SCIENCE AND TECHNOLOGY ORGANIZATION
CENTRE FOR MARITIME RESEARCH AND EXPERIMENTATION

Reprint Series **CMRE-PR-2019-070**

Secure underwater acoustic networks: Current and future research directions

Chhagan Lal, Roberto Petroccia, Mauro Conti, João Alves

June 2019

Originally published in:

2016 IEEE Third Underwater Communications and Networking Conference,
30 Aug-1 Sept 2016, Lerici, Italy, doi: 10.1109/UComms.2016.7583466

About CMRE

The Centre for Maritime Research and Experimentation (CMRE) is a world-class NATO scientific research and experimentation facility located in La Spezia, Italy.

The CMRE was established by the North Atlantic Council on 1 July 2012 as part of the NATO Science & Technology Organization. The CMRE and its predecessors have served NATO for over 50 years as the SACLANT Anti-Submarine Warfare Centre, SACLANT Undersea Research Centre, NATO Undersea Research Centre (NURC) and now as part of the Science & Technology Organization.

CMRE conducts state-of-the-art scientific research and experimentation ranging from concept development to prototype demonstration in an operational environment and has produced leaders in ocean science, modelling and simulation, acoustics and other disciplines, as well as producing critical results and understanding that have been built into the operational concepts of NATO and the nations.

CMRE conducts hands-on scientific and engineering research for the direct benefit of its NATO Customers. It operates two research vessels that enable science and technology solutions to be explored and exploited at sea. The largest of these vessels, the NRV Alliance, is a global class vessel that is acoustically extremely quiet.

CMRE is a leading example of enabling nations to work more effectively and efficiently together by prioritizing national needs, focusing on research and technology challenges, both in and out of the maritime environment, through the collective Power of its world-class scientists, engineers, and specialized laboratories in collaboration with the many partners in and out of the scientific domain.

NOTE: The CMRE Reprint series reprints papers and articles published by CMRE authors in the open literature as an effort to widely disseminate CMRE products. Users are encouraged to cite the original article where possible.

Secure Underwater Acoustic Networks: Current and Future Research Directions

Chhagan Lal*, Roberto Petroccia†, Mauro Conti*, João Alves†
* Department of Mathematics, University of Padova, Italy
{chhagan,conti}@math.unipd.it
† NATO STO Centre for Maritime Research and Experimentation, La Spezia, Italy
{roberto.petroccia,joao.alves}@cmre.nato.int

***Abstract*—Underwater Acoustic Networks (UANs) are widely used in various applications such as climate change monitoring, pollution control and tracking, tactical surveillance and offshore exploration. However, limited consideration is given to the security of such networks, despite the fact that the unique characteristics of UANs make these networks vulnerable to various malicious attacks. In this paper, we address future aspects of how to improve security in UANs. We start by reviewing and discussing the state-of-the-art security threats for underwater networks along with their existing solutions. We then identify the open research issues and challenges in the design of secure protocols for communication in UANs. We propose innovative approaches based on node cooperation, cross-layering, software-defined cognitive networking and context-aware communication in order to effectively provision new or strengthen existing security frameworks in UANs. By using these approaches, we address the problem of detecting malicious behaviours and rogue nodes in order to address the major security issues in UANs. We also investigate the use of a covert channel based detection mechanism which needs to be considered when monitoring or deploying UANs at sea. We believe that the issues raised and future possible solution approaches proposed in this paper will greatly help the researchers contributing towards fortifying security in an inherently in-secure UAN.**

***Index Terms*—Underwater acoustic networks, security, software defined underwater networks, cross-layering, cognitive notworks, context-aware security, DoS attacks.**

I. Introduction

Underwater networks have been recognised as a key asset to support monitoring the marine environment for scientific observations, commercial exploitation and military applications. The maturity and reliability of underwater communication technologies has grown rapidly in the last few decades [1]. The commercial and research communities moved from the deployment of few underwater assets from the same manufacturer to networks composed by few tens of heterogeneous nodes, including teams of cooperating autonomous underwater and surface vehicles. Increasing the size and the complexity of the network led to the problem of efficient delivery of the data to and from the network nodes.

In the underwater environment, both radio and optical signals are greatly attenuated, and acoustics remains the main technology used for communications. Nonetheless, acoustic-based solutions suffer from long propagation delays, low data rates and several factors affecting the quality of the received signals (multipath, attenuation, etc.), which complicate the implementation of reliable networks. Given the challenges imposed by the underwater acoustic channel, it has been clear that trying to simply reuse what it has been done for the terrestrial domain is not performing as expected. Many distributed and ad-hoc solutions addressing channel reservation and message routing have been therefore proposed for UANs in the recent past. It is common understanding that there is no solution fitting all the possible scenarios, since the communication parameters (intrinsic and channel) may significantly vary in space and time.

All aspects related to security have been however marginally investigated (or not considered at all) leaving room for potential attackers, which might make a UAN unusable [2].

The properties of acoustic channels and underwater networks exposes UANs against a large array of malicious attacks. Novel simple but scalable and efficient networking security solutions have to be explored to increase the level of flexibility and adaptation currently provided. To reach this goal, and to overcome the limitations imposed by the existing monolithic integrated modems and communications stacks, a software defined networking system is needed with the support for significant cross-layering, from physical coding to routing and application. Accurate context awareness has to be built at the node and network level to forecast in real-time potential challenges and risks. In order to deploy an efficient and sustainable UAN, security, reliability and robustness of the communication have to be key metrics to be considered in the decision of the different networking protocols and node components. To the best of our knowledge, this is the first paper that proposes the inclusion of new underwater security techniques based on software-defined cognitive networks and context-aware (or context-centric) networking. In addition, we also describe the use of a covert channel as a detection mechanism for revealing the presence of UANs in the target sea area.

The rest of this paper is organised as follows: Section II describes the state of the art of security for UANs. Future research and way forward to achieve security in the underwater domain is discussed in Section III. Finally, concluding remarks are given in Section IV.

978-1-5090-2696-8/16/$31.00

II. Attacks on UANs and countermeasures

In this section, we review the existing attacks along with the effectiveness and feasibility of their corresponding defence mechanisms proposed for UANs. Instead of an in-depth survey on existing attacks and their countermeasures in UANs, which is already available in [3] [4], our focus will be on identifying limitations in current solutions and provide future directions to improve the security of UANs. In what follow we discuss potential attacks in UANs.

- The most common yet highly destructible Denial-of-Service (DoS) attack is the jamming attack performed at the physical layer. During a jamming attack, a malicious node continuously floods the channel with illegitimate signals in order to deny services to legitimate users. In [5] [6], the authors introduce and analyse the effects of jamming on UANs using real-world field tests. Due to the way acoustic signals propagate underwater, the existing approaches used in terrestrial sensor networks for jamming detection and avoidance are less effective in UANs. Spread spectrum techniques are the most used solution to counteract jamming attacks [7]. However, these are susceptible to wide band and adaptive jamming. Multi-path routing, used to avoid the jammed area of the network [8] is difficult to implement due to the typically sparse deployments of underwater sensors. Adaptive and cooperative networking solutions are therefore required to be combined with the waveform encoding techniques and improve the security of the network.
- Other widely studied attacks in UANs are wormhole, spoofing and sinkhole. In a wormhole attack, the colluding attackers create a virtual high-quality tunnel between two distant legitimate nodes making them believe they are neighbours. In [9], the author uses a multi-dimensional scaling technique, which allows each node to reconstruct the network topology up to two hops, thus preventing the wormhole attack. However, the dependency on secure distance estimation (which could be difficult in UANs) limits its applicability. Another approach to mitigate the wormhole attack is proposed in [10]. This uses the direction of arrival (DoA) of acoustic signals for secure neighbour discovery. The complexity and latency in true neighbour discovery using DoA is high, thus consuming the scarce network bandwidth and node energy.
- Location spoofing and sybil attacks are performed by impersonating false location and identity. A secure pressure routing protocol using cryptographic techniques, implicit acknowledgements, geographic constraints and randomisation is proposed in [11] to mitigate location spoofing. In [12], [13], [14], [15], the authors present a complete security suite to protect integrity and confidentiality of received messages using cryptographic based authentication, thus securing from internal attacks such as spoofing, replay and sybil. However, the use of encryption and authentication processes increases the size of the communication messages, thus reducing the limited network resources. Additionally, the network-wide security key distribution and maintenance, along with the imposed geographic constraints, present a trade-off between performance and resilience for the proposed approach. Furthermore, the scalability of such solutions are questionable due to high computational complexity, energy consumption and overhead for the one-to-one key and group key maintenance and distribution.
  In a sinkhole attack, the adversary drops all or a selection of the received data packets. To mitigate such attacks in UANs multi-level trust and reputation based solutions have been proposed [16], [17]. However, the trade-off between the estimation of accurate trust values and the introduced overhead should be considered carefully when applying these solutions.

III. Fostering security in underwater networks

In this section, we firstly identify the major challenges that should be addressed to mitigate the UAN's security issues raised in Section II. We then proceed to discuss our proposed approaches to improve the security. Based on our literature review, we condensed various attacks on different layers of the protocol stack along with their existing solutions in Figure 1. We choose the distributed surveillance or monitoring system as our reference UAN scenario. The network consists of underwater sensor nodes deployed in the presence of Autonomous Underwater Vehicles (AUVs), surface stations (static or mobile) bridging the underwater and the terrestrial networks, and a command and control station (C2S). The C2S can be placed onshore or on board of a ship. Commands and data are transmitted in and out of the network. The AUVs can be used for various purposes such as data muling, replacement of damaged sensors, filling short-term connectivity holes and adjusting the network topology to counteract to the on-going attacks.

A. Challenges and future solutions

In order to provide strong security measures against various internal and external attacks in UANs we present envisaging solutions based on software-defined cognitive networking with the support for cross-layering communications [18] [19] and context-aware networking. Additionally, we investigate detection mechanisms for UANs based on the use of covert channels. The objective is to highlight how these detection mechanisms can be explored (for both "good" and "bad" nodes) to monitor the presence of acoustic nodes or networks operating in an area of interest and to eventually lead to the the culprit of an hypothetical leak of information.

1) Software defined cognitive networking and node cooperation: The use of encryption and of more reliable and robust waveforms at the physical layer can secure the communication channel. However, as described in Section II, many other DoS attacks can be conducted to make a UANs unusable. The only way to detect and efficiently counteract several DoS attacks is through the cooperation of the network nodes. The nodes and cooperative network strategies need, however, to be able to adapt to the changes in the environment, the status of the system and the attacks, thus enabling a secure and reliable

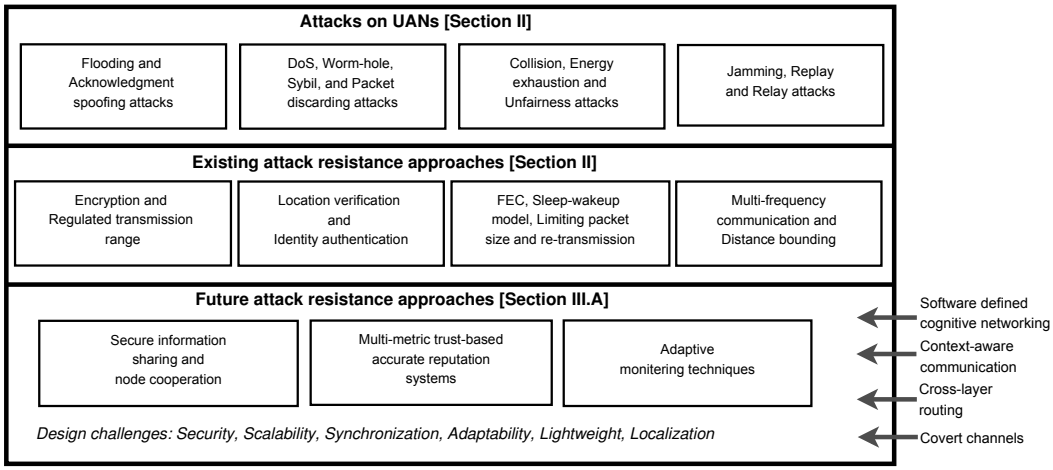

Figure 1: Security aspects on Underwater Acoustic Networks

data exchange in the best way possible. The trade-off between the required level of security and the resources available at the node and in the network needs to be considered. In order to reach this goal, the use of monolithic integrated acoustic modems and communications stacks is a significant limitation. Novel communication and networking paradigms are therefore required to increase the context awareness at the node and network level. This will help to forecast and promptly react to potential challenges and threats in the network. The use of a software defined and cognitive system with the support for a significant cross-layering interaction, from the physical to the application layer, seems to be the way forward. Separately addressing secure actions at each layer of the stack, as traditionally done in the Open System Interconnection (OSI) stack, can lead to less secure and sometimes conflicting overall strategies which can potentially result in an overall degradation of the system performance. Sharing all the relevant information across the stack would make possible to have the different layers working as a single and coordinated unit. This empowers each layer to adapt and react to the changes and attacks occurring in the network. Having such a flexible system in place would make possible the design of a cognitive component (running in each node and on the C2S) that is able to collect and process the provided cross-layer information (about the node and the neighbourhood/network), thus leading to a better picture of the status of the system. This component can then use security as a key metric driving the actions to perform in order to accomplish the required tasks, *e.g.*, channel reservation, message routing, network coding, packet fragmentation and re-assembling. Additionally, the use of this cognitive component can ensure that the decisions and actions taken at node level reflect the strategies and the needs of the overall network.

To improve the efficiency of the described software defined cognitive system, the cooperation of static and mobile nodes is a key aspect to consider. Node mobility can be exploited in a dynamic way to adapt the network topology according to the on-going attack. This would allow to avoid the presence of single points of failure and to enable efficient and energy-saving data delivery in the network. Data muling solutions can be explored to create mobile collection points, and to cover connectivity holes in the network in the presence of attacks such as jamming, sinkhole, and resource exhaustion. Through the cooperation of the network nodes it is possible to monitor and keep track of neighbour node operations when reserving the channel and relaying messages. Relevant information can be also shared across the network, if required, to increase the overall context awareness at the network level. Unexpected behaviours can then be detected. These include:

- Too many/few packets getting in/out of a node, repeated transmissions of obsolete packets or repeated transmission requests addressed to the same node (replay and resource exhaustion attacks);
- Continuous dropping of the received packets after requesting to be selected as relays (sinkhole attack);
- Fake advertising of a node as the best relay or continuous forwarding of messages through the same node(s) while other good relays are available (packet redirection);
- Nodes advertising themselves in different parts of the network (sybil and wormhole attacks).

The use of software-defined networking (SDN) paradigm to facilitate the development of next generation UANs is one of the possible solutions to dynamically detect the above mentioned malicious behaviours [20]. However, before using SDN for UANs, one should look for research challenges, such as energy-efficient routing (as sensors and AUVs have limited energy resources), and robust and fault tolerant design for control plane (as it alone is responsible for updating routing tables and enforcing security policies in the network).

2) Security in multi-metric reputation systems: In a reputation system [21], each sensor node keeps a reputation value for all its neighbour nodes based on historical information such as the success of the past transmissions. The accuracy of such systems depends on the reliability of the collected information and on the metrics used for trust estimation. During the computation and assignment of reputation values to the neighbour nodes, the following aspects should be carefully considered: unreliability of underwater channels, possible involvement of security attacks, energy consumption and node

mobility. Security attacks, such as relay and wormhole attacks, ensure that two far-away nodes falsely believe that they are neighbours. These attacks disrupt the normal working of reputation systems and create vulnerabilities. For example, a node X falsely assumes, due to the presence of an adversary, that node Y is its neighbour and select Y as next-hop for data transmission. Later, when node X monitors Y, it finds out that Y is not forwarding the received packets. Node X falsely assumes that node Y might be a selfish node and assigns Y a lower trust value in order to decrease its reputation.

The use of context-aware [22] based route discovery for multi-hop transmissions in UANs can provide resilience to relay and wormhole attacks. Since underwater acoustic sensors have a large transmission range (in the order of several kilometres), the context in the proximity of two distant nodes might not be similar in terms of depth, temperature, salinity, conductivity and other external features (such as marine life, rocks and boats). At the same time the structure of the received signal is different across various links. Due the recent advancements [23] in hardware technologies for underwater sensors, collecting the aforementioned context information is not a difficult task. Context information collected at a node can be then used to verify whether the claiming node(s) are in proximity (*i.e.* neighbours) during the context-aware route discovery phase.

This way, context-aware routing can be used to develop a secure reputation system that analyses the true neighbour behaviour and reject routes that include suspected adversary nodes. A node using the context information can check whether the neighbour's current behaviour is affected by a nearby adversary or not before assigning a reputation value.

To increase the security and accuracy of the reputation system, the use of cross-layer metrics needs to be integrated in the process of estimating trust values for neighbour nodes. This bridges the use of a context-aware network with the software defined and cognitive component. Different trade-offs have to be explored between the use of an increasing number of cross-layer metrics and the introduced overhead and delays. Unlike the reputation systems used for terrestrial sensor networks, the following metrics should be considered in UANs:

- Trust calculations for sensors as well as the data they transmit (to handle data modification attacks);
- Unique characteristics of acoustic links such as multipath structure, packet error rate or link loss rate;
- Credibility of the third party recommendation (in cases where indirect trust measurements are included in the reputation system).

3) Adaptive monitoring and secure deployment techniques: When deploying a UAN, in some cases one may want to keep the network undetected (*e.g.* military, coastguard and homeland security applications). In other cases, there is no need to remain incognito and ensuring secure communications is enough (*e.g.* scientific and industrial applications). One possible method that can be exploited for the detection of unknown UANs is the use of covert channels (i.e., leveraging the functionalities of covert channels for identifying unknown UANs). A covert channel is a communication channel that unintentionally leaks information about the primary communication system in a manner that violates the security policies of the network. The acoustic waves used in UANs have a certain impact in the environment (through sound pressure) of the operational area, thus potentially affecting the presence of marine life (*e.g.* increasing or decreasing the quantity and movement frequency) in the area [24]. Assuming the use of capable aerial unmanned drones patrolling the sea surface, one can consider the possibility to visually detect such effects without having hydrophones or instruments in water, thus possibility identifying the existence of an UAN in the area of interest.

Insecure deployment of UANs could leave potential vulnerabilities that can later be exploited by malicious nodes. An example being an adversary or a group of adversaries silently monitoring UAN communications without causing any disruption (*i.e.* eavesdropping attack). This type of attack can be accomplished, for example, by exploiting the use of fibre optic cables running on the seabed [25]. These are affected by the changes in the pressure caused by acoustic transmissions. Other potential sources of eavesdropping attacks are the monitoring observatories deployed at sea in ever-increasing numbers. It is not uncommon to re-use operational areas for experiments at sea, especially when detailed environmental data required for the analysis of the collected results are available. The presence of observatories and cables running in the areas of interest, although not intended to be used for malicious purposes, can pose a threat by enabling the collection and recording of valuable operational data for long periods of time, thus resulting in security leaks (*i.e.* replay attack). Such attacks can be addressed by avoiding the reuse of crypto-keys or shared secrets over time or masquerading those.

IV. Conclusions

In this paper, we survey the existing security attacks along with their state-of-the-art countermeasures and respective limitations. We then propose new security paradigms for detection and countermeasure malicious activities both from a generic perspective and also considering specific use-case scenarios in UANs. The main research challenges related to the cooperation of mobile and static nodes in a distributed and ad-hoc way have been addressed, together with the investigation of multi-metric accurate reputation systems, secure deployment and adaptive monitoring techniques. Possible future solutions using software-defined cognitive networks, context-aware routing, cross-layer communications and covert channel has be proposed and discussed. These research issues and the proposed future solutions remain wide open for future investigations.

Acknowledgement

Mauro Conti is supported by a Marie Curie Fellowship funded by the European Commission (agreement PCIG11-GA-2012-321980). This work is also partially supported by the EU TagItSmart! Project (agreement H2020-ICT30-2015-688061), and by the projects "Physical-Layer Security for Wireless Communication", and "Content Centric Networking: Security and Privacy Issues" funded by the University of Padua.

REFERENCES

[1] T. Melodia, H. Khulandjian, L.-C. Kuo, and E. Demirors, "Advances in underwater acoustic networking," in *Mobile Ad Hoc Networking: Cutting Edge Directions*, S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic, Eds. Hoboken, NJ: John Wiley & Sons, Inc., March 5 2013, ch. 23, pp. 804–852.

[2] E. Souza, H. C. Wong, I. Cunha, A. A. F. Loureiro, L. F. M. Vieira, and L. B. Oliveira, "End-to-end authentication in under-water sensor networks," in *Proceedings of the 18th IEEE International Symposium on Computers and Communications*, ser. ISCC'13, Split, Croazia, 7–10 July 2013, pp. 299–304.

[3] G. Han, J. Jiang, N. Sun, and L. Shu, "Secure communication for underwater acoustic sensor networks," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 54–60, 2015.

[4] H. Li, Y. He, X. Cheng, H. Zhu, and L. Sun, "Security and privacy in localization for underwater sensor networks," *IEEE Communications Magazine*, vol. 53, no. 11, pp. 56–62, 2015.

[5] M. M. Zuba, Z. Shi, P. Z., and J.-H. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," in *Proceedings of the Sixth ACM International Workshop on Underwater Networks*, ser. WUWNet'11, Seattle, Washington, USA, 1–2 December 2011.

[6] M. M. Zuba, Z. Shi, P. Z., J.-H. Cui, and S. Zhou, "Vulnerabilities of underwater acoustic networks to denial-of-service jamming attacks," *Security and Communication Networks*, vol. 8, no. 16, pp. 2635–2645, November 2015.

[7] M. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Communications*, vol. 18, no. 1, pp. 22–28, February 2011.

[8] M. Goetz, S. Azad, P. Casari, I. Nissen, and M. Zorzi, "Jamming-resistant multi-path routing for reliable intruder detection in underwater networks," in *Proceedings of the Sixth ACM International Workshop on Underwater Networks*, ser. WUWNet'11, Seattle, Washington, USA, 1–2 December 2011.

[9] W. Wang, J. Kong, B. Bhargava, and M. Gerla, "Visualisation of wormholes in underwater sensor networks: A distributed approach," *International Journal of Security and Networks*, vol. 3, no. 1, pp. 10–23, January 2008.

[10] R. Zhang and Y. Zhang, "Wormhole-resilient secure neighbor discovery in underwater acoustic networks," in *Proceedings of 29th IEEE International Conference on Computer Communications*, ser. INFOCOM'10, San Diego, CA, USA, 15–19 March 2010, pp. 1–9.

[11] M. M. Zuba, Fagan, Z. Shi, and J.-H. Cui, "A resilient pressure routing scheme for underwater acoustic networks," in *Proceedings of the 57th IEEE Global Communications Conference*, ser. GLOBECOM'14, Austin, Texas, USA, 8–12 December 2014.

[12] G. Dini and A. L. Duca, "A secure communication suite for underwater acoustic sensor networks," *Sensors*, vol. 12, no. 11, pp. 15 133–15 158, November 2012.

[13] A. Caiti, V. Calabro, G. Dini, A. Lo Duca, and A. Munafo, "Secure cooperation of autonomous mobile sensors using an underwater acoustic network," *Sensors*, vol. 12, no. 2, pp. 1967–1989, February 2012.

[14] Y. Liu, J. Jing, and J. Yang, "Secure underwater acoustic communication based on a robust key generation scheme," in *Proceedings of the 9th International Conference on Signal Processing*, ser. ICSP'08, Leipzig, Germany, 10–11 May 2008, pp. 1838–1841.

[15] G. Ateniese, A. Capossele, P. Gjanci, C. Petrioli, and D. Spaccini, "SecFUN: Security Framework for Underwater acoustic sensor Networks," in *Proceedings of MTS/IEEE OCEANS 2015*, Genova, Italy, 18-21 May 2015, pp. 1–9.

[16] A. Capossele, G. De Cicco, and C. Petrioli, "R-CARP: A Reputation Based Channel Aware Routing Protocol for Underwater Acoustic Sensor Networks," in *Proceedings of the 10th ACM International Workshop on Underwater Networks*, ser. WUWNet'15, Washington DC, USA, 22-24 October 2015.

[17] G. Han, J. Jiang, L. Shu, and M. Guizani, "An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor network," *IEEE Transactions on Mobile Computing*, vol. 14, no. 12, pp. 2447–2459, Dec, 2015.

[18] G. Toso, D. Munaretto, M. Conti, and M. Zorzi, "Attack resilient underwater networks through software defined networking," in *Proceedings of the 9th International Conference on Underwater Networks & Systems*, ser. WUWNET'14, Rome, Italy, 12-14 November 2014, pp. 1–2.

[19] J. Potter, J. ao Alves, T. Furfaro, A. Vermeij, N. Jourden, G. Zappa, A. Berni, and D. Merani, "Software defined open architecture modem development at cmre," in *Proceedings of UComms 2014*, Sestri Levante, Italy, September, 3–5 2014.

[20] I. F. Akyildiz, P. Wang, and S.-C. Lin, "Softwater: Software-defined networking for next-generation underwater communication systems," *Ad Hoc Networks*, vol. 46, pp. 1 – 11, 2016.

[21] A. Capossele, G. D. Cicco, and C. Petrioli, "R-CARP: A Reputation Based Channel Aware Routing Protocol for Underwater Acoustic Sensor Networks," in *Proceedings of ACM WUWNet 2015*, Washington DC, USA, October 22-24 2015.

[22] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, "Using contextual co-presence to strengthen zero-interaction authentication: Design, integration and usability," *Pervasive and Mobile Computing*, vol. 16, Part B, pp. 187 – 204, 2015.

[23] E. Demirors, G. Sklivanitis, T. Melodia, S. N. Batalama, and D. A. Pados, "Software-defined underwater acoustic networks: toward a high-rate real-time reconfigurable modem," *IEEE Communications Magazine*, vol. 53, no. 11, pp. 64–71, 2015.

[24] P. L. Tyack, "Human-generated sound and marine mammals," *Physics Today*, vol. 62, no. 11, pp. 39–44, 2009. [Online]. Available: http://hdl.handle.net/1912/3074

[25] V. V. Grishachev, "Detecting threats of acoustic information leakage through fiber optic communications," *Journal of Information Security*, vol. 3, no. 2, pp. 149–155, 2012.

Document Data Sheet

Security Classification		Project No.
Document Serial No.	**Date of Issue**	**Total Pages**
CMRE-PR-2019-070	June 2019	5 pp.

Author(s)

Chhagan Lal, Roberto Petroccia, Mauro Conti, João Alves

Title

Secure underwater acoustic networks: Current and future research directions

Abstract

Underwater Acoustic Networks (UANs) are widely used in various applications such as climate change monitoring, pollution control and tracking, tactical surveillance and offshore exploration. However, limited consideration is given to the security of such networks, despite the fact that the unique characteristics of UANs make these networks vulnerable to various malicious attacks. In this paper, we address future aspects of how to improve security in UANs. We start by reviewing and discussing the state-of-the-art security threats for underwater networks along with their existing solutions. We then identify the open research issues and challenges in the design of secure protocols for communication in UANs. We propose innovative approaches based on node cooperation, cross-layering, software-defined cognitive networking and context-aware communication in order to effectively provision new or strengthen existing security frameworks in UANs. By using these approaches, we address the problem of detecting malicious behaviours and rogue nodes in order to address the major security issues in UANs. We also investigate the use of a covert channel based detection mechanism which needs to be considered when monitoring or deploying UANs at sea. We believe that the issues raised and future possible solution approaches proposed in this paper will greatly help the researchers contributing towards fortifying security in an inherently in-secure UAN.

Keywords

Underwater acoustic networks, security, software defined underwater networks, cross-layering, cognitive notworks, context-aware security, DoS attacks

Issuing Organization

NATO Science and Technology Organization
Centre for Maritime Research and Experimentation

Viale San Bartolomeo 400, 19126 La Spezia, Italy

[From N. America:
STO CMRE
Unit 31318, Box 19, APO AE 09613-1318]

Tel: +39 0187 527 361
Fax:+39 0187 527 700

E-mail: library@cmre.nato.int