Exploring the Security Landscape of Underwater Positioning and Navigation Systems: An Attack Surface Analysis

Hosam Alamleh
Computer Science
University of North Carolina Wilmington
Wilmington, North Carolina
hosam.amleh@gmail.com

Bilge Karabacak
Congdon School of Supply Chain
University of North Carolina Wilmington
Wilmington, North Carolina
karabacakb@uncw.edu

2024 IEEE 49th Conference on Local Computer Networks (LCN) | 979-8-3503-8800-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/LCN60385.2024.10639769

***Abstract*—Underwater positioning and navigation systems are vital for maritime operations but face significant security threats like spoofing, jamming, interception, sensor manipulation, and algorithm exploitation. This paper categorizes underwater navigation techniques (acoustic, GPS buoys, multi-sensor fusion, vision-based, hybrid) and analyzes their potential attack surfaces. To mitigate these threats, a multi-layered defense strategy is proposed, encompassing cryptographic authentication, secure communications, physical security, sensor redundancy, data validation, image authentication, and algorithm robustness. Specific countermeasures against jamming, spoofing, interception, sensor attacks, and algorithm attacks are discussed. A holistic approach integrating secure software practices, anomaly detection, and fusion technique diversity is emphasized to fortify system resilience against advanced persistent threats, ensuring maritime safety and security. This research contributes to understanding security vulnerabilities and providing a comprehensive mitigation framework for enhancing the resilience of underwater navigation systems.**

***Index Terms*—underwater, navigation, security analysis.**

I. Introduction

In the latter half of the previous century, extensive exploration of the deep seas and oceans ignited a push to improve underwater positioning and navigation systems. Oceans and seas present diverse physical characteristics, including depth, topology, magnetic fields, and thermal profiles , posing challenges for a universal positioning solution. Vehicles often use a combination of techniques and sensors, with the choice depending on factors such as required accuracy, environmental conditions, update frequency, sensor types, cost, power consumption, depth, range, deployment time, and calibration needs. Over the past two decades, advancements in acoustic, optical, gyroscopes, and inertial measurement units have refined positioning and navigation capabilities by integrating traditional and emerging sensor technologies. The evolution of advanced sensing technologies has driven the development of innovative underwater systems.

Concerns about attacks on navigation systems are rising in maritime security [1]. These critical systems for submarines, unmanned underwater vehicles, and marine operations are susceptible to malicious activities like spoofing, which involves injecting false signals, and jamming, which disrupts communication signals. Physical attacks, such as sabotage or tampering with sensors, and cyberattacks targeting software or communication protocols, also pose risks. As reliance on these systems grows, safeguarding against such attacks becomes imperative for the safety and security of maritime activities.

This paper categorizes underwater navigation and positioning systems into five categories: acoustic, multi-sensory, GPS buoys, vision-based, and hybrid systems. It then analyzes attack surfaces for each system and discusses measures to bolster the resilience of these systems against potential attacks.

II. Categories of underwater positioning and navigation techniques

TThe need for underwater navigation emerged in the mid-20th century, primarily for submarine operations. It includes surface/near-surface navigation using above-water signals and deepwater navigation using sensors like gyroscopes and speed-measuring devices. Advancements in computing and sensing technologies have driven the evolution of underwater robot navigation. These vehicles perform tasks such as surveying, data collection, salvage, and research . Underwater navigation involves positioning to determine location, mapping to create detailed maps, routing to plan paths, and motion control to guide the vehicle along the route. Feedback loops with updated position data ensure accuracy.

Underwater positioning and navigation can be classified into fixed, movable, and portable categories based on equipment placement [2]. Fixed systems have equipment on the ocean bed, enabling long-range navigation but are costly and limited to specific areas; movable systems have components on a nearby surface ship, allowing easy adjustment by relocating the ship [3]; and portable systems involve lightweight, compact equipment for easy transport but with limited range [4]. Methods for underwater positioning include surface GPS buoys, machine vision, and various sensor technologies, each with different costs, accuracy, operational depths, and performance, requiring careful consideration for different environments.

Authorized licensed use limited to: IEEE Xplore. Downloaded on September 15,2024 at 23:53:27 UTC from IEEE Xplore. Restrictions apply.

A. Acoustic

Acoustic signals are essential for underwater positioning and navigation because they propagate farther than electromagnetic signals in water. Despite variations in equipment, all acoustic underwater technologies use geometric acoustic water positioning. This method is classified by the baseline length of the radio receiving array: long-baseline [5], short-baseline [6], and ultra-short baseline [7]. Short and ultra-short baseline systems offer high accuracy and flexibility over short ranges but are limited over longer distances. Long-baseline systems provide high accuracy and extended range but are more expensive and less adaptable.

B. GPS buoy

The Global Positioning System (GPS), developed by the United States, offers high precision, flexibility, and ease of use, making it widely used in various applications [8]. However, GPS is limited to open sky environments, as its signals cannot penetrate water [9]. Underwater navigation requires supplementary devices. Typically, GPS buoys on the water's surface intercept GPS signals and transmit them underwater via acoustic waves [10]. Submerged receivers on underwater vehicles capture these signals, while additional sensors measure the angle of arrival to compute distances using acoustic principles [11]. Alternatively, a single buoy can correct the vehicle's position in real-time by receiving and transmitting GPS signals. Another approach uses buoy arrays, where multiple buoys receive GPS signals and locate underwater vehicles using ultrasound based on differences in signal arrival times [12]. While multiple buoys enhance accuracy, they also increase acquisition and deployment costs.

C. Multi-sensory fusion

Multi-sensor information fusion technology integrates data from multiple sensors to enhance the precision of underwater vehicle positioning and velocity calculations [13]. Sensors can be internal (measuring vehicle parameters like speed and angle) or external (capturing environmental data like object distance and shape) [14]. Examples [15] include inertial sensors, speedometers, infrared, sonar, ultrasonic, and optical sensors . Fusion algorithms like weighted averages, Bayesian networks , Kalman filters, clustering , and neural networks are used to validate and refine navigation. A popular technique is Simultaneous Localization and Mapping (SLAM), which combines sensor data for positioning and mapping unfamiliar environments [16]. SLAM maps fall into three categories: grid maps (2D representations using LIDAR), geometric feature maps (describing environments with points, lines, and polygons from sensor data), and topological maps (representing structure with nodes and paths between them). Each map type offers advantages for navigation and mapping in diverse environments.

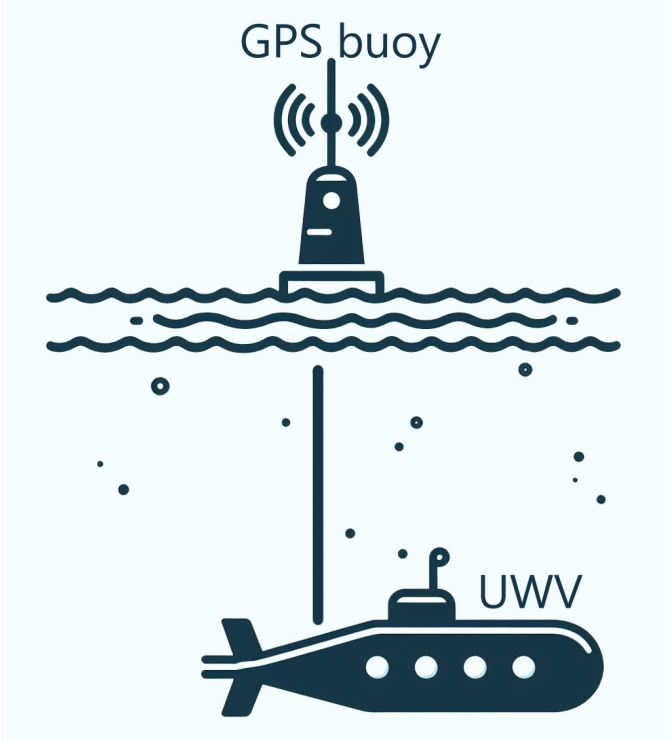

Fig. 1. GPS Buoy

D. Vision-based

Vision-based methods rely on machine vision and image processing techniques to extract points and features from images, aiding in positioning . Recent advances in optical sensor technology have increased research interest in vision-based positioning and navigation [17]. Computer vision approaches can be monocular, processing three-dimensional data into two-dimensional planes, or binocular, processing data across all three dimensions [17]. Some systems utilize geometry, analyzing single-frame images to navigate based on nearby geometric features [18]. Another approach involves pattern matching, comparing captured images to a database to estimate the vehicle's position and ensure it follows the correct path [19].

E. Hybrid positioning

Hybrid positioning involves underwater vehicles exchanging information via acoustic communication to enhance positioning accuracy through information fusion technology [20]. This collaborative approach uses multiple vehicles working together to achieve precise positioning and navigation. Typically, these methods involve devices with different capabilities, known as pilots and parallels [21]. Pilots are equipped with high-precision sensors, while parallels have less capable equipment [22]. Pilots transmit their positions via acoustic signals at regular intervals, which parallels receive to calculate their relative positions and refine their own positioning calculations.

Authorized licensed use limited to: IEEE Xplore. Downloaded on September 15,2024 at 23:53:27 UTC from IEEE Xplore. Restrictions apply.

III. Attack surface analysis

A. Acoustic

Acoustic underwater navigation systems are vulnerable to various forms of attack, including jamming, spoofing, interception , and physical tampering . Jamming involves attackers emitting strong interfering acoustic signals within the same frequency range as the navigation system, disrupting communication between the transmitter and receiver . This interference can result in inaccurate positioning or a complete loss of navigation capability [23]. Spoofing occurs when attackers transmit false acoustic signals that mimic legitimate navigation signals. As shown in Fig. 2., spoofing devices deceive the system with incorrect positioning information, attackers can lead vessels or underwater vehicles astray. This deception can involve impersonating a legitimate transponder or broadcasting false positional data [24].

Interception involves attackers intercepting the acoustic signals transmitted between transmitters and receivers. This breach can provide attackers with insights into the operational patterns of vessels or underwater assets, compromising the security and privacy of the navigation system's users and their missions [25]. Physical tampering involves attackers physically manipulating the acoustic transducers or other components of the navigation system to degrade performance or render it non-functional. This tampering can include sabotage of equipment or tampering with underwater cables connecting the components [26].

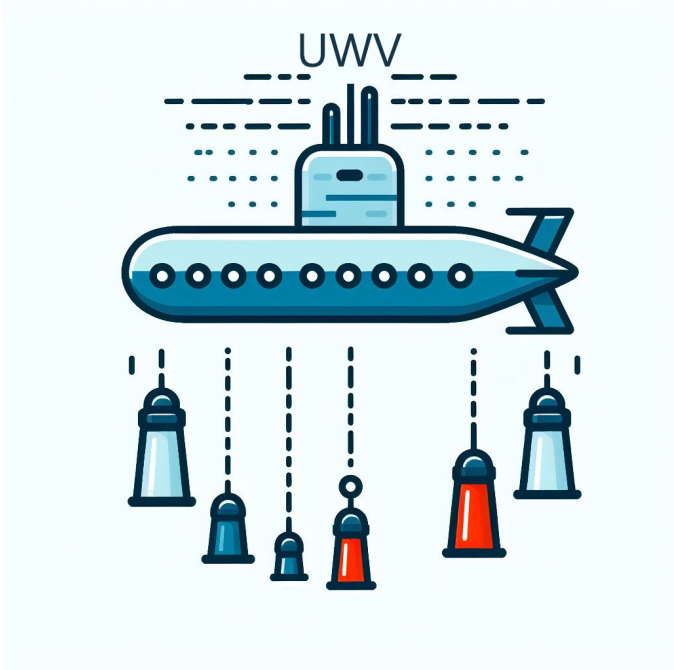

Fig. 2. Attack scenario on accoustic navigation

B. GPS buoy

GPS buoys, particularly surface GPS buoys, are vulnerable to various GPS attacks. Firstly, attackers may jam the GPS signals received by surface buoys, disrupting the transmission of accurate positioning data to underwater vehicles. By emitting strong interfering signals, attackers can prevent the buoys from relaying precise GPS information to submerged receivers, resulting in navigation errors or a loss of positioning capability [27]. Alternatively, attackers may transmit spoofed GPS signals. Similar to acoustic navigation systems, they can mimic legitimate GPS signals by transmitting false signals. By deceiving GPS buoys with fake positioning data, attackers can lead underwater vehicles astray, potentially causing navigation errors or even dangerous situations [28]. Moreover, attackers may target channel interception, intercepting acoustic transmissions between GPS buoys and underwater receivers. By eavesdropping on these communications and potentially sending tampered information, attackers compromise the integrity and security of the navigation system.

C. Multi-sensory fusion

Multi-sensor systems, which rely on gathering information from various sensors and combining them through algorithms, are susceptible to multiple types of attacks. One such vulnerability is Sensor Tampering [29], where attackers physically interfere with sensors, modifying their readings or rendering them inoperative. For example, internal sensors like inertial sensors or speedometers could be sabotaged through calibration manipulation or component damage [30]. Likewise, external sensors might be tampered with to provide false environmental data. Additionally, attackers can engage in Sensor Spoofing, where they transmit false signals or manipulate sensor inputs to deceive fusion algorithms with counterfeit sensor data. This manipulation can result in inaccurate positioning and velocity calculations, potentially leading to navigation errors or misguidance of the underwater vehicle [31]. Finally, attackers may target the fusion algorithms themselves by injecting malicious code or exploiting vulnerabilities in their implementation [32]. By tampering with the fusion process, attackers can manipulate navigation calculations and mislead the underwater vehicle regarding its position or velocity [33]. These attacks pose significant threats to the integrity and reliability of multi-sensor information fusion systems.

D. Vision-based

Vision-based systems are susceptible to various attacks. In Image Manipulation attacks [34], adversaries could tamper with images captured by the system to convey false information about the environment or the vehicle's position. By altering key features or landmarks in the images, attackers could deceive the navigation system, leading it off course. Similarly, in Database Spoofing attacks [35], if the system relies on a database for pattern matching, attackers could manipulate the database by inserting false images or modifying existing ones. This could result in inaccurate estimations of the vehicle's position, causing navigation errors or deviation from the intended path. Furthermore, communication interception poses a threat. Attackers could intercept communications and modify image data before it reaches the navigation system

Authorized licensed use limited to: IEEE Xplore. Downloaded on September 15,2024 at 23:53:27 UTC from IEEE Xplore. Restrictions apply.

[36]. By tampering with the image data during transit, attackers could manipulate navigation calculations, compromising the system's integrity. Lastly, attackers could exploit vulnerabilities in the image processing algorithms employed by the vision-based system [37]. By injecting malicious code or adjusting algorithm parameters, attackers could distort image processing results, misleading the navigation system regarding the vehicle's position or the surrounding environment.

E. Hybrid positioning and navigation

In hybrid positioning, multiple methods are utilized simultaneously, often incorporating two or more of the techniques mentioned above. Consequently, they may inherit the same weaknesses and vulnerabilities present in individual methods. Furthermore, these systems are susceptible to algorithm attacks, where the algorithm responsible for combining position or navigation data from multiple methods can be targeted to produce false outputs [38].

IV. Possible Mitigation

After exploring the attack surface and various attack scenarios within different underwater navigation and positioning systems, we identified main categories of attacks. In the following discussion, we'll focus on mitigating these main categories of attacks, with each category addressed in its own subsection.

A. Jamming

Jamming of navigation systems is a widespread and effective method of attack, presenting a considerable challenge for defense. However, various techniques exist to counteract its effects. One strategy involves utilizing Frequency Hopping Spread Spectrum [39] and Direct Sequence Spread Spectrum [40], which broaden the signal across a wider frequency range, making it more resistant to jamming. By dispersing the signal, it becomes increasingly difficult for jammers to disrupt the entirety of the transmission.

Another method to combat jamming involves Beam Forming [41] and Directional Antennas [42]. These technologies focus transmitted signal energy in specific directions, diminishing the impact of jamming from other angles. Directional antennas further enhance this by concentrating the signal toward intended receivers while minimizing interference from other sources [42]. Adaptive Filtering [43] and Nulling [44] present another potential solution, adjusting receiver parameters to filter out jamming signals based on their unique characteristics, such as frequency or direction. Nulling algorithms can pinpoint the jamming source's direction and create nulls in the antenna pattern to suppress interference. Frequency Agility offers an additional approach. If jamming is detected on a particular frequency band, the system can swiftly switch to an alternative band to evade interference. This method relies on support for multiple frequency bands and effective spectrum sensing capabilities [45]. Lastly, incorporating Forward Error Correction codes and interleaving techniques can aid in data recovery amidst jamming-induced errors [46], ensuring transmission reliability despite interference.

B. Spoofing attacks

There are various strategies available to counter spoofing attacks within underwater navigation systems. One approach involves signal authentication, wherein cryptographic methods are utilized to validate the authenticity of received acoustic or GPS signals [47]. Techniques such as digital signatures or message authentication codes are employed to ensure that only signals from trusted sources are accepted and processed by the navigation system [47]. Alternatively, signal source verification techniques can be employed to confirm the origin of received signals [48]. Time-of-arrival [49] or time-difference-of-arrival measurements [49] can aid in identifying the true source of the signal and detecting unauthorized spoofing attempts. Additionally, signal processing and filtering techniques can be implemented to discern and filter out potential spoofing signals. Advanced methods like adaptive filtering or signal correlation [50] enable the identification and rejection of signals that deviate from expected patterns or exhibit anomalous characteristics. Finally, redundancy and diversity measures can enhance mitigation efforts by utilizing multiple independent navigation systems or sensors [51]. Combining different systems, such as acoustic navigation with inertial navigation systems, allows for cross-checking and data fusion, thereby enabling the detection and mitigation of spoofing attacks targeting any single system. It is essential to adopt a multi-layered approach, combining various mitigation techniques, to enhance the overall security and resilience of the underwater navigation system against spoofing attacks. As a general comment on preventing spoofing attacks, While cryptographic methods can be employed to validate the authenticity of received acoustic or GPS signals, the practicality of modifying GPS to encrypt civilian signals must be considered. The implementation of such encryption would likely incur significant costs for users, who would need to update both hardware and software. Additionally, the effectiveness of these methods could be undermined by spoofers capable of replicating authentic signals through replay attacks.

C. Interception

To mitigate intercepting attacks, which can potentially target all the methods discussed above, one effective approach is to establish secure communication channels. This involves creating secure connections between all components of the navigation system [52], including transmitters, receivers, GPS buoys, and sensors. To achieve this, protocols such as IPsec [53], TLS/SSL, or secure tunneling mechanisms can be implemented to safeguard the integrity and confidentiality of transmitted data. Furthermore, employing robust encryption algorithms ensures that even if an attacker manages to intercept the data, they cannot decipher its contents without the appropriate decryption keys. Additionally, incorporating authentication mechanisms helps verify the legitimacy of communication parties within the navigation system. Utilizing digital signatures or message authentication codes [54] can ensure the integrity of transmitted data, thereby preventing tampering or unauthorized modifications during transit. Another effective

Authorized licensed use limited to: IEEE Xplore. Downloaded on September 15,2024 at 23:53:27 UTC from IEEE Xplore. Restrictions apply.

technique to counter intercepting attacks is the implementation of frequency hopping and spread spectrum techniques [55]. These methods introduce frequency variations and spread the signal across a wider bandwidth, making it significantly more challenging for attackers to track and intercept transmissions. By incorporating these measures, the navigation system can enhance its resilience against interception threats.

D. Sensor manipulation

To defend against sensor manipulation attacks, implementing robust physical security measures becomes handy by utilizing tamper-evident seals [56], secure enclosures, and access controls to protect the sensors and critical components from unauthorized access or tampering. Environmental monitoring systems should be employed to detect potential tampering attempts or anomalies in the sensor environments. Sensor redundancy and diversity is important; utilizing multiple redundant sensors of different types to measure the same physical quantities or environmental conditions can help cross-check and fuse data from diverse sensor sources, thereby detecting and mitigating potential tampering or spoofing attempts on individual sensors [57]. Additionally, implementing sensor data validation techniques to detect anomalous or suspicious sensor readings that deviate from expected patterns or thresholds, and using advanced filtering algorithms, such as Kalman filters [57] or particle filters [58], to fuse sensor data and reject outliers or inconsistent measurements can be beneficial. Secure sensor calibration and configuration, using digitally signed configurations and firmware updates to ensure integrity and authenticity, can prevent unauthorized modifications or tampering. Finally, for vision-based systems, implementing image authentication techniques, such as digital watermarking [59] or cryptographic hashes, to verify the integrity and authenticity of captured images and detecting and rejecting images that have been tampered with or modified by attackers is crucial.

E. Algorithm attacks

To counter algorithm attacks aimed at underwater navigation systems reliant on multi-sensor fusion and vision-based methods, several mitigation strategies can be adopted. Firstly, prioritize securing software development practices to ensure fusion and image processing algorithms are crafted with security at the forefront. This involves implementing secure coding practices, conducting code reviews, and employing static code analysis to detect and rectify potential vulnerabilities. Additionally, enforce input validation and sanitization to filter out illegitimate or unexpected data inputs, thereby bolstering algorithm integrity. Similarly, validate sensor and image data against predefined criteria to discard any malicious or abnormal inputs. Moreover, enhance algorithm robustness by incorporating diverse fusion and image processing techniques, enabling cross-validation to thwart manipulation attempts. Furthermore, integrate anomaly detection mechanisms to scrutinize algorithm behavior and outputs for deviations from expected norms, leveraging machine learning, statistical analysis, or rule-based approaches to flag potential attacks.

F. Data exfiltration

Data exfiltration represents a substantial threat to underwater navigation systems due to the critical and sensitive nature of the information these systems handle. Underwater navigation relies heavily on precise, real-time data from various sensors, including sonar, GPS, and inertial navigation systems, to ensure accurate positioning and navigation. Unauthorized access and extraction of this data can result in severe consequences, such as compromised mission integrity, exposure of strategic movements, and increased vulnerability to cyber-attacks [60]. Exfiltration of navigation data can occur through several methods, such as targeting navigation system nodes, where attackers may attempt to extract logs or historical data from navigation system nodes [61]. This method typically requires physical access to difficult locations and significant resources. Some navigation systems might not include data from the underwater vehicle, reducing the risk of immediate data exfiltration. Another, method would be planting capture devices inside the underwater vehicles, this involves planting devices that can capture navigation paths and subsequently exfiltrate the data. These devices can leverage network connections when the underwater vehicle surfaces, utilizing cellular networks [62], Wi-Fi [63], or the Apple Find My network [64]. The latter method is particularly dangerous as it does not require a dedicated connection; data can be reported to the Find My network via any nearby Apple device, enabling global data transmission.

To mitigate the first type of data exfiltration, where the navigation system is targeted, encryption of data on these system nodes and logs is recommended. This ensures that any recorded information about the traveling vehicles within the navigation system nodes remains secure. For the second type of exfiltration, involving capture devices, several countermeasures can be employed. One is detection, where methods are Implemented to detect spying devices within underwater vehicles [65]. Another is jamming [66], where jamming techniques are used to disrupt the communication capabilities of unauthorized devices. Finally, firewalls, which prevent unauthorized network access and data transmission.

V. Discussion

This paper explores various types of underwater navigation systems, which operate under challenging environmental conditions such as pressure, temperature, and corrosion. These conditions can gradually degrade the performance and reliability of the equipment, potentially resulting in navigation errors or failures. Despite these challenges, underwater navigation systems are inherently difficult to target, often becoming objectives for Advanced Persistent Threats (APTs) due to their resourcefulness in disrupting navigation.

APT adversaries may attempt to disturb navigation systems by deploying devices in specific areas or deploying underwater vehicles. Despite the primary target being APTs, these systems are not adequately protected against attacks, often relying on the difficulty of physical access as a form of defense. Consequently, there is often a lack of fortification, including

Authorized licensed use limited to: IEEE Xplore. Downloaded on September 15,2024 at 23:53:27 UTC from IEEE Xplore. Restrictions apply.

the absence of encryption, which stems from the challenges attackers face in reaching navigation devices physically.

Another critical factor affecting these systems is the limited processing power of the devices, which hinders their ability to handle encryption and additional overhead. This limitation is significant because such devices typically have restricted access to power, relying on batteries or energy harvesting. Thus, the inherent weakness in processing complex calculations poses a challenge.

Furthermore, underwater navigation systems must operate in real-time, requiring accurate location calculations as devices move. Delays resulting from additional processing for security functions can affect the real-time nature and accuracy of the system.

In summary, underwater navigation systems present challenges due to their remote and harsh environments, making them difficult to access. However, these conditions also lead to weaknesses in powering the devices and processing complex security functions without introducing delays. Consequently, these systems are vulnerable to Advanced Persistent Attacks, particularly from adversaries capable of physically accessing the areas where navigation systems are deployed.

VI. Conclusion

Underwater positioning and navigation systems are vital for a wide range of maritime operations, from submarine maneuvers to unmanned vehicle deployments. However, the diverse array of techniques employed, each with its unique strengths and vulnerabilities, necessitates a comprehensive understanding of potential attack vectors and mitigation strategies. This paper has presented a categorization of prominent underwater positioning and navigation methods, including acoustic, GPS buoys, multi-sensor fusion, vision-based, , and hybrid positioning systems. For each category, an in-depth analysis of potential attack surfaces was conducted, highlighting vulnerabilities such as spoofing, jamming, interception, sensor manipulation, and algorithm exploitation.

To fortify the resilience of these critical systems, a multi-layered defense approach is recommended, encompassing various mitigation techniques. Strategies like cryptographic authentication, signal verification, and filtering can counter spoofing attacks, while secure communication protocols and frequency hopping can mitigate interception threats. Robust physical security measures, sensor redundancy, and data validation techniques are crucial for defending against sensor manipulation. For vision-based systems, image authentication and algorithm robustness enhancements are pivotal. Ultimately, a holistic security posture that integrates secure software development practices, anomaly detection, and diverse fusion techniques is essential to safeguard underwater navigation systems from advanced persistent threats.

References

[1] E. News, "Researcher: Navigation systems attacks are becoming increasingly common," 2024.

[2] S. J. McManus, "A method of navigation using a modified ultra short base line directional acoustic transponder," in *OCEANS 2007 - Europe*, pp. 1–5, 2007.

[3] J. Tong, X. Xu, L. Hou, Y. Li, J. Wang, and L. Zhang, "An ultra-short baseline positioning model based on rotating array amp; reusing elements and its error analysis," *Sensors*, vol. 19, no. 20, 2019.

[4] D. Thomson and S. Elson, "New generation acoustic positioning systems," in *OCEANS '02 MTS/IEEE*, vol. 3, pp. 1312–1318 vol.3, 2002.

[5] X. Lurton and N. Millard, "The feasibility of a very-long baseline acoustic positioning system for auvs," in *Proceedings of OCEANS'94*, vol. 3, pp. III/403–III/408 vol.3, 1994.

[6] K. Chterev, "One-way short baseline underwater positioning system," 10 2018.

[7] S. Dajun, G. Jia, Z. Jucheng, and H. Yunfeng, "Design of high accuracy ultra short baseline underwater acoustic position system," in *2017 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, pp. 1–4, 2017.

[8] L. Paull, S. Saeedi, M. Seto, and H. Li, "Sensor-driven online coverage planning for autonomous underwater vehicles," *IEEE/ASME Transactions on Mechatronics*, vol. 18, no. 6, pp. 1827–1838, 2013.

[9] L. Jurišica, F. Duchoň, D. Kastan, and A. Babinec, "High precision gnss guidance for field mobile robots," *International Journal of Advanced Robotic Systems*, vol. 9, p. 1, 11 2012.

[10] M. Fujita, T. Ishikawa, M. Mochizuki, M. Sato, S.-I. Toyama, M. Katayama, K. Kawai, Y. Matsumoto, T. Yabuki, A. Asada, and O. Colombo, "Gps/acoustic seafloor geodetic observation: Method of data analysis and its application," *Earth Planets Space*, vol. 58, pp. 265–275, 03 2006.

[11] R. Almeida, N. Cruz, and A. Matos, "Synchronized intelligent buoy network for underwater positioning," in *OCEANS 2010 MTS/IEEE SEATTLE*, pp. 1–6, 2010.

[12] A. Alcocer, P. Oliveira, A. Pascoal, and J. Xavier, "Estimation of attitude and position from range-only measurements using geometric descent optimization on the special euclidean group," in *2006 9th International Conference on Information Fusion*, pp. 1–8, 2006.

[13] A. Aguileta, R. Brena, O. Mayora, E. Molino Minero Re, and L. Trejo, "Multi-sensor fusion for activity recognition—a survey," *Sensors*, vol. 19, 09 2019.

[14] F. Kamil, T. S. Hong, W. Khaksar, M. Y. Moghrabiah, N. Zulkifli, and S. A. Ahmad, "New robot navigation algorithm for arbitrary unknown dynamic environments based on future prediction and priority behavior," *Expert Systems with Applications*, vol. 86, pp. 274–291, 2017.

[15] D. Masumoto, T. Kimoto, and S. Nagata, "A sensory information processing system using neural networks," in *IEEE International Conference on Neural Networks*, pp. 655–660 vol.2, 1993.

[16] L. Paull, S. Saeedi, M. Seto, and H. Li, "Auv navigation and localization: A review," *IEEE Journal of Oceanic Engineering*, vol. 39, no. 1, pp. 131–149, 2014.

[17] Z. Mingjun, L. Shupeng, and L. Xuan, "Research on technologies of underwater feature extraction and target location based on binocular vision," in *The 27th Chinese Control and Decision Conference (2015 CCDC)*, pp. 5778–5784, 2015.

[18] F. Dalgleish, S. Tetlow, and R. Allwood, "Vision-based navigation of unmanned underwater vehicles: A survey part i: Vision based cable-, pipeline-and fish tracking," pp. 51–56, 01 2004.

[19] P. Zhang, E. Milios, and J. Gu, "Underwater robot localization using artificial visual landmarks," in *2004 IEEE International Conference on Robotics and Biomimetics*, pp. 705–710, 2004.

[20] W. Gao, Y.-L. Liu, and B. Xu, "Observability analysis of cooperative navigation system for multiple auv based on two-leaders," *Xi Tong Gong Cheng Yu Dian Zi Ji Shu/Systems Engineering and Electronics*, vol. 35, pp. 2370–2375, 11 2013.

[21] P. Xie, F. Kang, and Y. Wang, "Cooperative navigation for multi-uuv using relative observations," in *2010 3rd International Congress on Image and Signal Processing*, vol. 7, pp. 3191–3194, 2010.

[22] P. Baccou, B. Jouvencel, V. Creuze, and C. Rabaud, "Cooperative positioning and navigation for multiple auv operations," in *MTS/IEEE Oceans 2001. An Ocean Odyssey. Conference Proceedings (IEEE Cat. No.01CH37295)*, vol. 3, pp. 1816–1821 vol.3, 2001.

[23] S. Misra, S. Dash, M. Khatua, A. V. Vasilakos, and M. S. Obaidat, "Jamming in underwater sensor networks: detection and mitigation," *IET communications*, vol. 6, no. 14, pp. 2178–2188, 2012.

[24] E. Ochin, "Spoofing detection for underwater acoustic gnss-like positioning systems," *Zeszyty Naukowe Akademii Morskiej w Szczecinie*, 2019.

Authorized licensed use limited to: IEEE Xplore. Downloaded on September 15,2024 at 23:53:27 UTC from IEEE Xplore. Restrictions apply.

[25] F. Campagnaro, D. Tronchin, A. Signori, R. Petroccia, K. Pelekanakis, P. Paglierani, J. Alves, and M. Zorzi, "Replay-attack countermeasures for underwater acoustic networks," in *Global Oceans 2020: Singapore–US Gulf Coast*, pp. 1–9, IEEE, 2020.

[26] L. R. Wrathall, "The vulnerability of subsea infrastructure to underwater attack: Legal shortcomings and the way forward," *San Diego Int'l LJ*, vol. 12, p. 223, 2010.

[27] H. Hu and N. Wei, "A study of gps jamming and anti-jamming," in *2009 2nd international conference on power electronics and intelligent transportation system (PEITS)*, vol. 1, pp. 388–391, IEEE, 2009.

[28] A. Androjna, T. Brcko, I. Pavic, and H. Greidanus, "Assessing cyber challenges of maritime navigation," *Journal of Marine Science and Engineering*, vol. 8, no. 10, p. 776, 2020.

[29] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, 2018.

[30] G. Yang, L. Dai, and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," *Sensors*, vol. 18, no. 11, p. 3907, 2018.

[31] I. Ahmad, T. Rahman, A. Zeb, I. Khan, I. Ullah, H. Hamam, and O. Cheikhrouhou, "Analysis of security attacks and taxonomy in underwater wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–15, 2021.

[32] S. Nashimoto, D. Suzuki, T. Sugawara, and K. Sakiyama, "Sensor confusion: Defeating kalman filter in signal injection attack," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pp. 511–524, 2018.

[33] C. Yang, L. Feng, H. Zhang, S. He, and Z. Shi, "A novel data fusion algorithm to combat false data injection attacks in networked radar systems," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 125–136, 2018.

[34] N. Akhtar, A. Mian, N. Kardan, and M. Shah, "Advances in adversarial attacks and defenses in computer vision: A survey," *IEEE Access*, vol. 9, pp. 155161–155196, 2021.

[35] Y. Xu, X. Han, G. Deng, J. Li, Y. Liu, and T. Zhang, "Sok: Rethinking sensor spoofing attacks against robotic vehicles from a systematic view," in *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, pp. 1082–1100, IEEE, 2023.

[36] B. Ly and R. Ly, "Cybersecurity in unmanned aerial vehicles (uavs)," *Journal of cyber security technology*, vol. 5, no. 2, pp. 120–137, 2021.

[37] L. González-Manzano and J. Garcia-Alfaro, "Software vulnerability detection under poisoning attacks using cnn-based image processing," 2024.

[38] W. Yang, Y. Zhou, Y. Cao, H. Zhang, Q. Zhang, and H. Wang, "Multi-channel fusion attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 8, pp. 1757–1771, 2017.

[39] A. Yahya, O. Sidek, J. Mohamad-Saleh, and C. Center, "Performance analyses of fast frequency hopping spread spectrum and jamming systems.," *Int. Arab J. Inf. Technol.*, vol. 5, no. 2, pp. 115–119, 2008.

[40] S. Zhou, G. B. Giannakis, and A. Swami, "Digital multi-carrier spread spectrum versus direct sequence spread spectrum for resistance to jamming and multipath," *IEEE Transactions on Communications*, vol. 50, no. 4, pp. 643–655, 2002.

[41] A. Aldarraji, L. Hong, and S. Shetty, "Polarized beamforming for enhanced countermeasure of wireless jamming attacks," in *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, pp. 1–2, IEEE, 2016.

[42] P. A. Molchanov and V. M. Contarino, "Directional antenna array (daa) for communications, control, and data link protection," in *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense XII*, vol. 8711, pp. 208–216, SPIE, 2013.

[43] K. Pärlin, T. Riihonen, and M. Turunen, "Sweep jamming mitigation using adaptive filtering for detecting frequency agile systems," in *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, pp. 1–6, IEEE, 2019.

[44] Q. J. O. Tan and R. A. Romero, "Jammer-nulling transmit-adaptive radar against knowledge-based jammers in electronic warfare," *IEEE Access*, vol. 7, pp. 181899–181915, 2019.

[45] X. Liu, G. Noubir, R. Sundaram, and S. Tan, "Spread: Foiling smart jammers using multi-layer agility," in *IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications*, pp. 2536–2540, IEEE, 2007.

[46] Y.-S. Liu, "Diversity-combining and error-correction coding for ffh/mfsk systems over rayleigh fading channels under multitone jamming," *IEEE transactions on wireless communications*, vol. 11, no. 2, pp. 771–779, 2011.

[47] G. Caparra, C. Wullems, S. Ceccato, S. Sturaro, N. Laurenti, O. Pozzobon, R. T. Ioannides, and M. Crisci, "Navigation message authentication schemes," *Inside GNSS*, 2016.

[48] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil gnsss: Recent solutions and perspectives," *IEEE signal processing magazine*, vol. 34, no. 5, pp. 27–37, 2017.

[49] Y.-T. Chan, W.-Y. Tsui, H.-C. So, and P.-c. Ching, "Time-of-arrival based localization under nlos conditions," *IEEE Transactions on vehicular technology*, vol. 55, no. 1, pp. 17–24, 2006.

[50] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Gps spoofing detection via dual-receiver correlation of military signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 4, pp. 2250–2267, 2013.

[51] J. N. J. Thomas, R. V. Kumar, and M. S. Murugan, "Prevention and detection of spoofing attack in wireless sensor network," *i-Manager's Journal on Wireless Communication Networks*, vol. 9, no. 1, p. 7, 2020.

[52] M. L. Das and N. Samdaria, "On the security of ssl/tls-enabled applications," *Applied Computing and informatics*, vol. 10, no. 1-2, pp. 68–81, 2014.

[53] N. Ferguson and B. Schneier, "A cryptographic evaluation of ipsec," 1999.

[54] S. Čapkun, M. Čagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 4, pp. 208–223, 2008.

[55] J. W. Park, D.-S. Yoo, and S.-J. Oh, "Interceptor complexity analysis for mixed bpsk–qpsk modulated frequency hopping spread spectrum systems," *Physical Communication*, vol. 40, p. 101063, 2020.

[56] T. Moran and M. Naor, "Basing cryptographic protocols on tamper-evident seals," *Theoretical Computer Science*, vol. 411, no. 10, pp. 1283–1310, 2010.

[57] G. Longo, E. Russo, A. Armando, and A. Merlo, "Attacking (and defending) the maritime radar system," *IEEE Transactions on Information Forensics and Security*, 2023.

[58] M. Khalaf, A. Youssef, and E. El-Saadany, "A particle filter-based approach for the detection of false data injection attacks on automatic generation control systems," in *2018 IEEE Electrical Power and Energy Conference (EPEC)*, pp. 1–6, IEEE, 2018.

[59] P. Singh and R. S. Chadha, "A survey of digital watermarking techniques, applications and attacks," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 2, no. 9, pp. 165–175, 2013.

[60] U. N. Institute, "The silent service," *Proceedings*, October 2023. Accessed: 2024-07-15.

[61] J. Rice, G. Wilson, M. Barlett, J. Smith, T. Chen, C. Fletcher, B. Creber, Z. Rasheed, G. Taylor, and N. Haering, "Maritime surveillance in the intracoastal waterway using networked underwater acoustic sensors integrated with a regional command center," in *2010 International WaterSide Security Conference*, pp. 1–6, 2010.

[62] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "{GSMem}: Data exfiltration from {Air-Gapped} computers over {GSM} frequencies," in *24th USENIX Security Symposium (USENIX Security 15)*, pp. 849–864, 2015.

[63] M. Guri, "Air-fi: Leaking data from air-gapped computers using wi-fi frequencies," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 3, pp. 2547–2564, 2023.

[64] A. Cantelli-Forti, M. Colajanni, and S. Russo, "Penetrating the silence: Data exfiltration in maritime and underwater scenarios," in *2023 IEEE 48th Conference on Local Computer Networks (LCN)*, pp. 1–6, 2023.

[65] S. B. Sadkhan, "Eavesdropping techniques role in information warfare - status, challenges and future trends," in *2021 2nd Information Technology To Enhance e-learning and Other Application (IT-ELA)*, pp. 172–176, 2021.

[66] Q. Sun, T. Shu, M. Tang, K.-B. Yu, and W. Yu, "Effective moving target deception jamming against multichannel sar-gmti based on multiple jammers," *IEEE Geoscience and Remote Sensing Letters*, vol. 17, no. 3, pp. 441–445, 2020.

Authorized licensed use limited to: IEEE Xplore. Downloaded on September 15,2024 at 23:53:27 UTC from IEEE Xplore. Restrictions apply.