SCIENCE AND TECHNOLOGY ORGANIZATION
CENTRE FOR MARITIME RESEARCH AND EXPERIMENTATION

Reprint Series **CMRE-PR-2017-012**

A distributed ID assignment and topology discovery protocol for underwater acoustic networks

Roberto Petroccia

November 2017

Originally presented at:

2016 IEEE Third Underwater Communications and Networking Conference (UComms)

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.

A Distributed ID Assignment and Topology Discovery Protocol for Underwater Acoustic Networks

Roberto Petroccia
NATO STO Centre for Maritime Research and Experimentation, La Spezia, Italy
roberto.petroccia@cmre.nato.int

***Abstract*—This paper presents a new protocol to self assign node IDs in an Underwater Acoustic Network (UAN). The proposed solution, termed DIVE for Distributed Id assignment and topology discoVEry, is fully distributed and self-adaptive. While assigning the node IDs, additional information is shared to discover the other nodes in the network, the type of these nodes (static or mobile), and the number of hops to reach them. The DIVE protocol exploits link quality information to increase its reliability and robustness against message losses. The protocol performance has been evaluated under a variety of networking scenarios including node mobility, and node addition and removal. The results show that DIVE is an efficient and reliable solution for node ID assignment and network discovery, which scales with the network size in the presence of a unreliable channel.**

***Index Terms*—Underwater networks, distributed ID assignment, self-ID assignment, network discovery, topology discovery.**

I. Introduction

Underwater networks have been recognised as a key asset in a variety of underwater technology application scenarios, including environmental monitoring, eco-system analysis, and military applications [1]. In the last decade increasingly capable and reliable underwater communication technologies have been made available to users and researchers alongside the growth of the maritime robotics field. The state of the art in underwater communications has evolved from the deployment of few underwater communications assets from the same manufacturer, to that of networks composed by tens of heterogeneous nodes, including teams of cooperating autonomous underwater and surface vehicles. This trend of deploying larger and more sophisticated cooperative underwater networks is not expected to stop in the near future. In order to cooperate nodes need to communicate. Given the impairments of optical and radio propagation in water, the acoustic medium is currently the most reliable and robust channel over which to communicate underwater. At the same time, the use of acoustic transmissions in water incurs several medium-specific challenges, such as long propagation delays, low data rate, significant temporal and spatial fluctuations in terms of link reliability and symmetry.

Many solutions have been proposed in the recent past for UANs, including protocols for channel reservation, packet routing, cluster formation, node localisation and synchronisation [2]. All these solutions assume the presence of unique IDs assigned to the network nodes to support the correct exchange of messages. A possible solution to this is the use of unique addresses assigned to every manufacture underwater nodes, similar to what is done for Ethernet cards (hardware or MAC addresses). However, this approach would require a high-level of coordination in a very small commercial market, and IDs of long bit length that are impracticable because of the combination of disadvantages already outlined. Another option is the *a priori* assignment of network-wide global IDs to nodes. This would permit the reduction of the node's ID length, but it significantly couples the deployment and operational complexity with the network size. Additionally such solution would introduce the requirement for complete knowledge of all future network sizes during a given deployment, categorically excluding ad-hoc solutions.

This paper proposes a distributed and self-adaptive solution for ID assignment and topology discovery in a UAN which aims at minimising the number of bits required for each ID. To the best of the author's knowledge, this is the first study combining self ID assignment and topology discovery in UANs. The performance of the DIVE protocol has been evaluated via simulations, measuring metrics such as network reconfiguration time, packet transmissions and energy consumption. The collected results show that the DIVE protocol is an effective solution for UANs which is able to scale with the network size. It has been able to correctly perform under a variety of scenarios, including message losses, node mobility, and the ad-hoc addition and removal of nodes to the network.

The remainder of the paper is organised as follows. Previous work on assigning node IDs in terrestrial networks is summarised in Section II. Section III describes the DIVE protocol in details. Simulation results are illustrated in Section IV. Finally, Section V concludes the paper.

II. Related Works

Though distributed and ad-hoc protocols to assign node IDs in UANs are poorly explored topics, the analogous problem for terrestrial Wireless Sensor Networks (WSNs) has been investigated thoroughly. Several schemes that assign locally unique addresses in sensor networks have been studied [3], [4], [5]. Since the communication in WSNs is mostly data-centric the use of local unique IDs can be sufficient to deliver the messages to the collection point (sink). In underwater networks, however, there is usually the need to send control messages from the command and control station (C2S) to the nodes in the network, to reconfigure the sensing operations or to change the mission/tasks of mobile nodes. Similarly,

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

the network nodes may require message exchanges without passing through the C2S to support cooperative behaviours. Globally unique IDs are therefore required to support the use of unicast packets for the delivery of commands and data to the correct node. Many protocols have been proposed to assign globally unique addresses in terrestrial networks, including cluster-based solutions [6], [7] and tree-based network organisations [8], [9], [10]. As underwater networks are usually composed by both mobile and immobile nodes, the cluster-based and tree-based representations may be time variant, and the update overhead required is prohibitive in a low-data-rate network such as a UAN. Additionally, most of the proposed solutions assume a two-way interaction between neighbour nodes, while asymmetric links can be experienced overtime in UANs further increasing the introduced overhead when a two ways message exchange is required. In [11] a protocol to assign a unique IP address to a new node joining a MANET is proposed. The protocol requires that the subject MANET starts with a single node, the *initiator* node, which initially owns the full IP pool. When a node joins the network, one of the nodes already in the network segments its own IP pool and assigns half of it to the joining node. Although this solution does not assume any hierarchical organisation of the network, it requires the presence of an initiator node which knows the number of IP addresses to use. Additionally, depending on the initiator location, long delays may be introduced together with an irregular distribution of the IP pools. Recently, an address assignment protocol for UANs has been proposed in [12]. This protocol does not require any hierarchical organisation in the network, however, it assumes that a name is pre-assigned to each underwater node. A hashing algorithm is then used to convert the node name of variable length into a numeric ID.

The DIVE protocol is proposed to overcome the limitations of existing solutions. It does not require any hierarchical organisation of the network and does not make any assumption on the presence of special nodes (or roles) and information in the network. It is fully distributed and self-adaptive. No link symmetry is assumed and the effective assignment of globally unique IDs in the presence of unreliable channels is specifically addressed. During the DIVE operation, additional information is exchanged to discover the network topology and to verify that a given ID has not been duplicated in the network. The topological information can be then used to better route messages and to support cooperative behaviours in the network.

III. DIVE PROTOCOL

The protocol is composed of two main procedures that run simultaneously. The first is in charge of sharing the information required to assign the node IDs and to discover the network topology. The second procedure is required to verify that node IDs are globally unique in the network.

A. Procedure 1: Assignment and Discovery

When the network is deployed the DIVE protocol starts. Each node x generates a long random integer key K_x[1] and a timer (`Tx_Timer`) is started. The duration of the timer depends on the generated key value: the lower the key the shorter the delay. When the timer expires, the node x broadcast a `HELLO` packet which carries the following information:

$$\texttt{HELLO}_x = \langle K_x, R_x, \texttt{isMobile}_x, C_x, \texttt{LIST}_x \rangle .$$

The field K_x is the key value generated by node x; R_x is an additional random integer value (much shorter than the key value) used in *Procedure 2*. A different R_x value is generated at each `HELLO` packet transmission; $\texttt{isMobile}_x$ is a flag set to 1 if node x is mobile, 0 otherwise; C_x is a counter to track how many `HELLO` packets have been transmitted by x so far; $\texttt{LIST}_x$ is the list of contacts stored by node x. Each contact on the list refers to another node y and contains the key K_y, the latest received value for $\texttt{R}_y$, $\texttt{isMobile}_y$, and the current estimation on the number of hops to reach y.

Re-transmission: After transmitting the `HELLO` packet, node x starts a second timer (`Waiting_Timer`). When this timer expires, node x has to decide if another `HELLO` packet has to be transmitted or if the ID assignment process can start. The decision on transmitting again the node information depends on three factors: 1) If any `HELLO` packets have been received by node x; 2) presence of mismatches between the list of keys, K, stored on x and the contact list received from any of its neighbours; 3) link quality estimation.

Link quality is currently estimated by each node based on the success of recent interactions with its neighbours[2]. A probability of retransmission is then computed based on the link qualities, the number of detected neighbours, the number of times a `HELLO` packet has been already transmitted at the expiration of the `Waiting_Timer`, and a robustness value which may be imposed by the user.

Reception: When node y receives a `HELLO` packet, it stores the related data (K_x is used as the key to identify the transmitter node) and checks for the presence of new information in order to update its list of keys and the hop counts to the other nodes[3]. If new key values are detected, node y starts the `Tx_Timer` in order to then transmit an `HELLO` packet with the updated information. If the `Waiting_Timer` was running it is stopped and restarted after the packet transmission.

B. Procedure 2: Duplication Recovery

The objective of this procedure is to detect the presence of duplicate keys in order to promptly react and update the network status. When creating the `HELLO` packet for transmission, node x generates an additional random integer value (R_x), which is shorter than K_x, and adds it to the packet. A new R_x values is generated for each `HELLO` packet. Additionally, node x adds to $\texttt{LIST}_x$ the latest R_y value received by node y. Since each node x keeps track of all the R_x values it has generated, it can easily check over

[1] Assuming the use of 20 bits to generated the key, $K \in [0, \ldots, 1048575]$.

[2] If the acoustic modem provides some quality measurements of the link, these data can be integrated in the link estimation process.

[3] The hop count value is updated only for static nodes, for mobile nodes the hop count is considered undefined.

time the presence of a node z with $K_x = K_z$ but with an associated random value R_z not belonging to the set of random values generated by x. The probability to have multiple nodes generating the same key and the same ordered list of random values over time is negligible, with a proper setting of the length of the key and of the size of the random value. When a nodes detects the presence of duplicate keys, it sends a `WARNING` packet following the same procedure used for the `HELLO` packet.

$$\texttt{WARNING}_x = \langle K_x, R_x, \texttt{isMobile}_x, C_x, \texttt{LIST}_x, \texttt{DKEYS}_x \rangle .$$

The additional field $\texttt{DKEYS}_x$ contains the list of duplicate keys K detected or received by x. When a node x detects or is informed about duplicate keys, it checks if its own key is in the list of duplicate keys, generating a new one if needed. If a new key is generated, the old value for K_x is added to $\texttt{DKEYS}_x$ while the new one is stored in K_x. The transmission of $\texttt{HELLO}_x$ packets in *Procedure 1* is then replaced with $\texttt{WARNING}_x$ packets to inform the rest of network about the detected/received duplicate key(s). No further changes and extra actions/packets are required, thus limiting the overhead and delays needed to update the network status.

When the DIVE procedures end, each node has collected the full list of keys in the network and topological information. Each node is therefore able to assign a global unique ID to itself and the other nodes. The ID assignment simply involves sorting the list of keys and then assigning incremental short addresses, e.g. 1 , 2 , 3. The DIVE protocol keeps running in background to react to nodes leaving/joining the network.

Node departure: When a node leaves the network, no changes are imposed by the DIVE protocol to the node ID assignment. This is to reduce the energy consumption of the node, since it is possible to have mobile nodes leaving the network to be re-charged and then coming back. These nodes can save the current list of keys and IDs and may reuse the information on reconnection, if no changes have occurred in the meanwhile.

Node joining the network: When a new node (or more than one) is deployed in the network, it will start the DIVE protocol. A `HELLO` packet will be transmitted when the `Tx_Timer` expires or when a control/data packet is received. When receiving the `HELLO` packets, the already-present nodes go back in the DIVE mode operations collecting the new key value(s) and sharing this information with the rest of the network. New IDs will be then assigned in the network according to the new list of keys. Each node keeps track of the previous mapping between keys and IDs to then update the routing information making use of the new ID assigned to the same key.

IV. Performance Evaluation

The performance of the DIVE protocol has been evaluated through an extensive set of simulations considering single-hop and multi-hop UANs. Various metrics have been investigated to assess the effectiveness and costs to assign node IDs and discover the network topology. These metrics include:

- *Duration*, i.e., the number of seconds it needs to complete the node IDs assignment and network discovery process.
- *Energy per node*, i.e., the energy (in Joule) consumed by each node to complete the DIVE protocol operations.
- *Transmitted packets per node*, defined as the number of packets transmitted in the network by the protocol.

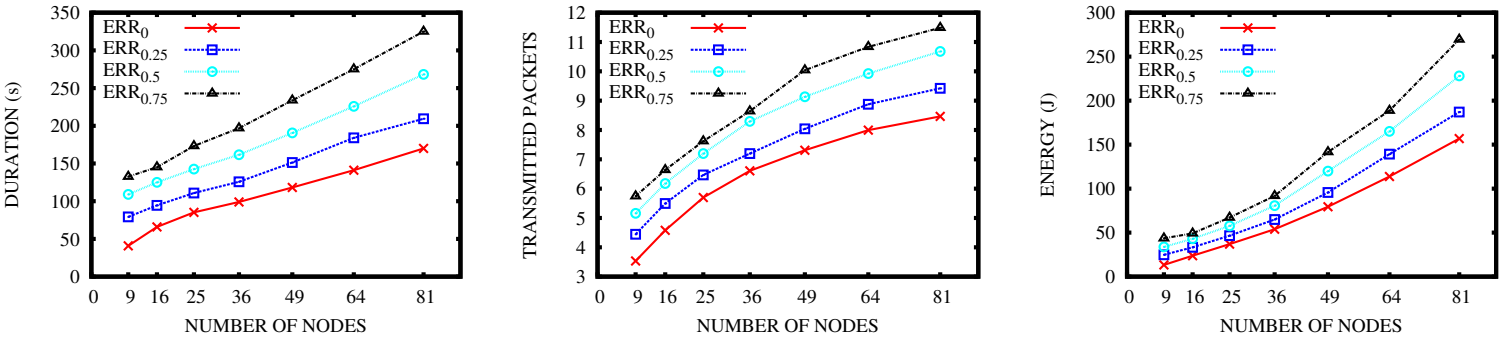
A. Simulation scenarios and settings

The DIVE protocol has been implemented in SUNSET [13], which can be freely downloaded at [14]. Various network configurations have been considered assuming a grid topology. The deployment area has been divided into $n \times n$ cells, with n varying from 3 to 9. Each cell is a square with a side of 500m. Nodes are placed randomly and uniformly within the cells (one node per cell) at different depths, ranging from 5 to 250m. The number of network nodes varies between 9 and 81, 70% of these nodes have been statically deployed while the remaining 30% is mobile. After the deployment, each mobile node starts moving within the target area using a random waypoint mobility model with a nominal speed of 2 knots. An increase in network size also increases the average number of hops, from the single-hop case ($n = 3$) to a multi-hop scenario. When the maximum network size ($n = 9$) is considered, the average number of hops is 3.5, while the maximum is 10.

To simulate the underwater acoustic channel, the SUNSET module for the Urick model [15] has been used, assuming a BPSK modulation at the physical layer. An additional packet error probability (0.25, 0.5, and 0.75) is also applied to each packet which is correctly received at the physical layer. This is to evaluate the DIVE protocol performance in the presence of unreliable channels with different errors on the direct links in the network. The SUNSET carrier sensing ALOHA protocol has been used at the MAC layer. A carrier frequency of 24kHz and bandwidth of 16kHz have been selected. The transmission power is set to 8W, while the reception power and the idle power are set to 1.3W and 0.285W, respectively. A nominal transmission rate of 7.5kbps is assumed. These setting correlate closely to the EvoLogics S2CR 18/34 commercial acoustic modem [16]. The number of bits used to generate the random key is 20, while 8 bits are used for the additional random value. The duration of the `Waiting_Timer` has been set to 30s.

B. Simulation results

Figure 1 shows the simulated performance data for DIVE using the previously enumerated parameters. For all the considered scenarios, the DIVE protocol has been able to correctly complete its task, including the case where a packet error probability of 0.75 is considered. As expected, when increasing the size of the network and the packet error probability, the time to complete the DIVE protocol operations also increases. The increase in the protocol duration is however sublinear (Figure 1a). Not assuming any special node (role) in the network, all the nodes can start operating simultaneously in different areas of the network. A similar trend can be noticed



(a) Duration. (b) Transmitted packets per node. (c) Energy per node.

Figure 1: DIVE protocol results.

on the number of packets transmitted by each node (Figure 1b). Instead of immediately forwarding any new received information, each node waits for the (`Tx_Timer`) to expire before sending a new `HELLO` packet. In this way, while waiting for the timer, more information may be received from the neighbours, merged into the contact list, and then transmitted as a single aggregated message. This helps to reduce the required medium access and the traffic load. Increasing the network size and the deployment area by 9 times, the number of packet transmitted by each node increases by 140% while the protocol duration increases by $\sim 300\%$.

The increment in the energy consumption per network size increase is however not sublinear (Figure 1c). More nodes deployed in an area induces longer lists of contacts to be shared. The size of the packets linearly increases with the size of the network, thus increasing the energy related to packet transmissions/receptions. When the network size increases more transmissions are needed to share data with the neighbours. Increasing the number of transmissions results in higher resource consumption, however more transmissions help to increase the robustness of the protocol to packet loss. In the presence of a high packet error rate, the most challenging scenario is that of fewer nodes in the network. This is evident looking at the average number of times there is a mismatch in the lists of keys, shared by the neighbours, when the `Waiting_Timer` expires. This number reduces from 1.4 to 0.65 when the network size increases from 9 to 81 nodes, with an overall reduction in the packet transmissions of $\sim 25\%$.

For all the considered simulations, the presence of duplicated keys was never encountered. In order to evaluate the performance of DIVE in this situation, the simulation was manually triggered to generate nodes with equal keys in opposite corners of the map. The DIVE protocol has been able to detect this event and to recover appropriately. An increase up to 20% (10%) has been experienced for the protocol duration (packet transmissions). A second scenario has been also considered where half of the nodes were initially deployed, while the second half joined the network in a second phase. The data collected show similar trends to the ones in Figure 1. As half of the nodes are already sharing the generated keys, the protocol duration and energy consumption are 10% lower, while 30% less packets are transmitted in the network.

In order to demonstrate the advantage of using the DIVE protocol, we have investigated the energy consumption of a monitoring network where each node has to transmits a data packet to the collection point every 30 seconds. We have compared the case where DIVE is first used to create short node IDs with the case where each node randomly chooses and uses a long ID [17]. To have a very low probability of duplicated IDs, 24 bits have been used for each long ID. Although for the assignment of long IDs no initial message exchange is required, the use of longer addresses results in adding extra bytes to each packet. When $n = 3$, using long IDs results in a higher energy consumption after ~ 4 minutes of monitoring operations, introducing more overhead than the case where DIVE is first run and short IDs are then used. This increases to ~ 60 minutes when $n = 9$. These results refer to the case where only data packets are transmitted. When assuming routing and MAC protocols making use of control packets, such as [18], [19], [20], [21], the benefit of using short IDs is more evident. Additionally, it is worth to remark that many networking protocols proposed for UANs assume some knowledge about the network topology. The DIVE protocol would provide already this information thus reducing the additional overhead introduced for the packet delivery.

V. Conclusions

In this paper the DIVE protocol has been presented to efficiently assign global unique IDs to the nodes of an underwater acoustic network. The proposed solution is fully distributed and self adaptive and it does not require any knowledge about the network, link symmetry, or the presence of special nodes. Additionally, node mobility is explicitly supported. The DIVE protocol has been designed to limit the overhead and delays introduced when increasing the size of the network with the support for built-in procedures to ensure correct operations in the presence of unreliable channels. Additional information is shared to discover the network topology and to verify that no duplicate IDs are assigned in the network. The protocol performance has been evaluated under a variety of network conditions and scenarios, increasing the network size, the deployment area, and the unreliability of network links. The collected results show that DIVE is an effective and reliable solution for node ID assignment and network discovery in UANs, scaling with network size in the presence of unreliable channels.

REFERENCES

[1] J. Heidemann, M. Stojanovic, and M. Zorzi, "Underwater sensor networks: Applications, advances, and challenges," *Royal Society*, vol. 370, no. 1958, pp. 158–175, May 2012.

[2] 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.

[3] C. Schurgers, G. Kulkarni, and M. B. Srivastava, "Distributed on-demand address assignment in wireless sensor networks," *IEEE Transactions on Parallel and Distributed System*, vol. 13, no. 10, pp. 1056–1065, October 2002.

[4] H. Zhou, M. W. Mutka, and L. M. Ni, "Reactive id assignment for sensor networks," in *Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, ser. MASS'05, Washington, DC, USA, 7–10 November 2005, pp. 1–6.

[5] M. Kim and M. W. Mutka, "Recycled id assignment for relocation of hopping sensors," in *Proceedings of the 12th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, ser. WoWMoM'11, Lucca, Italy, 20–23 June 2011, pp. 1–3.

[6] J. H. Kang and M.-S. Park, "Structure-based id assignment for sensor networks," *International Journal of Computer Science and Network Security*, vol. 6, no. 7, pp. 158–163, July 2006.

[7] R. C. Doss, D. Chandra, L. Pan, W. Zhou, and M. U. Chowdhury, "Dynamic addressing in wireless sensor networks without location awareness," *Journal of Information Science and Engineering*, vol. 26, no. 2, pp. 443–460, March 2010.

[8] J. Lin, Y. Liu, and L. M. Ni, "Sida: Self-organized id assignment in wireless sensor networks," in *Proceedings of the Fourth IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, ser. MASS'07, Pisa, Italy, 8–11 October 2007, pp. 1–8.

[9] E. Ould-Ahmed-Vall, D. M. Blough, B. H. Ferri, and G. F. Riley, "Distributed global id assignment for wireless sensor networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1194–1216, August 2009.

[10] Q. Zheng, Z. Liu, L. Xue, Y. Tan, D. Chen, and X. Guan, "An energy efficient clustering scheme with self-organized id assignment for wireless sensor networks," in *Proceedings of the 16th International Conference on Parallel and Distributed Systems*, ser. ICPADS'10, Shanghai, China, 7–11 December 2010, pp. 635–639.

[11] M. R. Thoppian and R. Prakash, "A distributed protocol for dynamic address assignment in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 1, pp. 4–19, January 2006.

[12] R. Agrawal, M. Chitre, and M. A., "Design of an address assignment and resolution protocol for underwater networks," in *Proceedings of MTS/IEEE OCEANS 2016*, Shanghai, China, April 10–13 2016.

[13] C. Petrioli, R. Petroccia, J. R. Potter, and D. Spaccini, "The SUNSET framework for simulation, emulation and at-sea testing of underwater wireless sensor networks," *Ad Hoc Networks*, vol. 34, pp. 224–238, 2015.

[14] SENSES Lab, "SUNSET: Sapienza University Networking framework for underwater Simulation, Emulation and real-life Testing," Last time accessed: April 2016. [Online]. Available: http://reti.dsi.uniroma1.it/UWSN_Group/index.php?page=sunset

[15] R. Urick, *Principles of Underwater Sound*. McGraw-Hill, 1983.

[16] Evologics, "Evologics S2C18/34 acoustic modems," Last time accessed: April 2016. [Online]. Available: http://www.evologics.de/

[17] J. R. Smith, "Distributing identity," *IEEE Robotics and Automation Magazine*, vol. 6, no. 1, March 1999.

[18] S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini, "CARP: A Channel-aware Routing Protocol for Underwater Acoustic Wireless Networks," *Ad Hoc Networks*, vol. 34, pp. 92–104, 2015.

[19] G. Toso, R. Masiero, P. Casari, O. Kebkal, M. Komar, and M. Zorzi, "Field experiments for dynamic source routing: S2C EvoLogics modems run the SUN protocol using the DESERT Underwater libraries," in *Proc. of MTS/IEEE OCEANS*, Hampton Roads, VA, Oct. 2012.

[20] C. Petrioli, R. Petroccia, and J. Potter, "Performance evaluation of underwater mac protocols: From simulation to at-sea testing," in *Proceedings of IEEE/OES OCEANS 2011*, Santander, Spain, June, 6–9 2011.

[21] C. Petrioli, R. Petroccia, and M. Stojanovic, "A comparative performance evaluation of MAC protocols for underwater sensor networks." in *Proceedings of MTS/IEEE OCEANS 2008*, Quebec City, Quebec, Canada, September 15–18 2008.

Document Data Sheet

Security Classification		Project No.
Document Serial No.	**Date of Issue**	**Total Pages**
CMRE-PR-2017-012	November 2017	5 pp.

Author(s)

Petroccia, R.

Title

A distributed ID assignment and topology discovery protocol for underwater acoustic networks.

Abstract

This paper presents a new protocol to self assign node IDs in an Underwater Acoustic Network (UAN). The proposed solution, termed DIVE for Distributed Id assignment and topology discoVEry, is fully distributed and self-adaptive. While assigning the node IDs, additional information is shared to discover the other nodes in the network, the type of these nodes (static or mobile), and the number of hops to reach them. The DIVE protocol exploits link quality information to increase its reliability and robustness against message losses. The protocol performance has been evaluated under a variety of networking scenarios including node mobility, and node addition and removal. The results show that DIVE is an efficient and reliable solution for node ID assignment and network discovery, which scales with the network size in the presence of a unreliable channel.

Keywords

Underwater networks, distributed ID assignment, self-ID assignment, network discovery, topology discovery.

Issuing Organization

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