commanders of military/search-and-rescue operations to effectively support critical and life-saving decision-making, while handling interoperability and cybersecurity issues on the Internet of Underwater Things (IoUT).

Keywords: IoUT, UUVs, interoperability, semantics, cybersecurity, simulation.

1 Introduction

Semantic modeling (e.g., ontologies) provides the ability to interconnect heterogeneous devices and applications, enabling their communication in a common standardized language. By providing a shared and commonly agreed conceptualization for representing domain knowledge related to entities and relations between them, the efficient and effective interaction between those entities (hardware, software, human) is facilitated [26]. By implementing such a communication ecosystem in a simulated environment, facilitates monitoring and prediction of possible situations in the field of action, eventually supporting efficient decision-making. Specifically, in the domain of IoUT, where there is a need for continuous, reliable, and secure interoperability between various trustworthy underwater assets, the main challenge is to preserve high-level understanding (common semantics) in the communication between them [11].

Especially due to the volume (big data) and veracity (heterogeneous data) of exchanged information, the utilization of suitable semantic models is a key factor.

UUVs are powerful complex assets operating in IoUT environment [31]. Establishing communication between them, as well as between them and other platforms (at sea, air, and surface), is critical. UUVs are self-managed and knowledge-based autonomous agents which can integrate different frameworks and applications, making them effective and versatile assets acting in unknown and hazardous networks, such as in Underwater Wireless Sensor Networks (UWSNs) [12]. The replacement of human factor in autonomous assets operating in such a trustworthy setting (to avoid the cost of human training and loss, as well as to overcome ethical barriers in military operations) is a key reason for their enormous development in the last decade. In addition, collaboration of underwater and aerial unmanned vehicles operating in swarms, unlock many more capabilities and potentials by accomplishing collaborative tasks even more effectively and efficiently. However, due to the complexity of the setting they act, many challenges and key issues are emerging such as interoperability and security issues [24].

To support efficient decision-making of commanders operating in such a complex setting, advanced simulation approaches that are based on the integration of different tools are required, effectively simulating/co-simulating critical situations and possible threats/vulnerabilities of heterogeneous assets 'living' in the underwater environment. The goal is to facilitate standardization of response in such situations towards trustworthy and less risky, decision-making in military and SAR operations.

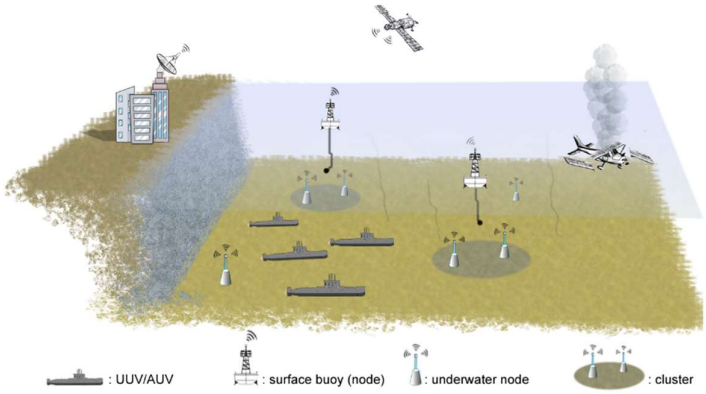

Fig. 1. Topology of UWSN in a SAR scenario involving UUVs, underwater nodes (and clusters), as well as surface nodes.

Let us assume the following SAR scenario (Figure 1). A swarm of UUVs must travel to an exact location of a plane crash at sea, safely and quickly, while interoperating in an UWSN, while exchanging information/data in real-time, utilizing adaptive path-planning. During the execution of predefined tasks, an unusual delay in communication between them and the underwater nodes is identified, affecting the robustness of the network architecture, resulting in the inability of commander to get the trans-

mitted information. An automated analysis of the incident issues an alert for huge numbers of data packets overwhelming the network, thus, an incoming DoS (Denial of Service) attack is flagged. Consequently, an automated process of various counter-methods and protocols is initiated, such as honeypots, encryption algorithms, security rules etc. Such a scenario must be simulated in order to be possible for commanders to be able to use, validate, and update security protocols, as well as to learn how to effectively anticipate such critical situations by testing alternative topologies, and so on, minimizing, eventually, handling costs and life losses.

IoUT is a new research and development domain that aims to tackle many of the challenges of UUVs introduced above, such as interoperability, data management, and cybersecurity [25]. The motivation of this research is the exploration of these challenges in order to propose an efficient and effective simulation approach that is necessary for commanders of military/SAR operations to effectively support critical and life-saving decision-making. More specifically, the ultimate goal is to support SAR and military commanders with an efficient UUVs swarm simulation environment that will emphasize interoperability and cybersecurity issues, in order to achieve and establish secure exchange of interoperable data/information. Based on this motivation the contribution of this paper is a) to review existing methods and tools of semantic modeling and simulation for cybersecurity on the IoUT, b) to propose an efficient and effective tool-supported simulation approach that is necessary for commanders of military/SAR operations to effectively support critical and life-saving decision-making.

The remainder of this paper is organized as follows. Section 2 presents related work on semantic modeling and simulation of cybersecurity issues, as well as freely available simulation tools in the domain of IoUT. Section 3 presents our experiments with existing approaches/tools, and introduce the proposed approach. Section 4 discusses identified challenges and issues in the underwater cybersecurity domain. Section 5 concludes the paper.

2 Preliminaries and Related Work

Recently, the utilization of UUVs has been demonstrated, especially in SAR incidents, taking advantage of underwater beacons generated by airplanes, activated in emergency situations (e.g., a crash) [38]. A representative example is the discovery of debris of Air France Flight 447 by a swarm of UUVs (using their side-scan sonar) at a depth of 3,980 meters [22].

As presented in related work [6], in order to overcome data heterogeneity between assets, an Ontology-Based Data Access (OBDA) approach is introduced based on the Sensor Observation Sample Actuator (SOSA) ontology [17], providing an interoperability layer and a domain-independent generalization of sensor measurements. SOSA ontology provides a formal but lightweight general-purpose specification for modeling interaction of entities in the acts of observation, actuation, and sampling.

To achieve adaptive path-planning and self-management, unmanned underwater assets use, as critical source, the exchanged internal and external data between various

platforms in a UWSN. Hence its robustness, from a cybersecurity aspect, is critical. Threat modeling and risk analysis are key factors in order to identify the security requirements of UUVs, as well as to define how adversaries act and achieve their objectives. In related work [23], a holistic approach is proposed, initialized with the identification of threats and vulnerabilities of software and hardware assets that a platform comprises. This process is mandatory in order to prioritize the existing numerous possible attacks. Also, due to the complexity of modern cyber-attacks, authors suggest dividing them into connected sequences of smaller attacks, encounter them as separate vulnerabilities. Considering the impact of contemporary sophisticated attacks, they conclude in the necessity of developing fault tolerant and redundant systems in order to survive and counter multiple intrusions.

The successful accomplishment of a task is most often depending on a key factor i.e., its prediction. Simulation tools provide the capability to evaluate a situation and decide following actions quickly and accurately across several domains. In the following paragraphs we present a set of open-source underwater simulation tools, which were chosen with specific requirements in mind: a) capability of heterogenous data integration using ontologies/semantic knowledge, b) support of multiple UUVs (swarms) simulation, c) support of modeling and simulation of sensors and network interfaces, and d) support of simple visualization for realistic scenario representation.

NS-3 (Network Simulator) [29] is a well-known open-source tool that has been used to represent underwater or other types of networks, especially due to its capability to be combined with external software libraries, animators, analysis and visualization tools, in contrast to other simulation tools that provide a single integrated graphical user interface (GUI). It has been developed to support basic networking research and education by providing configuration with numerous Internet protocols. It is compatible to Linux and Windows operating systems. Nevertheless, its operation mainly through command line and C++, may be a barrier for users without coding skills [30].

UWSim is a tool used by researchers for underwater robotic missions' simulation, highly suitable for UWSNs [33]. Users are able to configure their working environment, even with widgets, displaying useful data during an operation. Import of XML data is also possible. A Robot operating system (ROS) can be effectively integrated also via a dedicated interface. Its main advantage is an easily integrated open-source extension, namely UWSim-NET; a network simulator, which gathers the benefits of NS-3 in modeling communication [8]. Finally, playback of the same mission is also available, facilitating the acquired results in a great extent.

Motivated by the need of fast and agile decision-making, and with the aim of integrating and dynamically representing knowledge from existing knowledge bases, related work [18] presents a hybrid ontology-based simulation framework for efficiently deriving a simulation model from a knowledge base. By converting use case ontologies into instances in their simulation ontology, using a suitable parser, this related work manages to overcome the time-restriction issue of simulations, even in complex and dynamic environments, also considering the uncertainty of information.

A number of other related processes should be performed by simulation tools. For example, in related work [5], in order to limit energy consumption during data trans-

mission in UWSNs, an Edge-Drone-based software-defined smart IoUT network is proposed and compared to existing approaches, using QualNet simulator. The energy restrictions of underwater sensors, in combination with the continuous process of data analysis, have serious impact in the network. Utilizing this tool, authors managed to perform accurate measurements, and extract useful conclusions for factors such as the packet delivery ratio.

Another active stand-alone open-source tool, namely Gazebo [13][14], has been included in our survey. Except from its scalability, ease of installation and handling, it is suitable for integration with ROS. This feature allows us to represent swarm of UUVs in an UWSN. Our research plan includes this extension in order to be able to represent packet flows during communications, as well as their protocols and the integration of the Simultaneous Localization and Mapping (SLAM) ontology [10].

Furthermore, simulation tools in the of cybersecurity domain were also investigated. Considering the diversity of each attack strategy and the need for quick response, simplicity of operation, but also facilitation of integrating various data and knowledge from databases, we have examined Nessi2 (Network Security Simulator) [43]. This is network security simulation software providing scalability, fidelity, and extensibility. It has been used for evaluating the security of network architectures [19]. By using MySQL as its main backend database, users can insert any entity, relation or event needed.

HackIt is another tool used for building dynamic cyber-attack scenarios [1]. Providing a realistic approach to a cyber-attack, essentially it provides scanning for vulnerabilities and gaining access. Also, HackIt run various commands used by adversaries, such as *nmap* and *msfconsole,* and is suitable for representing deception method, such as honeypots and honeynets.

Moreover, an effective representation of cyber-attacks must be able to establish the necessary security protocols and confront adversaries or restore the function of the network. In related work [9], an open-source tool chain for modeling and simulating attacks, namely Power-Attack, is utilized. In order to simulate attacks in power systems, but also analyze them, this tool uses a sequence of steps, and PyPower-Dynamics, to provide an extra security layer for dynamic sophisticated attacks. Its major advantage is the fully editable source-code written entirely in Python.

Caldera is an open-source simulation tool for Linux OS, which provides users the ability to create their own adversaries and defenders, as well as their abilities [7] [27]. Thereafter, the process of attack and defend is fully automated. Because of its automated nature, reproducing the same processes is straight forward. Also, the extensibility of this tool is very useful for the cyber domain, due to the heterogeneity of strategies and methods.

Probably one of the most modern open-source penetration testing tools is the Infection Monkey [15]. It has numerous features and configurations e.g., the ability to be executed inside the user's network in order to breach it using methods, tools and strategies from remarkable sources of this domain such as the MITRE ATT&ACK [28] knowledge base. The process is fully automated and can be configured to infect another host to make it a zombie machine. Furthermore, the users can choose specific attack and defense methods, and import their files from external databases.

Finally, with the aim to implement a robotic sensing network to respond adaptively to extreme underwater environmental changes, related work [4] realizes this through a Digital Twin prototype approach. Researchers have managed to reduce cost and time factors drastically by overcoming real-life challenges, such as the replacement of underwater observation system due to software errors and the absence of vessel and crew. Thus, when an adjustment improves measurements in a Digital Twin, it sends a specific message to its Physical Twin in order to inform it, and to make the same adjustment in turn. Authors conclude that Digital Twins prototypes are suitable for simulation in underwater networks.

Although simulation tools support decision-making, the new trend lying above IoT layer is Digital Twins. This technology concerns the bidirectional management of entities and assets of a simulated environment. Tools for representing and managing Digital Twins are neither limited to simulation, nor to the representation of digital prototypes. These tools essentially replicate processes, bridging the digital with the physical information to model and predict its condition's degradation throughout system's lifecycle and performance [20][41]. Digital Twins is the future, but this topic is out of the scope of this paper.

Low-bit rate issues, due to the medium (water), have as a consequence latency in exchanging information, which, in combination with the native complexity of UWSN, emerges vulnerabilities in network architecture robustness, affecting the known CIA Triad (Confidentiality, Integrity, Availability of data). In related work [36], the Unified Cybersecurity Ontology (UCO) is presented. UCO, in order to support information integration and cyber situational awareness, maps the most commonly used cybersecurity standards. On the other hand, in Cybersecurity Vulnerability Ontology (CVO) [35], knowledge about known attacks, patterns and strategies of adversaries, as well as possible vulnerabilities exploitation, are included. In related work [35], CVO is utilized in order to develop an accurate and effective cyber intelligence alert system.

Decision-making and adaptive-planning, two main capabilities of UUVs, are depended on a key factor i.e., weather conditions. In related work [37], efforts to overcome sensor-generated Big Data restrictions, as well as to extract accurate information about weather conditions at exact locations, the Oceanographic Weather Ontology (OWO) is proposed, supporting data integration in a single platform for analysis, information retrieval, and decision making. The experimental results with the proposed weather data model, data processing, ontology creation, and a query engine, prove the overall importance of the OWO.

3 Experiments and Proposed Approach

Threat modeling automation, distributed simulation, and integration of ontologies in various domains, are necessary to approach the presented problem. The main reason is the heterogeneity and complexity of the UWSN and IoUT domains. So, blending various approaches, tools and methods that originate from those domains is highly promising.

Several related ontologies have been developed or are under development by our team, specifically in the related domains of IoT/IoT-trust[1], drones' semantic trajectories[2], Digital Twins[3], and cybersecurity for communication/network assets. Our aim is to integrate them with existing semantic approaches of cybersecurity and underwater domain ontologies (UCO, CVO and OWO) and utilize them in selected simulation tools. Our previous work in the representation of heterogeneous trustworthy IoT entities to facilitate their semantic data integration in other domains (smart cultural spaces) [42], will be also applied here.

Initially, in order to prove the ease/risk of a cyber-attack and its consequences, we have been experimenting with two different operating systems, a Kali Linux (host machine) as the adversary and a Windows Server 2019 (target machine) as the UUV, or the central platform on surface, or even a surface buoy which communicates with the central platform. We have developed these systems through virtualization using VMware Workstation. The experimentation involves attacker eavesdropped communications using simple tools (Wireshark [3][40]), extracted vulnerabilities, and the MITM (Man in the Middle) performed ARP Poisoning [39]; a method when attacker tries to associate its IP address with the victim's. The scenario includes adversarial redirection of every command issued by the commander or the leader of a UUV in the adversarial machine. Hence, by "confusing" UUVs, and gaining administrative privileges by taking advantage of vulnerabilities, as well as extracting all necessary information from the knowledge base of the UWSN, the adversary performs a DoS (Denial of Service) attack, by overwhelming the network. Finally, the Security Operations Center (SOC) of the Central Platform imports some new security rules, in order to defend against this type of attack in the future, and implements a honeynet for early alert. Although this approach is the most effective due to the manual attacking method and strategy of the user, it requires knowledge of cyber-security domain commands and tools, and comes in conflict with the required quickness in a critical real-time situation.

Further experimentation was conducted using a semi-automated tool for attack and response, namely Caldera [20]. Process initialized by creating an adversary (agent) with the ability to scan, enumerate, and exploit our network architecture, and then we attacked a given IP address. The responder of the created incident, with its own abilities, was ready to counter these attacks with its own tools, simulating a real-time process. From exported log files we were able to conclude how vulnerable the network is. Ease of handling and configuration of this tool satisfies the need of fast and precise responses, supporting decision-making process of commanders.

Due to its advantage of importing files in XML/RDF format, facilitating the integration of semantic knowledge/ontologies, Nessi2 tool was evaluated. We have achieved the development of semantics in respect to necessary entities and relations between them, such as *attack-type*, *event-type*, etc., as well as *weather conditions* at specific *locations*. Also, we have managed to represent a logical topology of the ex-

[1]https://github.com/KotisK/IoTontos
[2]https://github.com/KotisK/onto4drone
[3]https://github.com/KotisK/SEC4DigiT

perimental scenario. Our future goal is the extension of this tool and the realization of a completed scenario.

For our last experiment, a fully automated attack and response process using Infection Monkey [21] has been utilized. The first step was the configuration of attacker machine (in Kali Linux OS). Then, we exploited two target machines (Windows Server 2019 and Ubuntu). To evaluate its functionality, we tried to infect one of the hosts, in order to manipulate it, and unleash our attacks from it. The result was to remain undetected. Finally, from the Security Reports tab, we were able to view critical vulnerabilities about our network architecture.

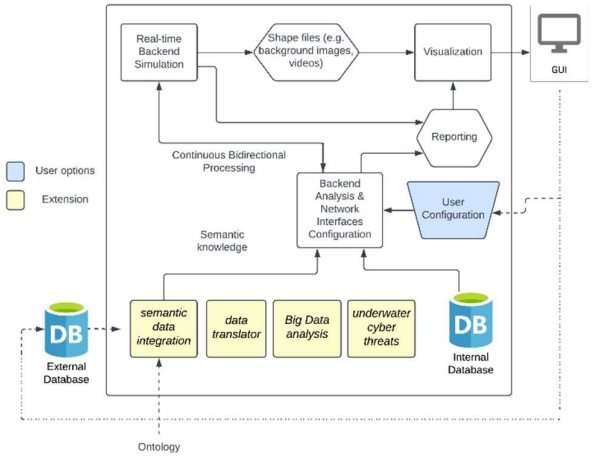

Fig. 2. General high-level architectural design of the proposed cybersecurity simulation tool.

Based on the above-mentioned experimentation and on challenges/issues related to the UWSN and IoUT domains presented in previous sections, we have concluded that it is possible to extend current functionality of existing simulation tools towards supporting the requirements specified in our preliminary work. The high-level architectural design of such an extension is briefly described below (and depicted in Figure 2):

- Initially, a primary configuration of data found in the internal database of the simulation tool (e.g., plug-ins, user environment, shape files, etc.) is taking place and representation of the initial graphical user interface is displayed. Then, numerous options of the tool can be configured (import templates, network creation, agent configuration, asset creation, etc.), depending on the scenario at hand.
- Thereafter, the Backend Analysis and Network configuration may start, continuously sharing data with the process of Backend Simulation, but also to Reporting.
- When Backend Simulation is prepared, elements from user configuration (background images, etc.) may be also imported.
- Then, Visualization process may start, exporting the graphical content to the user, combined with reporting information (network vulnerabilities, elements of time, statistics, etc.).

- Finally, the whole process can be restarted, either with the same configuration or with a new one.

In order to achieve a robust simulation using an ontological model, capable of a) translating semantic knowledge, b) analyzing huge volumes of heterogeneous data, and c) simulating specific underwater cyber-attacks, we propose the following extensions:

- A *semantic data integration* framework, providing the ability to integrate heterogeneous data in various formats,
- A *data translator framework*, which will convert semantic data in a language understandable by the simulation tool,
- A *Big Data analysis framework*, in order to analyze input data, and extract knowledge and conclusions from them, utilizing the huge amount of data in UWSNs,
- An *underwater cyber threats* framework, which will comprise libraries (tactics, strategies, threats, attacks, etc.) specifically about Internet of Underwater Things, as well as tools to simulate such attacks.

4 Discussion and Future Plans

Based on extensive research in IoUT and cybersecurity domains, we have identified the need to further investigate the key issue of interoperability, standardization, and the lack of common communication protocols. A recent representative approach for tackling this issue is the initiative to define a common language to achieve initial contact and data exchange between nodes, namely, the JANUS by NATO STO CMRE [32][34]. This is the first underwater digital communications protocol which was promulgated as a NATO standard, enabling interoperability between heterogeneous military and civilian devices. Moreover, in combination with the Software-to-Software Communications protocol [16], the challenge of a required common message encoding and decoding scheme is also delimited.

During further investigation on the topic, we have identified the lack of semantic modeling and simulation tools specifically for the underwater cybersecurity domain. It appears that the communication protocols between traditional operating systems differ from those in underwater communications. Underwater assets include electro-acoustic transducers to receive and transmit sound signals [2]. Thus, adversaries exploit the native vulnerability of water, i.e., latency, but also the inability of inspection of compromised nodes. Hence, the classification of attacks also differs. Node infection, Protocol-Oriented and Repudiation attacks or Jamming DoS are a few examples [37]. On the other hand, countermeasure methods are very similar, making the goal of our research more feasible.

Finally, as the high-level design of the proposed cybersecurity simulation tool is shown in Figure 2, our future plans include the extension of cybersecurity simulation tools described in Section 3. The selection of such tools will be based on availability of source code, license, and developer support, as well as on the requirements that

such tool meet in terms of the proposed designed architecture. Gazebo and Nessi2 are two candidates that partially cover requirements in respect to semantic modeling, cybersecurity simulation, simulation of dynamic underwater environments, simulation of swarm of UUVs in IoUT.

5 Conclusion

Although UUVs and their applications are popular in civil and military operations, the establishment of interoperability across various platforms, and the establishment of robust underwater network architectures in IoUT from a cybersecurity perspective, are key challenges. Sharing knowledge between trustworthy IoUT assets in a common machine-understandable language is the key to overcome communication issues emerging due to their heterogeneity and the volume of data they produce. The volume of data, in combination with latency issues in the medium of water, result to numerous vulnerabilities and security issues in UWSNs. Automated threat modeling, semantic knowledge representation, and simulation of the above challenges is required, in order to be able to efficiently predict the impact of fast and trustworthy decision-making in critical situations such as military and SAR ones. Towards this direction, in this paper we have presented related, proposed, and future work towards the semantic modeling and simulation of cybersecurity on the IoUT.

References

1. Aggarwal, P., Gonzalez, C., & Dutt, V. (2019). HackIt: A real-time simulation tool for studying real-world cyberattacks in the laboratory. In Handbook of Computer Networks and Cyber Security: Principles and Paradigms (pp. 949–959). Springer International Publishing. https://doi.org/10.1007/978-3-030-22277-2_39.
2. Ahmad, I., Rahman, T., Zeb, A., Khan, I., Ullah, I., Hamam, H., & Cheikhrouhou, O. (2021). Analysis of Security Attacks and Taxonomy in Underwater Wireless Sensor Networks. In Wireless Communications and Mobile Computing (Vol. 2021). Hindawi Limited. https://doi.org/10.1155/2021/1444024.
3. Bagyalakshmi, G., Rajkumar, G., Arunkumar, N., Easwaran, M., Narasimhan, K., Elamaran, V., Solarte, M., Hernandez, I., & Ramirez-Gonzalez, G. (2018). Network Vulnerability Analysis on Brain Signal/Image Databases Using Nmap and Wireshark Tools. IEEE Access, 6, 57144–57151. https://doi.org/10.1109/ACCESS.2018.2872775.
4. Barbie, A., Pech, N., Hasselbring, W., Flogel, S., Wenzhofer, F., Walter, M., Shchekinova, E., Busse, M., Turk, M., Hofbauer, M., & Sommer, S.(2021).Developing an Underwater Network of Ocean Observation Systems with Digital Twin Prototypes - A Field Report from Baltic Sea. IEEE Internet Computing. https://doi.org/10.1109/MIC.2021.3065245
5. Bhattacharjya, K., & De, D. (2021). IoUT: Modelling and simulation of Edge-Drone-based Software-Defined smart Internet of Underwater Things. Simulation Modelling Practice and Theory, 109. https://doi.org/10.1016/j.simpat.2021.102304.
6. Bouter, C., Kruiger, H., & Verhoosel, J. (2021). Domain-Independent Data Processing in an Ontology Based Data Access Environment Using the SOSA Ontology. http://ceur-ws.org.

7. Caldera Description page, https://www.pwc.co.uk/issues/imitation-game-attacker-emulation.html, last accessed 2022/03/06.
8. Centelles, D., Soriano-Asensi, A., Martí, J. V., Marín, R., & Sanz, P. J. (2019). Underwater wireless communications for cooperative robotics with UWSim-NET. Applied Sciences (Switzerland), 9(17). https://doi.org/10.3390/app9173526.
9. Chhokra, A., Barreto, C., Dubey, A., Karsai, G., & Koutsoukos, X. (n.d.). Power-Attack: A comprehensive tool-chain for modeling and simulating attacks in power systems.
10. Cornejo-Lupa MA, Cardinale Y, Ticona-Herrera R, Barrios-Aranibar D, Andrade M, Diaz-Amado J. OntoSLAM: An Ontology for Representing Location and Simultaneous Mapping Information for Autonomous Robots. Robotics. 2021; 10(4):125. https://doi.org/10.3390/robotics10040125.
11. Domingo, M. C. (2012). An overview of the internet of underwater things. *Journal of Network and Computer Applications*, *35*(6), 1879–1890. https://doi.org/10.1016/j.jnca.2012.07.012
12. Fattah, S., Gani, A., Ahmedy, I., Idris, M. Y. I., & Hashem, I. A. T. (2020). A survey on underwater wireless sensor networks: Requirements, taxonomy, recent advances, and open research challenges. *Sensors (Switzerland)*, *20*(18), 1–30. https://doi.org/10.3390/s20185393.
13. Gazebo Github page, https://github.com/osrf/gazebo, last accessed 2022/03/06.
14. Gazebo Homepage, http://gazebosim.org/, last accessed 2022/03/06.
15. Infection Monkey, https://github.com/guardicore/monkey, last accessed 2022/03/06.
16. J. Braga, R. Martins, C. Petrioli, R. Petroccia and L. Picari, "Cooperation and networking in an underwater network composed by heterogeneous assets," *OCEANS 2016 MTS/IEEE Monterey*, 2016, pp. 1-9, doi: 10.1109/OCEANS.2016.7761219.
17. Janowicz, K., Haller, A., Cox, S. J. D., le Phuoc, D., & Lefrançois, M. (2019). SOSA: A lightweight ontology for sensors, observations, samples, and actuators. Journal of Web Semantics, 56, 1–10. https://doi.org/10.1016/j.websem.2018.06.003.
18. Jurasky, W., Moder, P., Milde, M., Ehm, H., & Reinhart, G. (2021). Transformation of semantic knowledge into simulation-based decision support. Robotics and Computer-Integrated Manufacturing, 71. https://doi.org/10.1016/j.rcim.2021.102174.
19. Kamoun-Abid, F., Rekik, M., Meddeb-Makhlouf, A., &Zarai, F. (2021). Secure architecture for Cloud/Fog computing based on firewalls and controllers. Procedia Computer Science, 192, 822–833. https://doi.org/10.1016/j.procs.2021.08.085.
20. Kutzke, D. T., Carter, J. B., & Hartman, B. T. (2021). Subsystem selection for digital twin development: A case study on an unmanned underwater vehicle. Ocean Engineering, 223. https://doi.org/10.1016/j.oceaneng.2021.108629.
21. LHN Infection Monkey page, https://latesthackingnews.com/2022/02/24/__trashed-4/, last accessed 2022/03/06.
22. LinkedIn page, https://www.linkedin.com/pulse/auv-deepwater-search-rescue-arnt-helge-olsen/, last accessed 2022/03/06.
23. Madan, B. B., Banik, M., &Bein, D. (2019). Securing unmanned autonomous systems from cyber threats. Journal of Defense Modeling and Simulation, 16(2), 119–136. https://doi.org/10.1177/1548512916628335.
24. Mary, D. R. K., Ko, E., Kim, S. G., Yum, S. H., Shin, S. Y., & Park, S. H. (2021). A systematic review on recent trends, challenges, privacy and security issues of underwater internet of things. In *Sensors* (Vol. 21, Issue 24). MDPI. https://doi.org/10.3390/s21248262.
25. Menaka, D., Gauni, S., Manimegalai, C T, & Kalimuthu, K. (n.d.). Vision of IoUT: advances and future trends in optical wireless communication. *Journal of Optics*, *50*. https://doi.org/10.1007/s12596.

26. Migueláñez, E., Patrón, P., Brown, K. E., Petillot, Y. R., & Lane, D. M. (2011). Semantic knowledge-based framework to improve the situation awareness of autonomous underwater vehicles. *IEEE Transactions on Knowledge and Data Engineering*, *23*(5), 759–773. https://doi.org/10.1109/TKDE.2010.46.
27. MITRE ATT&CK Description page for Caldera, https://www.mitre.org/research/ technology-transfer/open-source-software/caldera%E2%84%A2, last accessed 2022/03/06.
28. MITRE ATT&CK Homepage, https://attack.mitre.org/, last accessed 2022/03/06.
29. Nayyar, A., & Balas, V. E. (2019). Analysis of Simulation Tools for Underwater Sensor Networks (UWSNs). In Lecture Notes in Networks and Systems (Vol. 55, pp. 165–180). Springer. https://doi.org/10.1007/978-981-13-2324-9_17.
30. NS-3 Introduction page, https://www.nsnam.org/docs/release/3.21/tutorial/ html/introduction.html, last accessed 2022/03/06.
31. Oceanic Engineering Society (U.S.). (n.d.). *Autonomous Underwater Vehicles 2016 : AUV 2016 : 6-9 November 2016, IIS, the University of Tokyo, Tokyo, Japan*.
32. Potter, John & Alves, Joao & Green, Dale & Zappa, Giovanni & McCoy, Kim & Nissen, Ivor. (2014). The JANUS underwater communications standard. 2014 Underwater Communications and Networking, UComms 2014. 10.1109/UComms.2014.7017134.
33. Prats, M., Perez, J., Fernandez, J. J., & Sanz, P. J. (2012). An open-source tool for simulation and supervision of underwater intervention missions. IEEE International Conference on Intelligent Robots and Systems, 2577–2582. https://doi.org/10.1109/IROS.2012.6385788.
34. Public Affairs Office, C. (2020). NATO STO-CMRE Science and Technology Organization Centre for Maritime Research and Experimentation.
35. Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Information and Management, 57(6). https://doi.org/10.1016/j.im.2020.103334.
36. Syed, Z., Padia, A., Finin, T., Mathews, L., & Joshi, A. (n.d.). UCO: A Unified Cybersecurity Ontology. http://tinyurl.com/ptqkzpq.
37. Velu, A., & Thangavelu, M. (2022). Ontology based ocean knowledge representation for semantic information retrieval. Computers, Materials and Continua, 70(3), 4707–4724. https://doi.org/10.32604/cmc.2022.020095.
38. Wikipedia page https://en.wikipedia.org/wiki/Air_France_Flight_447#Underwater_search, last accessed 2022/03/06.
39. Wikipedia page for ARP spoofing, https://en.wikipedia.org/wiki/ARP_spoofing, last accessed 2022/03/06.
40. Wireshark Home page, https://www.wireshark.org/docs/, last accessed 2022/03/06.
41. Wu, J., Yang, Y., Cheng, X. U. N., Zuo, H., & Cheng, Z. (2020). The Development of Digital Twin Technology Review. Proceedings - 2020 Chinese Automation Congress, CAC 2020, 4901–4906. https://doi.org/10.1109/CAC51589.2020.9327756.
42. Zachila K, Kotis K, Paparidis E, Ladikou S, Spiliotopoulos D. Facilitating Semantic Interoperability of Trustworthy IoT Entities in Cultural Spaces: The Smart Museum Ontology. IoT. 2021; 2(4):741-760. https://doi.org/10.3390/iot2040037.
43. Zhao, Y., Wang, Y., Zhang, H., Zhang, C., & Yang, C. (2015). Agent-based Network Security Simulator Nessi2.