# MOOS MIDDLEWARE AND NODE ADAPTIVITY IN UNDERWATER SENSOR NETWORKS: RESULTS FROM THE UAN11 SEA TRIAL

Andrea Caiti Dept. of Energy and Systems Engineering, Inter-university Ctr. on Integrated System for the Marine Environment, Research Ctr. E.Piaggio, University of Pisa, Pisa, Italy
Vincenzo Calabrò Dept. of Energy and Systems Engineering, Inter-university Ctr. on Integrated System for the Marine Environment, Research Ctr. E.Piaggio, University of Pisa, Pisa, Italy
Gianluca Dini Dept. of Information Engineering, Inter-university center on Integrated System for the Marine Environment, Research Ctr. E.Piaggio, University of Pisa, Pisa, Italy
Angelica Lo Duca Dept. of Information Engineering, Inter-university Ctr. on Integrated System for the Marine Environment, Interdepartmental Research Ctr. E.Piaggio, University of Pisa, Pisa, Italy
Andrea Munafò Dept. of Energy and Systems Engineering, Inter-university Ctr. on Integrated System for the Marine Environment, Research Ctr. E.Piaggio, University of Pisa, Pisa, Italy

## 1 INTRODUCTION

An underwater acoustic network (UAN) embodies a communication infrastructure with the necessary flexibility for continuous monitoring and surveillance of critical infrastructures located by the sea. Application of such networks range from environmental, climate and pollution monitoring to off-shore industry to patrol and surveillance in security systems (both military and civilian). Recent trends in underwater communication are investigated, for instance, in the special issue [1], and in [2] where an extensive list of references is given. The FP7 project UAN - Underwater Acoustic Network [3], launched in 2008 and ended recently at the end of 2011, moved within these lines, having among its goals the investigation of networked communication modalities in which mobile nodes are located in the environment in order to optimize the communication characteristics of the acoustic channel. The UAN concept is based on the idea that the protection of off-shore and coastline critical infrastructures has to be based on a multi sensor network, connected to a command and control (C2) center, which eventually integrate data coming from aerial, terrestrial, surface and underwater sensors. While the wireless connection of above water sensors is nowadays quite straightforward, collecting data from multiple heterogeneous underwater devices still requires specific approaches, in particular when some of these nodes are mounted on mobile platforms, as for example in the case of surface vessels, or autonomous underwater vehicles (AUVs) used for quick intervention as a response to possible threats. The idea is hence that of having a network which is always able to establish a path between any two nodes, so that messages travel from a source to the desired destination. In practice, this means that the communicating route may be achieved only by moving mobile nodes mounted on AUVs to positions that are acoustically reachable or to positions were the communication is more efficient. Furthermore, in operative scenarios, becomes of paramount importance the possibility of securely communicate, so that the correct data is transmitted and received by the right agents/nodes, and only among the desired group. The possibility to share in a secure way the necessary information may in fact determine the success or the failure of a mission. Listening to private messages, or modification or injection of fake data are all usual threats in communication networks. In this regard, the underwater environment poses unique challenges, and the traditional security mechanisms successfully used and implemented on radio-based network suddenly becomes infeasible, while the security solutions must be tailored according to the communication limitations of the medium. To this aim, the UAN network includes a middleware layer, namely the IS-MOOS publish/subscribe system, which allows for the smooth integration of both fixed and mobile nodes at application level, and where all the network security mechanisms, cryptography, authentication, and integrity, are confined. In this way all the system components are integrated in a modular way almost regardless from the specific network infrastructure and nodes characteristics.

This work describes solutions implemented for the integration of AUVs of e-Folaga class as mobile nodes of the UAN network, and for the inclusion of network security. Results are given of the final UAN project demonstration, UAN11, held in the May of 2011, when an underwater acoustic network composed by four fixed nodes, two autonomous underwater vehicles (AUVs), and one mobile node mounted on the supporting research vessel, was continuously operated for one week, and integrated into the UAN global protection system.

The paper is organized as follow: Section 2 describes the e-Folaga AUV and its integration as mobile node of the acoustic network. Section 3 gives a description of the IS-MOOS framework. Section 4 reports the main experimental results achieved during the UAN11 sea trial. Finally, conclusions are drawn in Section 5.

## 2 UAN MOBILE NODES: THE E-FOLAGA AUV

This paragraph gives a brief overview on the general characteristics of the e-Folaga vehicles and on the modifications of the AUVs done in order to integrate them within the UAN network. The e-Folaga is a torpedo like vehicle, consisting in two fiber-glass water-proof cylinders, which compose the main hull, and one or more additional modules that can be mounted at mid-vehicle to host a mission-driven payload (mechanical modularity). The two main cylinders are connected to two wet ends where are located jet-pumps for steering and the propeller for the surge direction. More specifically, yaw, sway and heave thrusters are distributed both fore and aft; furthermore, the forward section contains a ballast for buoyancy control. The e-Folaga trusters distribution guarantees a great amount of maneuverability and permits the vehicle motion in all directions. As an example, the vehicle is capable of moving vertically in the water column, at a desired pitch angle; a desirable property for a mobile node of a network which may need to adapt its position to follow the best acoustic channel. The addition of a new module requires mechanically splitting the vehicle to graft in the additional part. The main vehicle computer is located into the aft section and the availability and the control of the components in the fore part, has to be communicated to it through the module stack (electrical connections between sections are made through flying leads).

When at the surface, the vehicle has continuous GPS (Global Positioning System) contact and land-station contact through a multi-radio link. The land station link allows for on-line modification of the mission requirements and for almost real-time data transmission. A summary of the main technical characteristics of the e-Folaga is reported in Table 1.

To integrate the e-Folagas within the UAN network a specific payload with dedicated hardware has been realized to connect the acoustic modem to the vehicle electronics. The main hardware of the payload is represented by a PC-104 board with serial lines to communicate with the modem and with the CTD probe, which is available for continuous monitoring of the water conditions. The Ethernet line is used for communication between the board and the e-Folaga native computer. Figure 1 shows the Folaga AUVs with the UAN module mounted at mid-vehicle (and in one case, a CT probe).

From a software perspective, the payload implements a mission supervisor capable of autonomous decisions, able of interpreting and generating messages to the other network nodes, and to give commands to the vehicle native Guidance, Navigation and Control (GNC) system [4]. The mission supervisor has to handle the communication tasks at the application level, while the lower level of communication (MAC and routing) is left to the software implemented in the acoustic modem itself. In this way it is possible to integrate in a modular way all the system components regardless from the specific nature of the vehicle, of the acoustic modem and of the MAC and routing strategy of the communication network.

Figure 1: Folagas on shore; the UAN module is visible, mounted at mid-vehicle.

| Item | Description |
|---|---|
| Diameter (m) | |
| External | 0.155 |
| Length (m) | 2.222 |
| Mass (kg) | 32.0 |
| Mass variation range (kg) (assuming water density 1027 kg/m3) | 0.5 |
| Range of moving mass disp.ment (m) | 0.050 |
| Energy storage | NiMh batteries, 12 V, 45 Ah |
| Autonomy (hrs.) | 8 at full speed |
| Diving scope (m) | 0 - 80 |
| Break point in depth (m) | 100 |
| Speed | |
| knots | 2 (jet pumps) / 4 (propeller) |
| m/s | 1.01/2.02 |
| Communication | multi-radio link (when on surface) |

Table 1: e-Folaga AUV, main technical characteristics.

# 3 THE IS-MOOS MIDDLEWARE

The network middleware and application layers (including the vehicles mission supervisor) utilized IS-MOOS as their software infrastructure. IS-MOOS (Intervehicle Secure MOOS) is an extension of MOOS (Mission Oriented Operating Suite). MOOS is a publish/subscribe system for inter-process communication (IPC), which supports dynamic, asynchronous, many-to-many distributed communication [5]. Its basic functioning, usual in all pub/sub systems, relies on a *dispatcher*, which is responsible for routing messages from publishers to subscribers. Messages are routed based on their *topics*, which is an information descriptor contained in the messages themselves. Subscribers have to declare their interests in specific topics by issuing subscriptions to the dispatcher, while publishers send their messages to the dispatcher. In the case of MOOS the dispatcher is represented by a central database (MOOSDB).

In the UAN project, the MOOS system has been extended in several ways to make it more robust and able to adapt to the delays and communication uncertainty of the acoustic channel. It has been modified to allow communication between processes located on different nodes of the underwater acoustic network removing any high-level handshake between the clients and the MOOSDB. This had also allowed to reduce the communication overhead introduced by the middleware and hence to increase the bandwidth available to the applications above it. Furthermore, network security mechanisms, namely cryptography, authentication, and integrity, has been added and tailored to the limitation of the medium. To give a flavor of the work done in this regard, but without entering into technical details which would go beyond the scope of this paper, in what follows we summarize the authentication mechanism implemented. More details can be found in [6]. To increase the network security, the IS-MOOS system always authenticates messages. This, in general, would cause a severe message expansion and a consequent communication overhead. IS-MOOS features a trade-off between security and performance by using 4 bytes digests resulting from truncating the value of the real hash function. While security is directly related to the length of the digest, it can proved [6] that using such a short hash function value is not detrimental to security and, as in the case of the UAN scenario (500 bps channel with 184-bit messages), compromising it would require about 25 years of continuous trials.

The IS-MOOS system represents a key point in the UAN proposed architecture: it permits the integration of all the autonomous mobile and fixed nodes into the application level of the UAN. Through IS-MOOS, each node of the network (a client within the MOOS framework) can thus convert messages coming from other network nodes into information for the onboard mission supervisor. Vice-versa, it can translate information on the node status to messages to be transmitted acoustically to other interested readers (e.g. other network nodes for cooperative mission planning). In this sense, the IS-MOOS system realizes the concept of a network, which, being composed by autonomous nodes, adapts its behavior (i.e. topology) to tackle change in the surrounding environment (e.g. change in the communication performance).

# 4 THE UAN11 EXPERIMENT

The UAN11 experiment was the final experimental activity of the project UAN [3]. The sea trial took place, between 23 May and May 27 2011, in the Trondheim fjord, off the coast of Norway. The area was ideally suited to an acoustic network testing because of its varying bathymetry with depth going from 40m to 150m. Moreover, the fjord is a commercial area, with daily commercial and touristic routes, to test the system in operative conditions. The network (see Figure 2) was composed by up to four fixed nodes including a base station (STU), two AUVs of e-Folaga class and one additional mobile node set-up on the supporting Research Vessel Gunnerus using a transducer located at about 20 m depth. The location of the fixed nodes is reported in Table 2. The base station connected the underwater network to the land station and to a wide area network which included above sensors and nodes. The complete scenario was hence that of an integrated system of underwater, terrestrial and aerial sensors for the global protection of an asset, which, during the sea trial, was collocated with the STU.

The physical layer of the UAN network was supported on hardware provided by Kongsberg Maritime (KM) and specifically adapted to the task. The acoustic modem operates at a center frequency of 25.6 kHz, with variable bandwidth up to 8 kHz and transmission power settable to a level between 187 and 194 dB re 1 $\mu Pa@1m$. The transmission bit rate goes from 200 bps to 1600 bps using turbo coding. The modem implements, on its Digital Signal Processing (DSP) board the link and network layers of the network to implement CSMA/CD medium access control (MAC), an addressing system to support data packet switching and forwarding, retransmission operations, the FLOOD routing protocol as described in [7] and adapted to manage movable underwater nodes [8]. The network stack was completed by an IP tunneling mechanism to establish the IP connection, and by UDP as transport protocol. The communication among the nodes was achieved (network application level) through the IS-MOOS publish/subscribe system.

The UAN network was continuously operated during the five days of the UAN11 sea trial, from 23 May to 27 May 2011. During the period, the entire network stack was fully tested. Nodes were routinely added and/or removed: eFolaga AUVs were deployed within the existing fixed network, and both fixed and mobile nodes were recovered for battery recharging and then redeployed. Overall, the underwater network showed a quite impressive level of robustness in terms of capability to tackle variations in the oceanic conditions and modification in its topology. During the experiment, the Folaga AUVs were tested both as relay nodes assisting static nodes, as for example to route messages coming from the STU and directed towards the furthest node FNO2 (Figure 2), and as movable source nodes [9].

Table 2: Position of network fixed nodes

| Node | North, East [UTM32V (m)] | Lat, Lon (decimal degree) | depth (m) |
|---|---|---|---|
| STU | 7035949,14; 585473,73 | 63,44171873; 10,71354497 | 90.3 |
| FNO1 | 7036078,29; 585562,49 | 63,44285603; 10,71539267 | 96 |
| FNO2 | 7036552,58; 586085,85 | 63,44698453; 10,72613567 | 39 |
| FNO3 | 7036342,20; 585455,33 | 63,44524920; 10,71338701 | 98 |

The channel conditions were very unstable, and the communication performance quite variable. Usually 500 bps data rate was used with success in the early hours of each day, but 200 bps was often necessary, especially in the afternoon. Partial explanation may be found in the fresh water coming from rivers and rain, and in the persistent presence of wind. Figure 3 shows Sound Speed Profiles (SSP) and salinity profiles measured in the area on 25 May 2011. It is visible the presence of more fresh water in the upper layers. Packet loss, at application level, varied between 0-68% approximately, and the Round Trip Time (i.e. end-to-end delay, back and forth) went from 7s to 240s. Both parameters strongly related to the relative locations between the nodes and to the mobile nodes movement. Note that if a packet was lost in the water channel due to noise or collisions, or signal fade, the KM modem would attempt retransmission up to three times before stopping any further attempt with that packet. Large delays were typically due to queue backlog (new ping packets fed into the system before the former was finished, or MOOS data traffic simultaneously with ping traffic) which can happen in the KM modem.

The first two days of the experiment were, for the most part, devoted to the network setup and to test the lowest levels of the UAN, from the physical transmission up to the MAC and routing layers. Multi-hop was successfully tested with the mobile nodes acting as relays, usually between the STU and the furthest node, FNO2. Between 23 May and 24 May 2011 IS-MOOS was used in limited periods of time, mainly to test its integration with the lower level components, whereas it was used continuously between 25 May and 26 May 2011. Network security was activated on 26 May 2011, at 3.14pm and left on from that moment on. Figure 4 shows a comparison between the network Average Delivery Ratio (ADR) for two different nodes, without security features and with cryptography, integrity and authentication services enabled. The ADR is defined as the average ratio between the number of received messages by a node and the number of sent messages to that node. It is clear from the picture that when the security was activated the network was subjected to a ADR decrease of 8%. This decrease was due to two concurrent effects: a) the message expansion caused by the authenticator which in turn increases the probability of packet loss; b) a decrease in the acoustic communication conditions. Since these two effects are strictly interleaved, it is not possible to separate the specific weight of each of the two components in the mix. However, the ADR decrease is sustainable and the effect of the use of network security appears not to be critical with respect to the decrease in performance due to the degradation of the communication channel.

On 27 May 2011, the UAN network was integrated into the global protection system. In this case, the two e-Folaga AUVs were used as active surveillance assets, and kept mostly on surface, but with just acoustic communication available for messaging with C2. Figure 5 shows the network nodes and the AUV trajectories in latitude and longitude during one of the tested intrusion simulations. The AUV was put in the water at about 4.10pm, when it received a first mission to reach $WP1$. At 4.30pm an intrusion was detected by FNO2 at location $OBJ_1 = (63,448914; 10,712293)$, and communicated via UAN to the C2. As a response, the C2 sent the AUV to location $OBJ_1$ for further investigation. When the vehicle reached the point, it found itself out of the network, without acoustic connectivity with the remainder nodes. For this reason, the mission supervisor onboard the vehicle autonomously planned a new mission to move the vehicle closer to the STU, where it was able to re-establish the connection. With the vehicle again in the network, the command and control was able to take over its control to request a new mission (manually aborted on the spot to proceed with other communication tests and hence not shown in the picture).

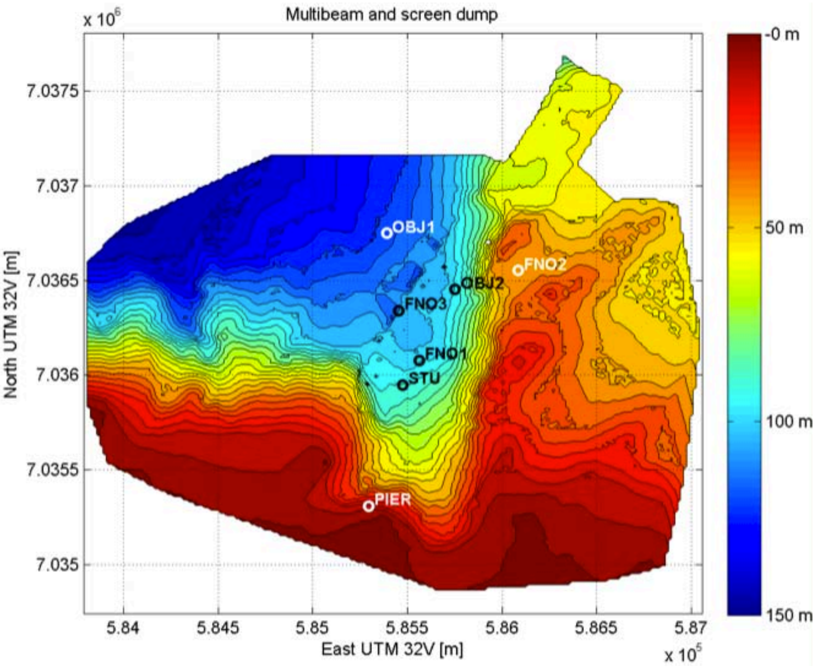

Figure 2: Test area during UAN11 experiment activity. The network topology is superimposed on the bathymetric lines of the area. The STU node represents the UAN base-station; FNO1, FNO2, FNO3 are the three fixed nodes; OBJ1 and OBJ2 indicate the locations of simulated intruders used for testing the underwater network for surveillance. PIER represents the UAN land station.

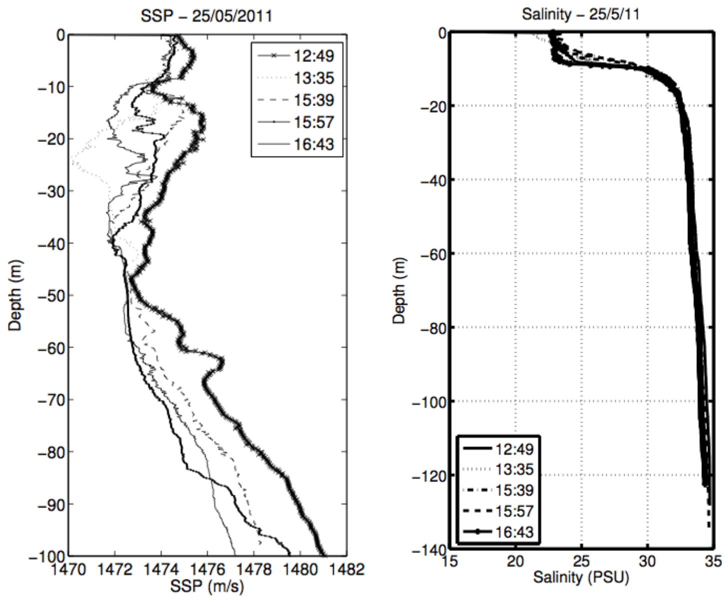

Figure 3: Sound speed profiles (left) and salinity profiles (right) measured on 25 May 2011.

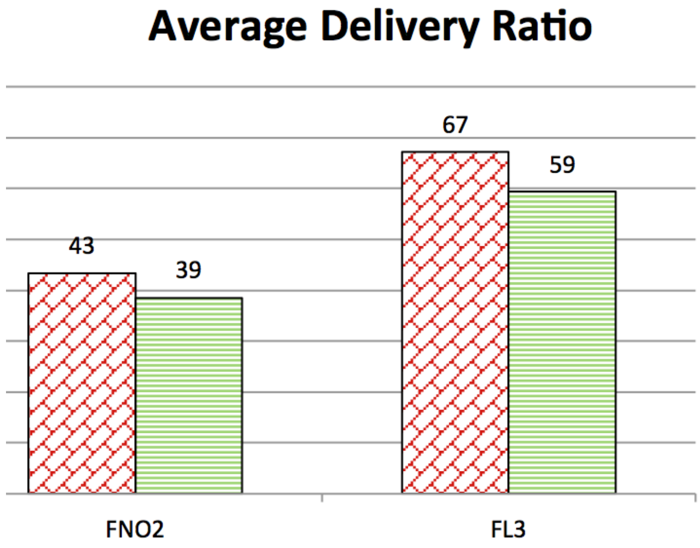

Figure 4: Average Delivery Ratio (ADR) performance. When the security was activated there was a decrease of 8% in the ADR. The decrease was due to two concurrent conditions: a decrease in the acoustic channel and in the message expansion due to the authenticator. Even though, at the current stage, we are not able to separate the two contributions, the ADR decrease is sustainable and the effect of the use of network security appears not to be critical.

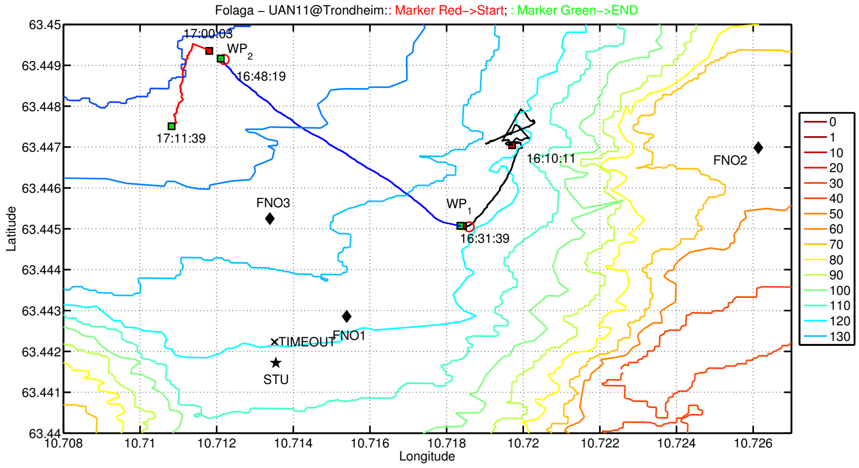

Figure 5: Folaga path during the experimental activity on May 27. In the first part of the day the vehicle was acoustically controlled by the UAN command and control center ($c^2$) to proceed to deeper investigation in an area where an intruder was detected. However, the $c^2$ moved the vehicle too far from the network where it lost the connectivity. As soon as the mission supervisor detected such a condition, it autonomously planned a new mission to move the vehicle towards the high value asset (closer to the remaining nodes of the network) where it could re-enter the network.

# 5 CONCLUSIONS

This work presented the integration of AUVs, namely the e-Folaga vehicles, as mobile nodes of an underwater network. The presence of such vehicles allowed for the network adaptation (e.g. topology) to the oceanic variations. To allow the integration of fixed and mobile nodes at application level the IS-MOOS middleware was presented. The IS-MOOS system modifies the MOOS framework to tackle the difficulties of the acoustic communication. Furthermore, it includes network security mechanisms to enhance the security level of the underwater network without being detrimental to the communication performance. The paper reports experimental results achieved during the UAN11 experimental activity of the Project UAN, held in the Trondheim area, Norway in May 2011.

# ACKNOWLEDGEMENTS

The work presented in this paper was partially funded by the European Union, 7th Framework Programme (FP7), under project Underwater Acoustic Network - UAN, Grant n. 225669.

# REFERENCES

1. J. Heidemann, U. Mitra, J. Preisig, M. Stojanovic, M. Zorsi, and C. L. (Eds.). Special issue on underwater wireless communication network. *IEEE Journal on Selected Areas in Communication*, 6(9), 2008.

2. M. Chitre, S. Shahabuden, and L. Freitag. Recent advances in underwater acoustic communication and networking. *IEEE Journal on Selected Areas in Communication*, 6(9), 2008.

3. The uan underwater acoustic network - project web site, 2011. ”Retrieved December 12, 2011, from http://www.ua-net.eu”.

4. A. Caiti, V. Calabrò, G. Dini, A. Lo Duca, and A. Munafò. Secure cooperation of autonomous mobile sensors using an underwater acoustic network. *Sensors*, 12(2): pp. 1967–1989, 2012.

5. Oxford Mobile Robotics Group. The moos cross platform software for robotics research. *http://www.robots.ox.ac.uk/ mobile/MOOS/wiki/pmwiki.php*.

6. G. Dini and A. Lo Duca. A cryptographic suite for underwater cooperative applications. In *IEEE International Symposium on Computers and Communications (ISCC'11)*, pp. 1–6, 2011.

7. H. Rudstad. A lightweight protocol suite for underwater communication. In *International IEEE Conference on Advanced Information Networking and Applications*, 2009.

8. T. Husoy, M. Pettersen, B. Nilsson, T. berg, N. Warakagoda, and A. Lie. Implementation of an underwater acoustic modem with network capability. In *Proc. IEEE Oceans Europe*, 2011.

9. U. Vilaipornsawai, A. J. Silva, and S. M. Jesus. Underwater communications for moving source using geometry-adapted time reversal and dfe: Uan10 data. In *Proc. IEEE Oceans Europe*, 2011.