Semantic Modeling, Simulation and Cybersecurity in the IoUT

Subjects: Computer Science, Information Systems | Engineering, Marine
Contributor: Konstantinos Kotis, Stavros Stavrinos, Christos Kalloniatis

As maritime and military missions become more and more complex and multi-factorial over the years, there has been a high interest in the research and development of (autonomous) unmanned underwater vehicles (UUVs). Latest efforts concern the modeling and simulation of UUVs' collaboration in swarm formations, towards obtaining deeper insights related to the critical issues of cybersecurity and interoperability. The research topics, which are constantly emerging in this domain, are closely related to the communication, interoperability, and secure operation of UUVs, as well as to the volume, velocity, variety, and veracity of data transmitted in low bit-rate due to the medium, i.e., the water.

Keywords: IoUT ; UUVs ; swarm ; interoperability ; semantics ; cybersecurity ; simulation

1. Introduction

Technology for maritime and military missions nowadays is demonstrating rapid development in different directions such as high-distance tracking radar, the integration of heterogeneous systems for improving operational time and cooperation with air and sea. Costly, uncertain, and dangerous operations such as search-and-rescue (SAR) or hydrography and ocean floor mapping, are now performed in few hours instead of days/months, in a cost-efficient manner, minimizing human involvement. On the other hand, assigning highly risky (and usually deadly) missions to humans, raises ethical concerns since prioritization and importance of human lives is undeniable. In addition, the cost of such operations is enormous, mainly due to the energy and fuel consumption of involved systems/platforms. Planning such operations must seriously consider the cost-efficiency factor, especially when combined with time and cost needed to repair damaged air, surface, or subsurface vehicles. A key solution for this challenge is the use of autonomous and unmanned vehicles, which are self-managing, cost-efficient, and effective in accomplishing several highly risky and resource-demanding tasks. As a result, unmanned vehicle systems/platforms below and above the water, and in the air, have become a priority of military and non-military industries.

In the last decade, the interest in unmanned underwater vehicles has been increasing. The North Atlantic Treaty Organization (NATO), in collaboration with academia, have developed distinct sectors for exclusive research related to this topic. Unmanned or autonomous underwater vehicles (UUVs/AUVs), namely drones, and remotely operated vehicles (ROVs), have been developed for years. There are several differences between them, with the most fundamental being the human factor. UUVs/AUVs demonstrate some form of intelligence, planning their own path, without exclusively depending on humans, acting completely autonomously most of the time. ROVs, on the other hand, depend on a remote human operator, and, as a result, many restrictions in their usage are emerging. Both UUVs/AUVs and ROVs, usually operate in an underwater wireless sensor network (UWSN). This type of network supports the monitoring of the aquatic environment and the wireless bidirectional transmission of data between users, i.e., underwater vehicles.

UUVs/AUVs are considered today a powerful scientific and military "tool" which, when operating in swarm formations, achieve tremendous goals. A swarm of UUVs concerns multiple UUVs that can interoperate, communicate, and behave as a unit. Ideally, one of the UUVs is the leader, having the main decision-making role. Several sub-groups with leaders could also exist. Every unit in the swarm should have the permission and ability to take leadership in situations where the leader is unable to operate efficiently (for any reason, e.g., circuits' damage). The operation of UUVs in a swarm is a powerful platform that provides huge capabilities towards a successful operation (military, scientific, other), even in risky and hazardous settings, putting aside any ethical doubts of a human (e.g., military commander, chief scientist), especially when the full-autonomous decision-making loop for the leader is achieved. Semantic knowledge and ontologies are key solutions to achieve successful interoperability in a swarm of UUVs, ensuring all the above requirements. Whatever the mission/operation, UUVs/AUVs can support it efficiently, either in civilian or in naval SAR and military operations. For example, the AUV A18D of ECA GROUP (https://www.ecagroup.com/en/solutions/a18-d-auv-autonomous-underwater-

vehicle, accessed on 20 November 2022) achieved the precise mapping of the seabed at a depth of 3000 m in the strong currents of Atlantic; it also efficiently detected various debris and wrecks [1]. Furthermore, AUVs supported a huge operation surrounding a plane crash (Air France Flight 447), discovering pieces of the plane and its “black box” with side-scan sonar [2]. Finally, Knifefish of the US Navy fleet can detect and classify mines in large depths of the underwater environment with high clutter [3]. NATO is integrating UUVs in their fleet gradually, trying to counter several challenges.

2. UUVs and Swarms

UUVs are decision-making mechatronic systems, which could expand people’s underwater activities in the marine engineering construction, underwater search-and-rescue, or ocean ranch operations [4]. They are powerful assets that can operate in underwater missions and operations autonomously and are capable of situation and environment awareness, making their own autonomous decisions, and planning their own trajectories. Moreover, they interoperate with other underwater, surface, and air vehicles or platforms. A UUV can be considered as a knowledge-based autonomous agent [5]. Furthermore, it has the ability of self-management, i.e., self-configuration, self-healing, self-optimization, and self-protection. An interesting, related work reporting on enhancing self-diagnosis and self-adaptation of UUVs, through a “metacontrol” framework with the implementation of ontological reasoning, has been recently published [5]. In the work of UX-1 in the UNEXMIN project (a robot developed to survey flooded old mine sites) [6], the authors were motivated by the lack of real-time communication, proposing a framework to enhance its ability for self-diagnosis and self-adaptation. To interconnect these valuable assets and achieve an efficient exchange of information, localization is mandatory. This capability allows a vehicle to determine its position and orientation in the world, both underwater and at the surface.

Localization ability of UUVs and underwater assets, is more than meaningful in creating vigorous network architectures, due to the facilitation of information sharing. However, this need generates new challenges to overcome. As has been seen in related work [7], there are different localization algorithms that can be applied to a UWSN and are divided in two broad categories, i.e., range-based and range-free schemes. The first category is based on accurate distance and angle measurements, by using different variables such as Time of Arrival (ToA), Angle of Arrival (AoA), etc. While this method is very precise in estimating an asset’s position, it relies on strict time synchronization for the exact information transmission and receiving instances. The second one does not use range or bearing information, relying on simplicity, but enhancing the localization error of nodes; this schema is useful for terrestrial sensor networks.

The technological progress of UUVs is required, towards an efficient operation in the marine environment. They are used to mitigate the risk to human lives and decrease the cost of operations. The need for smart and durable UUVs increases as the maritime operations become more complex and riskier, for instance, supporting the installation of oil and gas facilities or settling underwater cables in depths that were previously unexplored. In addition, in the context of military operations in an Internet of Underwater Things (IoUT) environment, a team of UUVs, each having an individual role and being interconnected, is participating in search-and-rescue operations (SAR) or in mine deactivation operations in Anti-Submarine Warfare [8][9]. Moreover, the interoperability of the UUVs is an issue of consideration when planning an operation, especially when they operate in a swarm formation. A swarm system of independent assets is a group of self-organizing autonomous agents aiming at the effective accomplishment of various collaborative tasks [10].

3. Swarm Simulation

In IoUT, the safe and secure movement of an underwater vehicle is a key issue. Especially in a swarm of UUVs, where efficient cooperation between agents is a challenging goal, the difficulties that emerge are tremendous, such as the secure movement and interoperability, as well as the secure communications between them. It is well known that science often tries to copy nature, thus, from the observation of flocks of birds, UUV/UAV technology has been developed [11]. The limitations and constraints of moving from nature to science are many, nevertheless significant advancements towards the development of autonomous UUVs operating in a swarm have been already accomplished. The Science Department of the Universita degli Studi Roma Tre proposed a new type of autonomous underwater vehicles (AUVs) swarm and simulated its operation in a diffused environment. They have developed an AUV with specific characteristics, without emphasis on robustness, with auxiliary systems such as a camera for taking pictures and classifying fishes or recognizing contamination. They have simulated a swarm of 25 AUVs, studying their movement, interconnection, and performance of their systems, using Matlab/Simulink tool [11]. Having neither a central platform to send further instructions for the operation nor a “leader” vehicle, the results obtained were satisfactory. The Naval University of Engineering in China, similarly using Matlab, a dataset from GEBCO (General Bathymetric Chart of the Oceans) for coordination, a grid system, and a fusion algorithm based on PSO (particle swarm optimization) and ACO (ant colony optimization) named PACO, proposed an approach for autonomous UAV path planning, verifying the effectiveness of their approach [12].

4. Internet of Underwater Things (IoUT)

Nowadays, technological innovations allow millions of devices to connect to the global network. This industrial revolution was described by the term IoT (Internet of Things) and was led by the need of users to be constantly connected to their devices to conduct daily activities [13]. The IoT supports a 'smarter' way of living, assisting daily tasks and our well-being, such as home automation. Regarding the underwater (sea) "world", there were various daily tasks which could be facilitated, and numerous devices of underwater vehicles needed to interoperate in an underwater sensor network (UWSN) or underwater wireless communication network (UWCN) [14]. Sea species tracking, maritime security and naval military activities and gas/oil extraction are some of these activities. The IoUT has been introduced, not necessarily to simplify such tasks, but to support the efficient interconnection of underwater vehicles, devices, and sensors to the Cloud. The IoUT has brought new research and development directions in a new ecosystem which facilitates the connection of assets "living" underwater and on the sea surface. It aims to tackle several challenges of UUVs such as interoperability, data management, and secure communications, contributing to the development of research, business and underwater military or civil operations [14]. In such an ecosystem, there is a need to establish a fault tolerance connection between underwater and surface assets, meeting key requirements such as heterogeneity, network coverage, low latency, low power usage or battery efficiency, and cyber-attacks. The IoUT must integrate heterogeneous assets, to be able to interoperate effectively in UWCNs and UWSNs. Specifically, a UWSN has its own requirements (longevity, accessibility, complexity, security, and environmental sustainability), and the need for a taxonomy based on specific key attributes, such as architectural elements, communication, routing protocol, security, and applications [15]. The establishment of a robust and secure underwater ecosystem is a continuous process as the threats to be countered are becoming more and more sophisticated.

IoUT has certain similarities to IoT such as its structure, function, and its energy limitation. However, a few differences exist, which are related mainly to the heterogeneity of assets in terms of their: (a) communication technologies, (b) tracking technologies, (c) low battery capacity and difficulty of recharge, (d) energy harvesting technologies, (e) network density, (f) localization techniques [16]. Therefore, as mentioned in [17], in order to successfully establish a UWCN/UWSN, and obtain IoUT capabilities, at least the following issues must be considered: (a) the communication medium, i.e., the water, (b) the dynamic changes of network topology, (c) the energy consumption and maintenance constraints, (d) the hazardous environment and physical security, and (e) localization [17].

Limited bandwidth, transmission media (acoustic communication) and low propagation speed of IoUT, in combination with the volume of data to be transmitted, as in IoT, lead to delays in information distribution. This fact allows cyber-adversaries to remain further undetected and achieve their goal efficiently. More specifically, slow transmission rates has consequences of the delayed evaluation of an alert and the delayed reaction to a cyber-attack. A way to deal with limited bandwidth and delay in underwater communications and environmental and ambient noise [18] on a communications channel, is the development of data analysis software to optimize the process. Such a method is proposed in [19], to balance data traffic loading in an underwater network and minimize latency issues. This is conducted by presenting intelligent data analytics (IDA), which support high packet allocation in combination with low latency and less energy consumption. Another way to support data gathering and overcome bit-rate issues is the creation of distinct communication channels in underwater sensor networks, such as UWSN [15]. Similarly, implementing an information-centric model facilitates the solution to this challenge. Therefore, in [20] a depth-based caching mechanism is recommended, in order to balance latency issues and exchange of unnecessary information, indicating that the creation of hybrid communication models is very important to overcome the physical phenomena of the water and further develop IoUT.

Fifth generation (5G) and the upcoming sixth generation (6G) connectivity networks are making essential improvements already to the interconnection of IoUT assets, facilitating their communication and exchange of data with tremendous speeds (>1 Gbps) on a large number of devices. In related work [14], the optical wireless communication (OWC) is proposed with the aim to improve underwater wireless communication, concluding that OWC with RF technology can solve big issues in the underwater domain, such as the efficient management of big data, with high bandwidth, low latency, high protection, and low fuel usage.

5. Semantic Modeling in IoUT

Semantic modeling concerns the conceptual modeling of domain knowledge in order to describe structured data (with formal semantics/metadata) in a specific logical way. Ontologies are formal vocabularies of concepts and relations, used for the semantic modeling and integration of heterogeneous data. An ontology is defined as the formal and explicit specification of conceptualizations which are used to assist programs and humans to share knowledge, describing entities

and relationships among them [21]. Ontologies are versatile tools that provide the means for machines to understand the meaning of terms provided in natural language. They should be reusable in terms of their concepts, axioms, instances, and relationships. Furthermore, according to the NeOn (networked ontologies) [22] methodology, ontologies should offer interoperability, modularity, and extensibility. Formal ontology employs machine-readable languages such as the Resource Description Framework Schema or the Web Ontology Language (RDFS/OWL), in combination with other semantic tools such as query engines, knowledge management tools, and automated reasoners. Semantic reasoning is the ability of a machine to infer logical consequences from a set of asserted facts [23]. Ontologies can improve the interoperability of IoUT assets.

A hybrid approach of context reasoning for underwater robots is proposed in [24], to cover the uncertainties of underwater environments. With the aim to expand the collaboration and cooperation of UUVs/AUVs, as well as the context-awareness concept, an ontological, rule-based, and multi-entity Bayesian network (MEBN) reasoning method is proposed. This framework is proposed to support the SWARM project and SWARM ontology [25], presenting a complete approach to context management and modeling of heterogeneous contexts using ontologies for underwater robots. Information fusion and reasoning techniques improve standardization, and provide a joint scheme of understandable information exchange, supporting cyber and trajectory situational awareness. Situational awareness (SA), which is a necessary condition for UUVs to be able to interoperate and to move safely, is represented in the ontology [26]. To achieve an autonomous decision-making loop for the “leader” of a swarm, it is critical that data can be handled effectively across various platforms and domains, and should be able to be reviewed, stored, accessed and shared efficiently. Almost as important as the mission and path planning is the adaptability of the mission and the recovery from failures [27]. The issue emerges when different protocols of communication are used, and due to the lack of standardization, interoperability is much more difficult to achieve. Semantic modeling of common communication protocols represented as ontologies is required to accomplish semantic interoperability between IoUT assets. It enables autonomous vehicles to understand the environmental situation, integrate new technologies by identifying them almost dynamically, perceive the reason of its actions and the purpose of its existence, and create the desirable autonomous decision-making loop.

6. Interoperability in IoUT

The Institute of Electrical and Electronics Engineers (IEEE) defines interoperability as “the ability of two or more systems or components to exchange information and use the information exchanged” [28]. As depicted in **Figure 1**, interoperability expands in six layers, based on the capability of interoperation between systems [29][30]. Herein, researchers focus on the first three layers, namely technical, syntactic, and semantic, in which network/connectivity and simulation/implementation are achieved. In UWSNs, where interoperability is inextricably linked to communication and achieved by the transmission of acoustic and electromagnetic signals, water as a medium is an important deterrent. With the aim to overcome the principal issue of IoUT, i.e., interoperability, the authors in [31] propose the SUNRISE model, which implements an abstraction layer for supporting the interconnection of various control software of different underwater vehicles. Motivated by the first initiative to define a common language, which is JANUS from NATO Science and Technology Organization—Centre for Maritime Research and Experimentation (STO CMRE) [8][9], and its being limited to initial contact and emergency message exchange, the authors created possibilities for a heterogeneous network of mobile assets. Encoding and decoding of messages is mandatory, even if a common physical coding scheme exists; any interaction between underwater assets using different control software isn’t possible. Therefore, a protocol named SSC (Software-to-Software) is proposed, supporting the cooperation of heterogeneous platforms, e.g., MOOS (https://oceanai.mit.edu/moos-ivp/pmwiki/pmwiki.php?n=Main.HomePage, accessed on 20 November 2022), ROS (https://www.ros.org/, accessed on 20 November 2022), DUNE (https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2350792?locale-attribute=en, accessed on 20 November 2022), etc. SSC provides simplicity, ease of implementation, extensibility, and expressiveness. However, the automated integration of an autonomous vehicle in a network of a swarm of UUVs/AUVs remains a challenging goal.

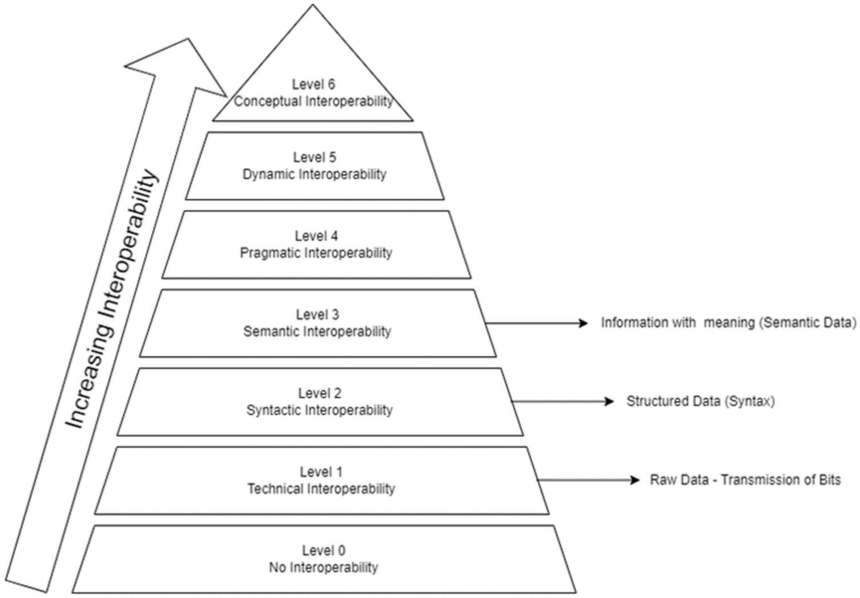

Figure 1. Levels of Interoperability.

7. Cybersecurity in IoUT

Nowadays, the term “communication” is implicitly linked to security. The technological advancements that are taking place every day in numerous domains, such as industrial IoT, digital twins, 3D printing, quantum computing, security blockchain, etc., have exponential growth. Upcoming trends such as 5G, IoT connectivity, Cloud computing, etc., are becoming part of our daily life. However, the major issue of this rapid technological development is the difficulty, in most cases, to follow along [32]. The tremendous development of information and communication technologies (ICTs) and automation of most processes in our daily life, improve mobility by offering a variety of services to a vast number of users [33]. However, vulnerabilities are raised even more, impacting users directly from the security perspective. The principal issue concerns non-awareness of the power of constantly emerging trends and the fact that users cannot perceive their function. Undoubtedly, the weakest link in defense against cyber-attacks is the human being [34]. Internet of Things (IoT) in combination with 5G can connect huge number of devices with huge speeds, but the majority are not aware of the potential threats this facilitation seeks. This increases the number of potential access points for cyber-criminals [35], and a great example is the era of COVID-19, in which remote work constantly raised extreme risks. From free-access hot-spots to personal devices, adversaries can find a path to exploit them and extract our personal data; in fact, according to the UK National Cyber Security Centre, in the first quarter of 2021, there were three times as many ransomware attacks as in the whole of 2019 [35].

Numerous security issues and vulnerabilities are emerging regularly, in networks across all domains. Unfamiliarity with technology, is one of numerous and various reasons security systems fail to detect and defend against sophisticated attacks. Statistics from IBM’s Cost of a Data Breach Report 2021 [36] indicate that the average cost of a data breach increased by 1.07 million USD in 2021. Furthermore, according to ENISA’s (European Network and Information Security Agency) Threat Landscape 2021 [37], DDoS attacks, a denial-of-service attack that malfunctions a network, have shown an upward tendency the last two years. Additionally, an infamous (in the cybersecurity community) virus named Emotet botnet, one of the longest-running and most widespread malware threats which is spread through spam emails, dealt a major blow, due to its enormous impact, especially in Windows administration and control servers [36]. Adversaries from “script kiddies” to the experienced can perform devastating attacks; most of these attacks concern networks and communication protocols between the host and the server. However, innovative tools can utilize new technologies to counter cybercrime. AI-powered cybersecurity for example, can predict vulnerabilities and identify suspect patterns, to alert incident responders for possible attacks. Thus, an interesting project, known as AIDA [38], utilizes artificial intelligence (AI) combined with machine learning (ML), in order to establish effective data analytics. Consequently, by developing big data analysis and an analytics framework equipped with automated data mining to deal with information extraction and knowledge management, they contribute to counter cyber-crime. The project is expected to be completed by the third quarter of 2022. Vulnerabilities and cyber threats exist across all domains, and it is undoubtedly irrational to deny their existence as well in the domain of IoUT. To ensure the security of the underwater domain, robust security systems equipped with effective frameworks and semantic knowledge are a recommended solution, offering suitable methods for “uncharted” behavior; the main issue of the cybersecurity domain [39].

Attack methodologies and tools are becoming more and more sophisticated, generating the need for determination of the specific steps of an attack. Cyber-attacks are divided in two broad categories: (a) active and (b) passive. The typical cycle of a cyber-attack has the following order: (a) reconnaissance (physical/social and Web/host), (b) scanning and enumeration, (c) gaining access (exploitation), (d) maintaining access, and (e) covering tracks. As a cyber-attack defender or cyber-attack analyst, the first two steps are the most crucial to prevent an attacker from enumerating and exploiting a network. Furthermore, accuracy in data recording and their analysis, have become challenging goals, mainly due to the data visibility challenges, which concerns the degree of ease by which data can be monitored and analyzed from numerous sources. It is very important to mention that almost every security mechanism an enterprise employs affects data visibility negatively. For example, the use of HTTPS (Hypertext Transfer Protocol Secure) protocol, which provides end-to-end secure connectivity, does not allow a security analyst to monitor data traffic. Nevertheless, several standards have been developed to tackle this issue, such as chain of custody (ISO standard 22095, https://www.iso.org/standard/72532.html, accessed on 20 November 2022), concerns “the chronological documentation that records the sequence of custody, control, transfer, analysis and disposition of materials, including physical or electronic evidence”, supporting the traceability of data.

The use of digital systems is now essential for civil/military maritime activity. The use of digitalization to help the automation of tasks without human interaction, in combination with the cooperation of a swarm of underwater assets, increases complexity in early detection of attacks, results in various weaknesses [40] and raises vulnerabilities in an exponential manner. Furthermore, security assurance, which is defined as: “the degree of confidence that the security requirements of an IT system are satisfied” [41] is not ensured. Threat assessment, risk analysis and modeling techniques enable IT systems to map security, privacy, and safety requirements, to specific counter measures [41]. Numerous standardized methods for industrial cyber risk assessment exist, with the most remarkable being the Formal Safety Assessment (FSA) and Cyber Preliminary Hazard Analysis (CPHA). The first one concerns “a structured and systematic methodology, aimed at enhancing maritime safety including protection of life, health, the marine environment and property, by using risk analysis and cost-benefit assessment” [42]. On the other hand, CPHA [43] requires several steps to establish a Security Risk Assessment and document all possible hazardous scenarios [43].

It is a fact, that most of the attacks carried out on the surface are undoubtedly achieved in the underwater domain also. In IoUT, which incorporates various special characteristics, the risk of a cyber-attack or exposure of sensitive information is increased, and the attack surface is expanded, namely the aggregation of vulnerabilities of a system. Due to the dynamic environment of IoUT, where uncertainty, heterogeneity, and big data generate potential vulnerabilities, there is an extremely high demand to establish real-time cybersecurity assessment. Moreover, slow bit-rate issues make the rapid alert evaluation unfeasible. Numerous methods are appropriate in achieving confidentiality, integrity, and availability in underwater communications, nevertheless, the priority should be the consolidation of security requirements considering the various components of this domain, the diversity of communication protocols and physical phenomena of water. Several cybersecurity frameworks have been developed to support and automate the process of protection from cyber adversaries and reduce cybersecurity risk. This process usually comprises standard steps such as detect, respond and recover. An example of the implementation of such a framework (National Institute of Standards and Technology—NIST framework, https://www.nist.gov/cyberframework, accessed on 20 November 2022) in UUVs’ functions is depicted in **Figure 2**.

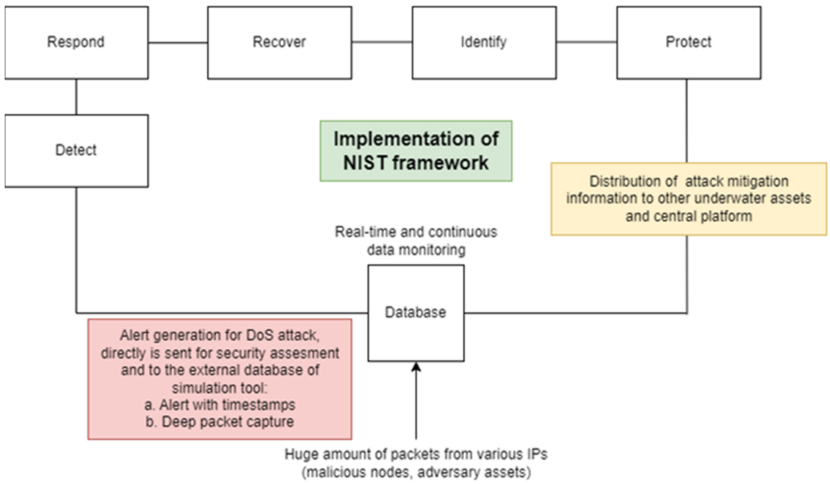

Figure 2. Implementation of NIST cybersecurity framework during a DoS attack.

Typically, the sequence is attack–defense–attack, and the attacker is ahead of security and intrusion detection systems (IDS). The most remarkable security challenges in IoUT are (a) node compromise, (b) routing attacks, (c) denial of service attacks [17]. However, network sniffing [44], a method of reconnaissance which is described as capturing passively information about a network environment, is the origin of every disastrous cyber-attack. Being impactful especially for military operations due to the high need of confidentiality for sensitive information, this method is achieved by eavesdropping (sniffing) traffic of packets, when transmitting data over a wired or wireless network. Subsequently, regarding the underwater domain, adversaries can potentially reveal critical information about the location of an underwater asset or a surface platform. A devastating attack, which can be executed despite the presence of protection mechanisms, such as multi-factor authentication and strong encryption algorithms [17], is the denial of service (DoS) Attack and distributed denial of service (DDoS) attack; a network layer (Layer 3 of the OSI—Open Systems Interconnection model) attack, but also in the application layer (Layer 7 of the OSI model). The attacker floods the network with huge amounts of queries, forcing devices to consume resources, preventing regular traffic from reaching its destination. In a complex and hazardous environment such as the IoUT, in which interoperability between heterogeneous assets is critical, a DoS attack could cause tremendous results. Consequently, a swarm of UUVs would be unable to receive information from the central platform or redistribute proper information to the rest of the units, affecting their adaptive decision-making and path-planning capabilities. Moreover, in [45], a very common and effective physical layer attack, known as jamming, is described in detail. The aim of this attack is the disruption of communication channels between hosts, in underwater domain nodes, or between other underwater assets. Additionally, due to dependence from the energy factor in IoUT, jammers are becoming even more dangerous. Their ability to reduce the lifetime of nodes by forcing them to unnecessarily transmit packets of traffic continuously, causing congestion and latency, allow attackers to achieve their goal efficiently. By simulating jamming in a realistic channel and considering that the jammer has a limited lifetime and the same characteristics as a friendly node, researchers conclude that this attack is nearly always successful.

References

1. Eca Group. News & Stories. Available online: https://www.ecagroup.com/en/news-stories (accessed on 3 October 2022).
2. France, B. Interim Report n°3 on the Accident on 1st June 2009 to the Airbus A330-203 Registered F-GZCP Operated by Air France Flight AF 447 Rio de Janeiro—Paris; BEA Bureau of Enquiry and Analysis for Civil Aviation Safety: Le Bourget, France, 2011.
3. Armed and Intelligent—Global Defence Technology. Issue 91. 2018. Available online: https://defence.nridigital.com/global_defence_technology_sep18/issue_91 (accessed on 4 October 2022).
4. Liu, F.; Tang, H.; Qin, Y.; Duan, C.; Luo, J.; Pu, H. Review on Fault Diagnosis of Unmanned Underwater Vehicles. Ocean. Eng. 2022, 243, 110290.
5. Hernandez Corbato, C.; Milosevic, Z.; Olivares, C.; Rodriguez, G.; Rossi, C. Meta-control and self-awareness for the UX-1 autonomous underwater robot. In Advances in Intelligent Systems and Computing; Springer: Berlin/Heidelberg, Germany, 2020; Volume 1092, pp. 404–415.
6. The UX-1 Robot. Available online: https://www.unexmin.eu/the-project/the-ux-1-robot (accessed on 4 October 2022).
7. Chandrasekhar, V.; Seah, W.K.; Choo, Y.S.; Ee, V. Localization in underwater sensor networks-survey and challenges. In Proceedings of the 1st Workshop on Underwater Networks, WUWNET 2006, Los Angeles, CA, USA, 25 September 2007.
8. Costanzi, R.; Fenucci, D.; Manzari, V.; Micheli, M.; Morlando, L.; Natale, D.; Stifani, M.; Tesei, A.; Caiti, A. At-Sea NATO Operational Experimentation with Interoperable Underwater Assets Using Different Robotic Middlewares; IOS Press: Amsterdam, The Netherlands, 2018.
9. CMRE_AR_2021M. Available online: https://www.cmre.nato.int/research/publications/other-publications/1653-cmre-ar-2021m (accessed on 20 November 2022).
10. Yan, Z.; Wu, Y.; Du, X.; Li, J. Limited Communication Consensus Control of Leader-Following Multi-UUVs in a Swarm System under Multi-Independent Switching Topologies and Time Delay. IEEE Access 2018, 6, 33183–33200.
11. Petritoli, E.; Cagnetti, M.; Leccese, F. Simulation of Autonomous Underwater Vehicles (AUVs) Swarm Diffusion. Sensors 2020, 20, 4950.
12. Hu, Z.; Wang, Z.; Yin, Y. Research on 3D global path planning technology for UUV based on fusion algorithm. J. Phys. Conf. Ser. 2021, 1871, 012128.
13. Gazis, A. What Is IoT? The Internet of Things Explained. Acad. Lett. 2021, 1003, 1–8.

14. Menaka, D.; Gauni, S.; Manimegalai, C.T.; Kalimuthu, K. Vision of IoUT: Advances and Future Trends in Optical Wireless Communication. J. Opt. 2020, 49, 494–509.
15. Fattah, S.; Gani, A.; Ahmedy, I.; Idris, M.Y.I.; Hashem, I.A.T. A Survey on Underwater Wireless Sensor Networks: Requirements, Taxonomy, Recent Advances, and Open Research Challenges. Sensors 2020, 20, 5393.
16. Domingo, M.C. An Overview of the Internet of Underwater Things. J. Netw. Comput. Appl. 2012, 35, 1879–1890.
17. Yisa, A.G.; Dargahi, T.; Belguith, S.; Hammoudeh, M. Security Challenges of Internet of Underwater Things: A Systematic Literature Review. Trans. Emerg. Telecommun. Technol. 2021, 32, e4203.
18. Mary, D.R.K.; Ko, E.; Kim, S.G.; Yum, S.H.; Shin, S.Y.; Park, S.H. A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things. Sensors 2021, 21, 8262.
19. Arul, R.; Alroobaea, R.; Mechti, S.; Rubaiee, S.; Andejany, M.; Tariq, U.; Iftikhar, S. Intelligent Data Analytics in Energy Optimization for the Internet of Underwater Things. Soft Comput. 2021, 25, 12507–12519.
20. Li, J.; Wu, J.; Li, C.; Yang, W.; Bashir, A.K.; Li, J.; Al-Otaibi, Y.D. Information-Centric Wireless Sensor Networking Scheme with Water-Depth-Awareness Content Caching for Underwater IoT. IEEE Internet Things J. 2022, 9, 858–867.
21. Allen, R.B. Definitions and Semantic Simulations Based on Object-Oriented Analysis and Modeling. arXiv 2019, arXiv:1912.13186.
22. (PDF) NeOn Methodology for Building Ontology Networks: A Scenario-Based Methodology. Available online: https://www.researchgate.net/publication/49911337_NeOn_Methodology_for_Building_Ontology_Networks_a_Scenario-based_Methodology (accessed on 4 October 2022).
23. Wikipedia Semantic Reasoner. 2015. Available online: https://en.wikipedia.org/wiki/Semantic_reasoner (accessed on 20 November 2022).
24. Li, X.; Martínez, J.F.; Rubio, G. Towards a Hybrid Approach to Context Reasoning for Underwater Robots. Appl. Sci. 2017, 7, 183.
25. European Commission. Smart and Networking UnderWAter Robots in Cooperation Meshes. SWARMs Project. Fact Sheet. H2020. CORDIS. Available online: https://cordis.europa.eu/project/id/662107 (accessed on 4 October 2022).
26. Liu, X.; Wang, J.; Li, W. A Formal Definition on Ontology Integration. IET Conf. Publ. 2012, 2012, 66–68.
27. Lane, D.; Brown, K.; Petillot, Y.; Miguelanez, E.; Patron, P. An Ontology-Based Approach to Fault Tolerant Mission Execution for Autonomous Platforms. Mar. Robot. Auton. 2013, 9781461456599, 225–255.
28. Std 610.12-1990(R2002); IEEE Standard Glossary of Software Engineering Terminology. The Institute of Electrical and Electronics Engineers: New York, NY, USA, 1990; pp. 1–88.
29. Wang, W.; Tolk, A.; Wang, W. The levels of conceptual interoperability model: Applying systems engineering principles to M&S. In Proceedings of the 2009 Spring Simulation Multiconference, San Diego, CA, USA, 22 March 2009.
30. Kotis, K.I.; Pliatsios, A.; Goumopoulos, C.; Kotis, K. A Review on IoT Frameworks Supporting Multi-Level Interoperability-The Semantic Social Network of Things Framework. Int. J. Adv. Internet Technol. 2020, 13, 46–64.
31. Braga, J.; Martins, R.; Petrioli, C.; Petroccia, R.; Picari, L. Cooperation and networking in an underwater network composed by heterogeneous assets. In Proceedings of the OCEANS 2016 MTS/IEEE Monterey, OCE 2016, Monterey, CA, USA, 19–23 September 2016; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2016.
32. LinkedIn. Top Trending Technology Domains of the Decade. Available online: https://www.linkedin.com/pulse/top-trending-technology-domains-decade-vignesh-pillai/ (accessed on 18 November 2022).
33. Kalloniatis, C.; Kavroudakis, D.; Polidoropoulou, A.; Gritzalis, S. Designing Privacy-Aware Intelligent Transport Systems: A Roadmap for Identifying the Major Privacy Concepts. Int. J. Appl. Geospat. Res. 2019, 10, 73–91.
34. North Atlantic Treaty Organisation NATO. NMIOTC 3000 NSC-74/ser.: NU 120. In Proceedings of the 3rd NMIOTC Cyber Security Conference—'Food for Thought', Souda Bay, Chania, Greece, 2 August 2019. Available online: https://nmiotc.nato.int/wp-content/uploads/2020/01/3000-NSC-74_NU120_02-08-19_NMIOTC-2019-cyber-security-FFT-Paper.pdf (accessed on 20 November 2022).
35. The Five Biggest Cyber Security Trends in 2022. Bernard Marr. Available online: https://bernardmarr.com/the-five-biggest-cyber-security-trends-in-2022/ (accessed on 4 October 2022).
36. Cost of a Data Breach 2022. IBM. Available online: https://www.ibm.com/reports/data-breach (accessed on 4 October 2022).
37. ENISA Threat Landscape 2021—ENISA. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (accessed on 4 October 2022).
38. AIDA Project. Available online: https://www.project-aida.eu/ (accessed on 4 October 2022).

39. Mozzaquatro, B.A.; Agostinho, C.; Goncalves, D.; Martins, J.; Jardim-Goncalves, R. An Ontology-Based Cybersecurity Framework for the Internet of Things. Sensors 2018, 18, 3053.
40. Jacq, O.; Laso, P.M.; Brosset, D.; Simonin, J.; Kermarrec, Y.; Giraud, M.-A. Maritime Cyber Situational Awareness Elaboration for Unmanned Vehicles; HAL: Lyon, France, 2019.
41. Pantazopoulos, P.; Haddad, S.; Lambrinoudakis, C.; Kalloniatis, C.; Maliatsos, K.; Kanatas, A.; Varadi, A.; Gay, M.; Amditis, A. Towards a security assurance framework for connected vehicles. In Proceedings of the 19th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2018, Chania, Greece, 12–15 June 2018; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2018.
42. International Maritime Organization. Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process; International Maritime Organization: London, UK, 2018.
43. White Paper Excerpt: Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies. Available online: https://gca.isa.org/blog/white-paper-excerpt-leveraging-isa-62443-3-2-for-iacs-risk-assessment-and-risk-related-strategies (accessed on 7 October 2022).
44. Network Sniffing—Attackics. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0842 (accessed on 8 October 2022).
45. Signori, A.; Chiariotti, F.; Campagnaro, F.; Zorzi, M. A Game-Theoretic and Experimental Analysis of Energy-Depleting Underwater Jamming Attacks. IEEE Internet Things J. 2020, 7, 9793–9804.