Section 2

CYBERSECURITY OF COMMUNICATION CHANNELS OF UNDERWATER MONITORING DEVICES

Mykyta Shypunov
National Aerospace University «Kharkiv Aviation Institute»
Zemlianko Heorhii

Relevance. Relevance. Underwater monitoring devices are essential in oceanography, marine exploration, environmental monitoring, and defense. However, the communication channels transmitting this data are vulnerable to cyber threats. Underwater environments pose challenges like limited bandwidth, high latency, signal degradation, and energy constraints, hindering traditional cybersecurity methods [1]. Acoustic communication, the primary method for underwater transmission, is prone to interference and signal loss, making it exploitable [2]. Optical and RF systems, while better in bandwidth and latency, are limited by range and security vulnerabilities [2,3]. This underscores the need for tailored cybersecurity solutions for underwater networks.

The purpose of this work is to investigate the cybersecurity risks associated with the communication channels of underwater monitoring devices and propose effective mechanisms to mitigate these risks. The study focuses on evaluating the vulnerabilities of acoustic, optical, and RF communication technologies commonly used in underwater environments and explores hybrid communication systems as potential solutions. The objective is to identify specific attack vectors, including data interception, man-in-the-middle attacks, and signal manipulation, and to propose cybersecurity protocols that can be implemented without overloading the energy and computational capacities of underwater devices.

Principal provisions. Vulnerabilities of Acoustic Communication: Acoustic communication is particularly susceptible to signal interference, attenuation, and eavesdropping. The slow data rates inherent to this technology make the integration of sophisticated encryption protocols challenging, as they can significantly increase the energy consumption of devices [3]. These limitations increase the risk of unauthorized data interception, particularly in noisy or hostile marine environments [4]. Challenges in Optical and RF Communication: Optical systems, while offering high bandwidth, are limited by short ranges and physical signal interception [3]. RF systems, used in surface communication, face absorption issues and intermittent security risks [4]. Hybrid Systems: Combining acoustic, optical, and RF communication offers flexibility, but adds complexity in securing multiple channels [4]. Multi-layer encryption can help but requires further optimization [5]. Device Physical Security: Physical tampering of

underwater devices can lead to data breaches. Tamper-proof hardware and integrity checks are vital [5].

Conclusions. The cybersecurity of communication channels in underwater monitoring devices presents significant challenges due to the limitations imposed by the marine environment, including signal attenuation, noise interference, and energy constraints. Acoustic, optical, and RF communication technologies each have specific vulnerabilities that can be exploited by malicious actors. Hybrid communication systems offer flexibility but introduce additional security complexities. To enhance cybersecurity in underwater networks, it is necessary to develop lightweight encryption protocols, adaptive security frameworks, and tamper-proof hardware designs that balance the need for robust security with the operational constraints of these systems. Future research should focus on testing these solutions in real-world environments to validate their effectiveness.

List of references

1. Abdi A., Zhang E., Rashid R. Multichannel signal transmission and reception using compact multichannel underwater communication devices: a unified theory and experimental results from different underwater media. *The journal of the acoustical society of america*. 2024. Volume 155(3). P. A317. DOI: https://doi.org/10.1121/10.0027648.
2. Sea water channel for underwater communication / T. S. Priya et al. *E3S web of conferences*. 2023. Volume 399. P. 01015. DOI: https://doi.org/10.1051/e3sconf/202339901015.
3. Channel polarization scheme for ocean turbulence channels in underwater visible light communication / X. Li et al. *Journal of marine science and engineering*. 2023. Volume 11(2). Page 341. DOI: https://doi.org/10.3390/jmse11020341.
4. Communication for underwater robots: recent trends / A. Quattrini Li et al. *Current robotics reports*. 2023. DOI: https://doi.org/10.1007/s43154-023-00100-4.
5. Pavlov I. I., Myshkin V. F., Khan V. A. Organization of an underwater wireless communication system. *T-Comm*. 2024. Volume 18(1). Page 4–12. DOI: https://doi.org/10.36724/2072-8735-2024-18-1-4-12.

Information about the authors

Mykyta Shypunov, cybersecurity researcher, kin.shypunov@gmail.com
Heorhii Zemlianko, a Senior Lecture, PhD of cybersecurity from the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University «Kharkiv Aviation Institute», g.zemlynko@csn.khai.edu