Mobile underwater sensor networks for protection and security: field experience at the UAN11 experiment

Andrea Caiti
Inter-university Ctr. on
Integrated Systems for the Marine Environment
Research Center "E.Piaggio"
University of Pisa
Pisa, Italy, 56127
caiti@dsea.unipi.it

Vincenzo Calabrò
Inter-university Ctr. on
Integrated Systems for the Marine Environment
Research Center "E.Piaggio"
University of Pisa
Pisa, Italy, 56127
v.calabro@dsea.unipi.it

Gianluca Dini
Inter-university Ctr. on
Integrated Systems for the Marine Environment
Research Center "E.Piaggio"
University of Pisa
Pisa, Italy, 56127
dini@iet.unipi.it

Angelica Lo Duca
Inter-university Ctr. on
Integrated Systems for the Marine Environment
Research Center "E.Piaggio"
University of Pisa
Pisa, Italy, 56127
loduca@iet.unipi.it

Andrea Munafò
Inter-university Ctr. on
Integrated Systems for the Marine Environment
Research Center "E.Piaggio"
University of Pisa
Pisa, Italy, 56127
munafo@dsea.unipi.it

Abstract

An underwater acoustic network (UAN) represents a communication infrastructure that can offer the necessary flexibility for continuous monitoring and surveillance of critical infrastructures located by the sea. Given the current limitation of acoustic-based communication methods, a robust implementation of UANs is still an open research field. The FP7 UAN project addressed such a problem, and it reached the integration of a mobile underwater sensor network within a wide-area network, which included above water and underwater sensors, for protection and security. In this work, we give details on specific solutions chosen, in particular for the upper-layers of the UAN, with focus on the integration of autonomous underwater vehicles (AUVs) as mobile nodes of the network, and on the inclusion of network security mechanisms. The AUVs were used both as movable communication nodes and as mobile assets of the underwater protection system, acoustically controlled by the command and control center to respond against intrusions. The paper describes how the algorithms and solutions have been implemented and discusses their performance in the field. Results are given of the final UAN project sea trial, UAN11, held in the May of 2011 in Norway. During the UAN11 experimental activities an underwater acoustic network composed by four fixed nodes, two autonomous underwater vehicles, and one mobile node mounted on the supporting research vessel, was continuously operated and integrated into a global protection

system. In this article the communication performance of the network are given in terms of round trip time, packet loss, and average delivery ratio.

1 Introduction

The increased interest in ocean natural resources has produced an increasing number of infrastructures to be located by the sea. New generation of wave-based power plants have been recently tested, not to mention the renewed tendency to push the exploitation of deep water oil and gas drills to tackle the exhaustion of grounds wells. These new ocean-based installations create new and great economic opportunities as they pose new challenges for their protection. Their location, usually far away from the coast; their exposure against intrusions or natural disasters (such as earthquakes, hurricanes, etc.); their high structural complexity, with many moving underwater and floating parts, make the security issue of such vital areas particularly delicate requiring an integrated approach from air coverage to underwater defense. It is clear, that in such scenarios, requirements such as flexibility, rapid reaction, resilience, fast deployment (possibility to plug and play new components), high level of automation and modularity play a key role. In this regard, the research for security has been so far concentrated on the optimization of fixed sensors to guarantee the best static anti-intrusion configuration (Becker et al., 2008). As a recent example, in (Caiti et al., 2012b), a software simulator is used to determine the deployment of underwater sensors. The protection system can include unmanned surface vessels but the skeleton of the monitoring system is only composed by fixed sonars or magnetometers. Of course, the presence of mobile nodes or agents adds an enormous amount of flexibility as it would permit the system online adaptation to the variation of the environment. This becomes of paramount importance in the underwater domain, characterized by very variable conditions; an anti-intrusion system optimized for a given environment may become useless when the oceanic conditions vary, e.g. presence of rain, temperature changes, etc. One of the first at sea experiment of adaptive behavior for AUVs is described in (Hamilton et al., 2010), with an explicit reference to the antisubmarine warfare. The AUV represented the entire surveillance system and no cooperation with additional sensors was included. Of course, when several mobile and fixed nodes cooperate to reach a common goal, the communication infrastructure becomes of key importance. While it may sound a convincing solution that fixed sensors can be cable-connected with each-other and with land-stations, through high-bandwidth and low delays communication links, when moving assets are included in the system, going wireless remains the only option. In this case, even more problems arise with respect to the terrestrial case (Akyildiz et al., 2005). The physics of acoustic propagation, the main mean of underwater communication, is strongly dependent on the specific environmental conditions, and during the life of the network each node can experience abrupt changes in the channel, with a consequent variation in communication performance. Acoustic communication is severely band-limited and range-limited. Sudden reduction of the channel capacity and bandwidth, or even a temporary loss of connectivity are frequent conditions for underwater communications (Stojanovic, 2007; Caiti et al., 2010), influencing the node ability to continue its mission.

Given the current limitations of acoustic-based devices, a robust implementation of underwater acoustic networks (UANs) is still an open research field. An interesting overview of recent protocols for underwater networks is provided in (Pompili and Akyildiz, 2009), where the main advantages and disadvantages of various network designs are pointed out. In this context, the FP7 UAN project (UAN, 2011) was aimed at conceiving, developing and testing at sea an operational concept for integrating in a unique communication system submerged, surface and aerial sensors with the objective of protecting off-shore and coastline critical infrastructures. The UAN project ended in 2011 with the UAN11 sea trial, where many of the previously described difficulties were overcome and the complete integration of mobile agents/sensors within a UAN for critical infrastructure protection was demonstrated. Some of the specific design solutions of the implemented network are in agreement with the results reported in (Pompili and Akyildiz, 2009) (e.g. MAC), others, as the routing level, followed different approaches. Independently of the particular architecture chosen, however, it is important to underline, that all the available technologies for underwater networking, suffer in some way or another of limitations (e.g. too much communication overhead, reliability, etc.). As a result, while the UAN architecture was based on known protocols and technologies, the novel result lays in its operative

deployment, as a robust system able to work continuously at sea for five days. While some specific choices may suffer of the limits pointed out in (Pompili and Akyildiz, 2009), the use of known solutions made the UAN realizable, and allowed to learn in the field lessons, identifying weak points and improvable aspects for future research.

It is important to stress that communication not only is the simple sharing of information. In operative scenarios, it becomes a key issue the ability to securely communicate, so that the correct data is transmitted and received by the right 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 the mission as a whole. Listening to private messages, or modification or injection of fake data are all usual threats in communication networks, and they become even more critical in the context of a distributed cooperation of autonomous agents/nodes for surveillance applications. Cooperation for protection may be achieved only when all the components receive the expected data from the legitimate peers. Underwater communication introduces peculiarities also as far as network security is concerned. In contrast to traditional wired networks, an adversary equipped with an acoustic modem can easily eavesdrop as well as modify and insert fake messages. Furthermore, the variability in communication performance together with bandwidth and range limitation makes the simple adaptation of traditional security solutions (e.g. digital signatures) practically infeasible. In this regard, the approach proposed in this work constraints all the protocols for the protection of the communication at middleware level of the acoustic network. To the best of our knowledge, the only middleware already available for UANs is Seaware (Marques et al., 2006b). Seaware is a publish/subscribe (pub/sub) system that has the advantage to be adaptable to both radio-based and acoustic communications, but it directly requires access to the node transmission devices, without any intermediate network layers, such as transport or routing, and hence reducing the network modularity and flexibility. Furthermore, it does not include any form of network security.

To sum up, the UAN11 network was composed by up to four fixed nodes, two autonomous mobile nodes (AUVs of Folaga class (Caffaz et al., 2010)) and one additional node mounted on the supporting research vessel. Each node implemented the network architecture depicted in Figure 1: the physical layer was represented by the acoustic modems built by Kongsberg Maritime (KM) which was capable of transmitting up to 500bps and which also implemented the MAC protocol, the routing layer and multi-hop strategies. The network architecture was hence completed by the implementation of a tunneling mechanism to establish the IP connection, by the use of UDP as transport protocol and finally, as middleware/application level, by the use of a version of the MOOS (Mission Oriented Operating Suite) pub/sub system (Newman, 2012; Benjamin et al., 2009), modified to include network security mechanisms. MOOS represented also the basic infrastructure for the software onboard the AUVs. The acoustic network was finally integrated into a global protection system, called Archimede (Casalino et al., 2010), which combined into a unique system, above water and underwater protection sensors (e.g. cameras, radars, etc.).

The paper is organized as follows: Section 2 gives an overview of the UAN11 sea trial, describing the equipment and algorithms used. In Section 3 the figures of merit used to evaluate the communication are described. Section 4 shows results from the sea trial, and comments are made on expected and obtained results. Section 5 draws conclusions, and Section 6 concludes the article summing up the lessons learned and suggesting some future improvements.

2 Description of the UAN11 sea trial

The UAN11 experiment was the final experimental activity of the project UAN (UAN, 2011). The sea trial took place, between 23 May and May 29 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. Our primary platform of operation was the Gunneurs Research Vessel of the Norwegian University of Science and Technology (NTNU). The fixed nodes of the network

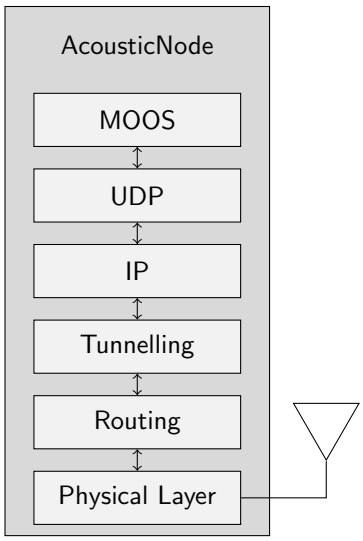

Figure 1: UAN network layers.

were deployed form Gunneurs and left in place for three days of continuos operation, and then recovered for battery recharging and re-deployed for the remaining period. The AUVs were deployed either from rubber boats or from Gunnuers. The goals of the experiment included a great deal of testing and data collection. Its main objectives, however, were to demonstrate the acoustic network functionalities and the integration of the underwater mobile sensors into the global protection system.

Figure 2 shows the network set-up superimposed on the bathymetric lines of the area of the sea trial. The underwater network was hence integrated into the air/land security system Archimede of the UAN partner Selex. The command and control center was located on shore, close to the pier.

The envisaged UAN scenario consists of (see Figure 3):

- A land station which acts as a Command and Control (C^2) center, for the physical defense of a critical infrastructure;
- A terrestrial/air protection system controlled by the C^2 and composed by fixed and mobile sensors;
- An underwater base station wired to the shore with a high bandwidth link. This station represents the connection between the above and below water environments; for this reason this element is both a part of the acoustic network and of a traditional wired communication infrastructure;
- Fixed and mobile nodes (n) acoustically connected in an underwater network which includes the base station. Each node is equipped with an on board sonar for intrusion detection and with an acoustic modem for communication purposes.

One of the critical aspects in this regard, is related to the integration between such different systems, which include above water and underwater components. In the case of the UAN system, this integration has been realized using two basic components or network layers: the Internet Protocol (IP), which permits to create a standard interface towards the higher-layers of the network, and on the use of a publish/subscribe system to abstract from the specific characteristics of the components. In the remainder of the paper we focus on the middleware and application level of the UAN concept, and we assume the presence of a reliable network able to support the physical communication. More details on the UAN lower level hardware can be found in (Husoy et al., 2011).

The following sections describe the experimental equipment, the node control and communication algorithms used during the sea trial.

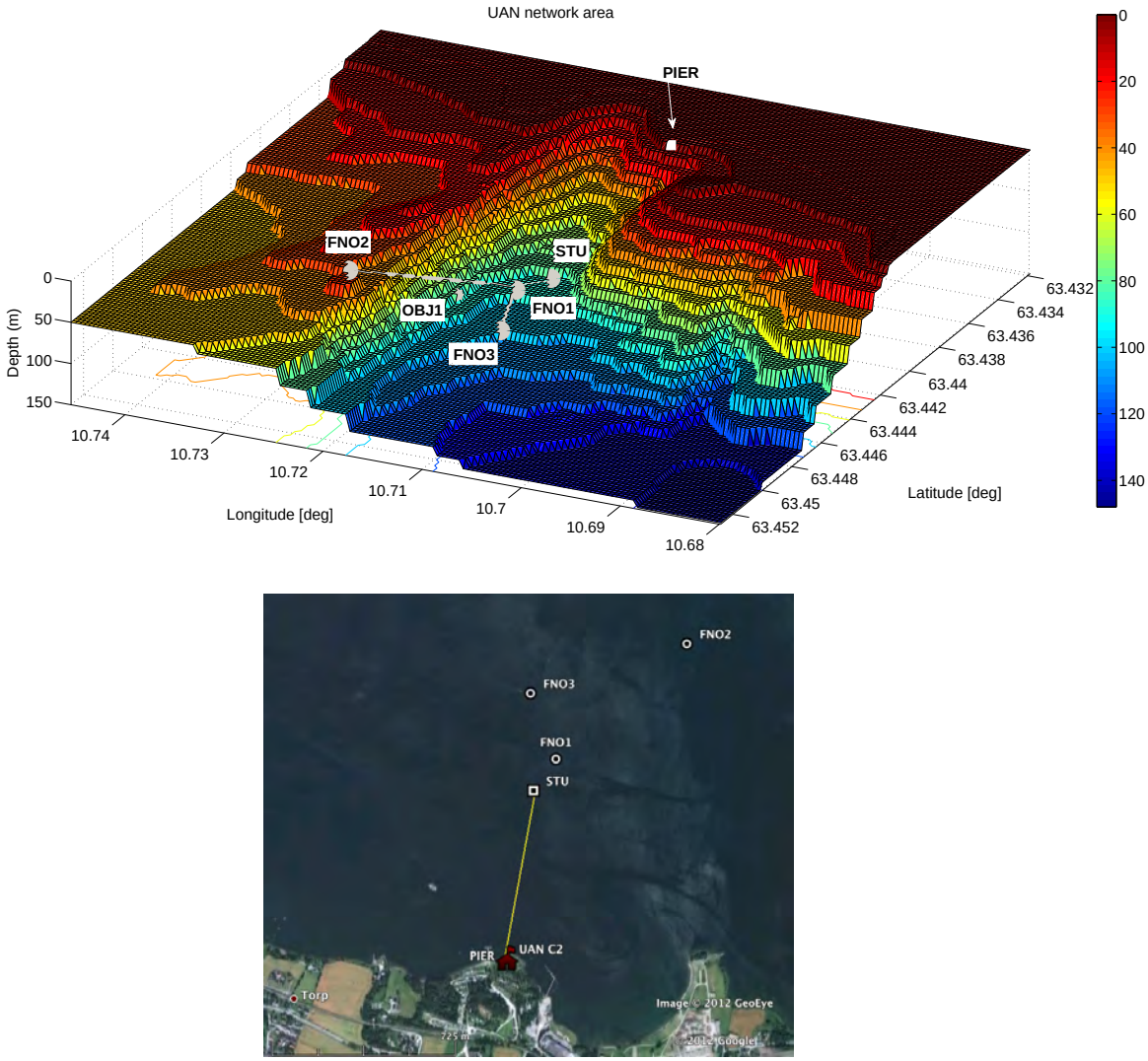

Figure 2: UAN11 experimental area. **Top:** network geometry shown on bathymetric contours. STU is the UAN base station. FNO1, FNO2 and FNO3 are the fixed nodes, OBJ1 is the location of a simulated threat. The gray lines connecting the nodes represent the shortest part between two nodes and are shown only to indicate the distance (i.e. they are not representative of the network topology). PIER represents the location of the UAN command and control center placed on shore. **Bottom**: aerial overview of the UAN area. The path of the cable, which links the underwater network to the terrestrial part is highlighted.

2.1 Equipment

2.1.1 The eFolaga AUV

The mobile node of the acoustic network was the eFolaga AUV modified to accommodate the KM acoustic modem. The eFolaga 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. The two main cylinders are connected to two wet ends where are located jet-pumps

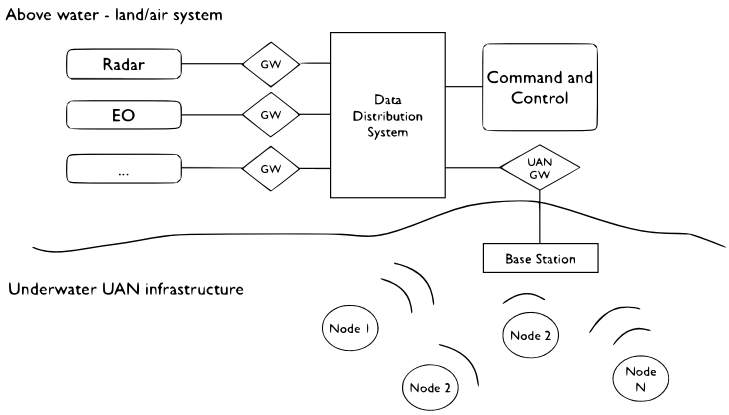

Figure 3: Conceptual overview of the UAN scenario: integration of above water and underwater systems.

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 eFolaga 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). Eight power conductors have to be carried through, to permit the bow and stern sections to operate. Of these, the module may tap into four: a common high-current Analogue Ground Return Line, +12 VDC Power Supply Line and a +12VDC Power Demand Line together with a low-current Digital Ground Return Line. The Demand Line supplies power to start up or shut down the module stack under control of the vehicle's computer. Modules may draw up to 100 mA from the Power Supply Line to power communication hubs, enable sleep modes, etc. Maximum peak current draw by a module from the Power Demand Line during a mission is 8 Amps, with a maximum total power consumption from this line of 100 Whrs during a mission. In addition to the power lines, the module stack is also required to carry through USB and Ethernet (100Mbps) connectivity from the aft section for any module that may need it.

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 eFolaga is reported in Table 1.

To integrate the eFolagas within the UAN network a specific payload with dedicated hardware (Table 2) 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 eFolaga native computer. Figure 4 shows the Folaga AUVs with the UAN module mounted at mid-vehicle (and in one case, a CT probe). Figure 5 shows the AUV deployment from Gunneurs during one of the trials.

Figure 4: Folagas on shore; the UAN module is visible, mounted at mid-vehicle.

2.2 Network base station and fixed nodes

The remaining nodes of the network were composed by a Subsurface Telemetry Unit (STU) and by underwater Fixed Nodes (FNOs). The STU represented the UAN base station and it was cable connected to shore with a high-bandwidth, no delay link, to integrate the acoustic part into the wide area network. On the acoustic side, it was equipped with the KM modem, with a vertical hydrophone array for unidirectional high bandwidth communication, and with a thermistor chain to measure the vertical temperature distribution. The STU is depicted in Figure 6, during a communication test on Gunnerus deck before deployment at UAN11. Three FNOs were used during the sea trial, with one of them (FNO3) only implementing the lowest layers of the network (physical, MAC, routing). Each FNO was equipped with an acoustic modem and with a vertical chain of thermistors similar to the one installed on the STU. The deployment of one of the FNO during the sea trial is shown in Figure 7. Further information on the STU can be found in (Zabel et al., 2011), while the FNOs will be treated in details in a separate paper.

2.3 Algorithms and software implementation

2.3.1 eFolaga mission supervisor

From an architectural perspective, the goal is that of implementing a mission supervisor capable of interpreting and generating messages to the other network nodes, and to give commands to the vehicle native Guidance, Navigation and Control (GNC) system. The approach followed is the *back-seat driver* paradigm, pioneered by the MIT group and co-workers (Balasuriya et al., 2009), (Eickstedt and Sideleau, 2008), (Benjamin et al., 2010): the mission supervisor must be able to take decisions and give high level commands to the native GNC vehicle system, which is the sole responsible for the low-level execution of the commands. Similarly, the supervisor has to handle the communication tasks at the application level, while the lower level of communication is left to the software implemented in the acoustic modem itself. In this way, conceptually depicted in Figure 8, 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. The Folaga mission supervisor is divided in different modules, called virtual bots, each of which is assigned to a specific task, and which is independent from the others as long as it shares a common interface to exchange data. Each virtual bot has its own input, which is dependent on the task it has to perform (e.g. the communication bot receives inputs from the acoustic modem) and produces an output towards a *central or decision bot*, which can be thought as the commander of the vehicle. The central

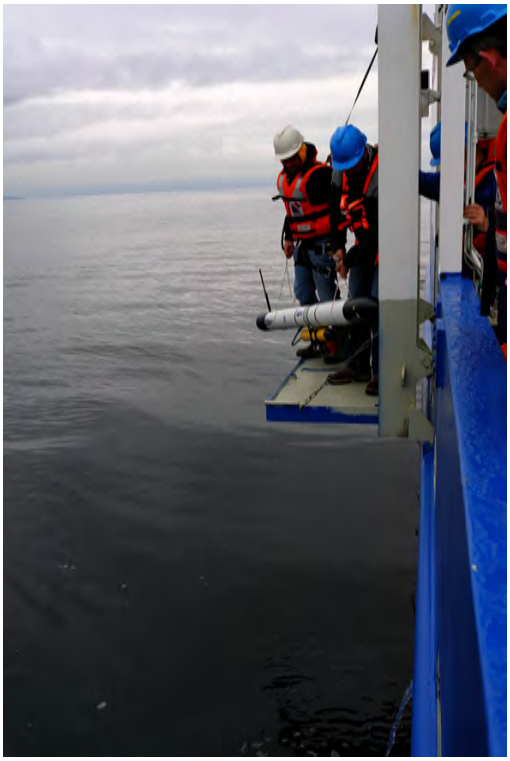

Figure 5: Folaga AUVs deployed from Gunnerus during the UAN11 experimental activities.

bot decides the next step of the mission depending on the user requirements and on the basis of the output produced by the other modules. The decision bot of the mission supervisor is implemented as an event-driven Mealy finite state machine, which generates an output based on its current state and input. Each one of the states of the machine is related to a desired mission task to be executed by the Folaga vehicle (e.g. Navigation task), or a task to be executed by a specific module of the system (e.g. the MOOS pub/sub system to send a specific acoustic message), or a waiting condition. One of the most critical part in the architecture described is represented by the interface between the mission supervisor on the payload computer and the eFolaga existing software. Two specific modules of the mission supervisor, Folaga Controller and Radio Controller, are dedicated to this task and each one of them has a counter part on the vehicle. Figure 9 shows the block diagram of the main processes running on the AUV. In particular:

- The Folaga Controller connects to a dedicated process (Payload Control Server) on the eFolaga. It is responsible for the communication between the Folaga Control System and the mission supervisor (e.g., communication of mission commands, errors, etc.).
- The Radio Controller represents the radio operator of the payload, as it connects to the Radio Modem Client on the eFolaga. It is responsible for receiving user commands when the eFolaga is on surface and to transmit logs and requests from the mission supervisor. The availability of the radio to the mission supervisor permits a real-time monitoring of the mission.

Communication at the mission supervisor level is handled through the MOOS system as described in the next section.

Finally, a dedicated *cooperation module* is responsible for the management of the cooperation with the other vehicles and fixed nodes of the network. Each agent, on the basis of the information received acoustically from its teammates (e.g. location), and on the basis of the environmental measurements periodically performed

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 displacement (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: eFolaga AUV, main technical characteristics.

Item	*Description*
CPU	1GHz, VIA EDEN, Ultra Low Voltage
DRAM	1GB, DDR2, 533/400 on SO-DIMM socket
Chipset	VIA CX700M
Serial ports	1 RS232 Full modem 1 RS232FM/422/485 Configurable
USB ports	2 x USB 2.0
Hard disk	4 GB Internal Flash Disk

Table 2: Payload hardware: main board characteristics

or transmitted by other nodes, is able to autonomously adapt its position to the specific communication and detection performance encountered as its mission proceeds. The cooperative algorithm is based on distributed decisions and each vehicle has to take individual choices to achieve the final goal, handling situations where it is completely disconnected from the network. From the mission supervisor standpoint, the presence of a cooperative module does not poses addition complexity as its output is utilized by the decision module in composition with the user requests and the output coming from the other modules. Specifically, the decision bot uses the commands coming from the cooperative module if no other commands from the C^2 are scheduled to be executed. We do not go further with the description of the cooperative algorithm as it would go beyond the scope of this work; however, more information on its theoretical aspects can be found in (Caiti et al., 2012a) for the area coverage problem, and in (Munafò et al., 2011) for cooperative explorations of marine areas.

2.3.2 IS-MOOS: autonomous node integration into UAN

Real world integration and distributed application development for underwater acoustic networks is quite a difficult task. However, an appropriate middleware may make application development easier, by providing common programming abstractions, by masking the heterogeneity and the distribution of the underlying hardware and operating systems, and by hiding low-level programming details (Bernstein, 1993). In underwater acoustic networks, the MOOS middleware has gained great popularity (Benjamin et al., 2009; Benjamin et al., 2010). In short, MOOS is a publish/subscribe system for *intra-vehicle* inter-process commu-

Figure 6: STU during a communication test on Gunnurus deck before deployment. The two yellow cylinders are the KM modems, of which, one is the STU's and the other is for testing. The grey box contains the STU electronics. It is also visible, in the photo, the blue cable used to connect the STU to shore, the black thermistor chain and the hydrophone array.

nication (IPC), which supports dynamic, asynchronous, many-to-many distributed communication (Oxford Mobile Robotics Group, 2012). In MOOS a *dispatcher* is responsible for routing messages from *publishers* to *subscribers*. Messages are routed according to their *topics*, which are message descriptors contained in the messages themselves. Subscribers declare their interests in specific topics by issuing *subscriptions* to the dispatcher, while publishers send the dispatcher messages belonging to the various topics. In the MOOS parlance the dispatcher is called MOOSDB.

The publish/subscribe paradigm is particularly suitable for distributed cooperative applications (Marques et al., 2006a; Marques et al., 2006b; Schneider and Schmidt, 2010). Therefore, a natural choice would be to adopt MOOS for *inter-vehicle* inter-process communication too. So doing, an application developer would experience a single communication abstraction and interface for inter-process communication. Unfortunately, MOOS presents severe limitations when employed for inter-process communication in an acoustic network. First of all, the communication between a client and the MOOSDB is usually based on TCP, an end-to-end protocol that requires an always-up connection. Whenever a client loses its connection to the MOOSDB, the system tries to re-establish it. Whereas this approach is effective for traditional radio-based networks, in the case of underwater networks, it creates undesired traffic and network overload. The underwater communication between any two nodes strongly depends on the oceanic conditions, which in general varies continuously making impossible to guarantee a reliable end-to-end communication (Akyildiz et al., 2005). Furthermore, since each client tries to re-connect to the MOOSDB as soon as it loses its connection (e.g., for a decrease in the channel capacity or bandwidth (Caiti et al., 2010)), this creates an additional communication overhead just in those moments when the acoustic channel is likely to be very poor so causing, as a consequence, network congestions and message loss. The second problem is that each client, which wants to connect to the database, must perform a preliminary handshake to register and enter into the system, specifying its topics of interest. Since this process is particularly delicate, MOOS ensures its robustness and coherence re-initializing it whenever a problem is encountered. Again, while the approach may be successful utilized for high-bandwidth and no-delay communications, it makes the entire client registration process unfeasible in presence of frequent disconnections and message loss. Finally, as it was thought for intra-vehicle inter-process communication, the MOOS system does not provide any network security mechanism. In the case of open communication channels, as the underwater one, this means that a *spoofing attack* (i.e., impersonation of a node) or a *snooping attack* (i.e., unauthorized eavesdropping of messages) may compromise the entire system integrity and confidentiality.

Figure 7: Deployment of a FNO from Gunneurs.

In order to cope with these limitations, within the UAN project, the basic MOOS system has been extended in two ways: first of all, it has been modified to improve efficiency and robustness of inter-vehicle inter-process communication; second, network security solutions have been integrated into the MOOS inter-vehicle communication protocol. The resulting middleware is called the *Inter-vehicle Secure MOOS* (IS-MOOS).

The IS-MOOS middleware represents a key point in the UAN proposed architecture. Actually, the resulting unified publish-subscribe communication framework allows the integration of all the heterogeneous autonomous mobile and fixed nodes into the application level of the UAN. With reference to the Folaga control architecture (Figure 9), the communication module of the mission supervisor is in fact realized as a IS-MOOS client. Through IS-MOOS, the client can thus convert the messages coming from other network nodes (e.g., the Command and Control Center) into information for the decision module of the vehicle, and hence into vehicle commands. Vice-versa, it can translate information on the vehicle 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).

In the next two sections we give some intuitions regarding IS-MOOS solutions for communication efficiency and security. The source code of IS-MOOS and the related user manual can be downloaded from the project web site (UAN, 2011).

IS-MOOS solution for efficiency

Figure 10 shows the general architecture of IS-MOOS. Making the MOOS system able to support the communication between different nodes of the underwater network, means that the MOOSDB becomes an external server, located in one of the network nodes, while the communication with the clients exploits the underwater channel. The use of acoustics implies that each node of the network must be extremely robust and able to autonomously adapt to the unexpected changes of the channel, avoiding, as much as possible, to send unnecessary messages. In UAN, this has been achieved in two ways: using the User Datagram Protocol (UDP) as the transport protocol of the network, and modifying the MOOSDB and clients structure to enhance the communication. UDP presents several advantages when used upon the underwater channel. In particular,

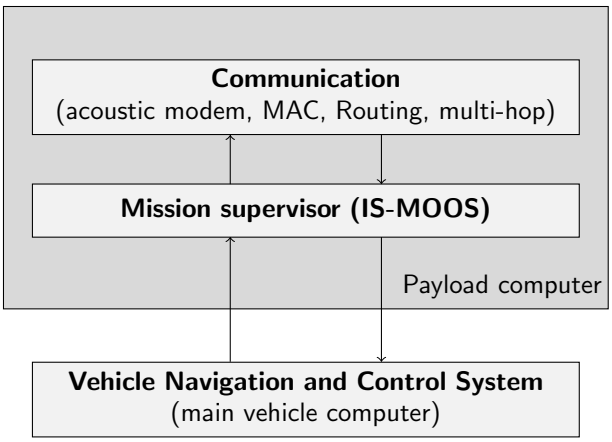

Figure 8: Conceptual architectural scheme of the implemented system.

it does not require an end-to-end connection, so it entirely avoids management issues (e.g. handshake at connection level) typical of connection oriented protocols, such as TCP. Its main drawback is that, of course, it does not provide the same level of reliability in message delivery: additional services, such as packet retransmission and delivery warrantees, hence, have to be transposed either to the lower layers of the network (e.g. MAC) or directly to the application level.

Furthermore, the MOOSDB structure has been modified to increase its robustness and capability to deal with delays, communication uncertainty and with the unreliabilities of the acoustic channel. Specifically, it has been given a multi-threaded architecture to completely isolate each client from the others. In practice, each client C is associated to a thread T_C on the database of which the client must know the address and the port in advance. In this way, while it is created a unique link between each client and the database (sandbox), it is also avoided the need for initial handshaking to set the communication parameters: if the client C wants to send a message m_C, it has simply to start its transmission towards its related address and port, while the dedicated thread T_C will be waiting for it. When the thread T_C has a message m_T for C, it sends C the message m_T together with the information for clock synchronization. However, since there is not any preliminary handshake, the described communication technique makes the system very fragile with respect to authentication issues. It may easily happen that a client C' begins to send messages to the thread T_C simply using the C's address and port. In order to avoid this problem, all the messages have to be authenticated as described in the next section, and upon receiving a message the thread T_C verifies the authenticity of its source. How IS-MOOS addresses these security issues will be discussed in next section.

The IS-MOOS security suite

Confidentiality of messages (i.e. communication between two nodes is "privileged" and may not be discussed or divulged to third parties) is achieved through encryption. In UAN, the specific encryption technique used is the symmetric one. Encryption is realized by splitting cleartext in blocks of fixed, predefined bit-length, and encrypting each single block. In the most general case, cleartext length is not a multiple of the block length and thus padding is necessary. However, padding has the negative effect that the ciphertext may result up to one block longer than the corresponding cleartext. This effect is called ciphertext expansion. While the ciphertext expansion overhead is negligible in a traditional network, it becomes relevant in wireless sensor networks and, in particular, in underwater acoustic networks, where the message size is typically quite small (because of energy and communication constraints). In order to avoid such a problem, the IS-MOOS security suite has been based on the CipherText Stealing (CTS) technique. According to this approach, we alter the processing of the last two blocks of plaintext, resulting in a reordered transmission of the last two blocks of ciphertext without the need for any ciphertext expansion (Schneier, 1995). The sole encryption without authentication is insecure (Menezes et al., 1996). For example, an adversary may flip bits in unauthenticated

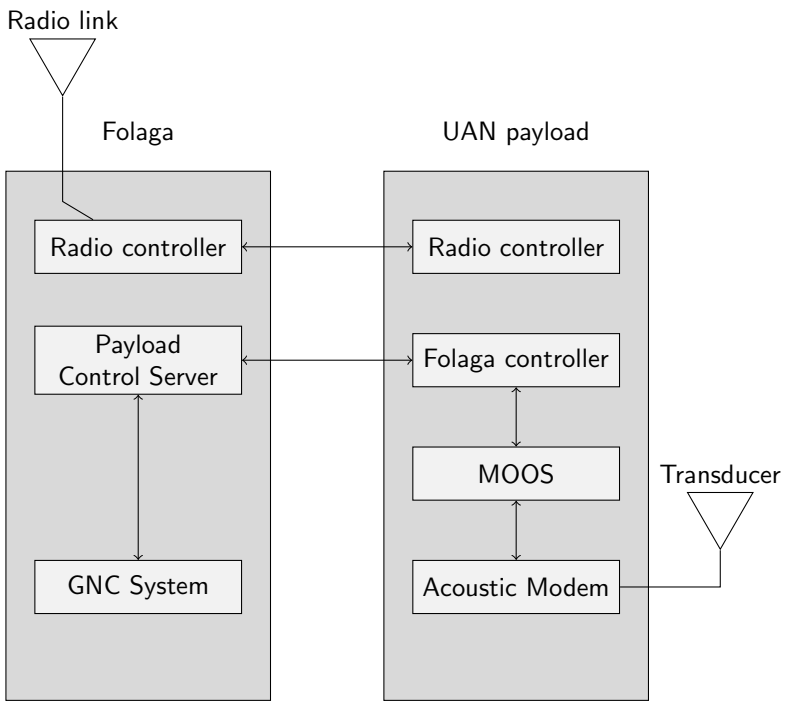

Figure 9: Interface between the eFolaga GNC and the UAN payload

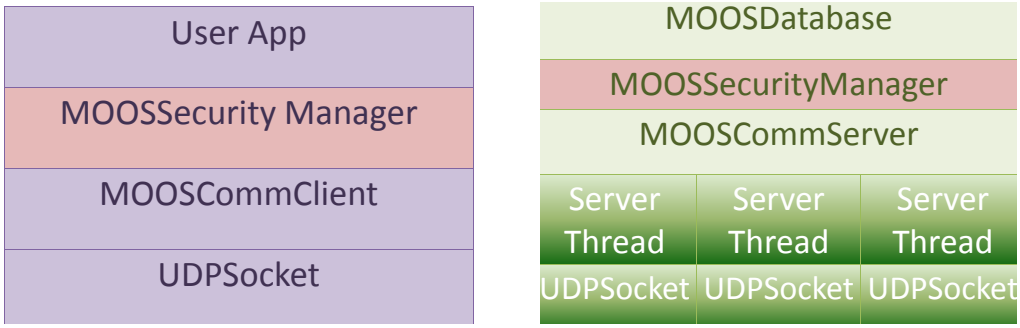

Figure 10: The IS-MOOS software architecture: client-side (left); server-side (right).

ciphertext and cause predictable changes in the plaintext that receivers are not able to detect. To address this vulnerability, the IS-MOOS system always authenticates messages. Security of hash functions is directly related to the length of the digest. However, as a digest is appended to the message, it becomes another source of message expansion and consequent communication overhead. UAN features a trade-off between security and performance by using 4 bytes digests resulting from truncating the real hash function value. Using such a short hash function value is not detrimental to security (Dini and Lo Duca, 2011). An adversary has 1 in 2^{32} chances to blindly forge a digest. If an adversary repeatedly tries to forge it, he/she needs at maximum 2^{31} trials, which, however, cannot be performed off-line. This means that the adversary has to validate a given forgery only by sending it to an authorized receiver. This implies that the adversary has to send 2^{31} messages in order to successfully forge a single malicious message. While in a conventional network this number of trials is not large enough, it is clear that in a underwater acoustic network this should provide an adequate level of security. An adversary can try to flood the network with forgeries, but on a 500 bps channel with 184-bit messages, he/she can only send about 2.71 attempts for second. Thus, sending 2^{31} messages requires around 306 months, i.e., about 25 years. Battery-operated vehicles have not enough energy to receive that many messages. Furthermore, the integrity attack would translate into a denial of service attack since the

Table 3: Position of network fixed nodes

$Node$	$lat, lon(decimaldeg)$	$depth(m)$
STU	63,44171873; 10,71354497	90.3
FNO1	63,44285603; 10,71539267	96
FNO2	63,44698453; 10,72613567	39
FNO3	63,44524920; 10,71338701	98

Table 4: KM modem technical characteristics

$info$	$settings$
Model	Km cNode mini transponder
frequency (kHz)	25.6
Source Level (dB)	187 - 190
Rate (bps)	200 - 500

adversary needs to occupy the acoustic channel for a long time, and it is feasible to detect when such a attack is underway. Simple heuristics have been used in UAN: vehicles signal the base station (command and control) when the rate of digest/MAC failures exceeds a predetermined threshold.

2.4 Mission setup for UAN11

This section describes specific settings for the network and for the algorithms used during the UAN11 activities. On May 23, 2011 the STU node was deployed. The network was used with a temporary topology composed by the STU and two fixed nodes, both located close to the pier. On May 24 two FNOs were deployed at their final location, as shown in Table 3. FNO3 was finally deployed on May 26 to substitute FNO1, which was lost at sea (rope broke during its recovery for recharging). Each node was equipped with the same acoustic modem, provided by UAN partner Kongsberg Maritime. This modem represented the physical layer of the UAN. Table 4 shows the main modem settings as used during the tests. The modem DSP board also implemented the link and network layers to execute medium access control (MAC) and data packet switching and forwarding. In particular, the medium access was realized through a Carrier Sense Multiple Access/Collision avoidance (CSMA/CA) mechanism, while the routing protocol was based on the FLOOD algorithm (Rudstad, 2009). Finally, the network stack was completed, as described in Section 2.3.2, using IP/UDP as inter-networking and transport protocols, and IS-MOOS as middleware and application level, which included network security mechanisms (see Figure 1). The underwater network was integrated as part of the global protection system as described in Section 2. According to the MOOS paradigm, all the network nodes connected to the central database (IS-MOOSDB), which was physically located on-shore, and logically on the UAN base station (STU). The network traffic was mainly composed by environmental data, transmitted periodically (once every $T_s = 120s$) from both the fixed and mobile nodes. In addition, further information could be requested by the C^2 when needed (e.g. node battery status, etc.). The average message size at application level was $150bytes$. Note that the transmission parameter T_s was set up empirically: decreasing or increasing such a parameter would diminish the network throughput due to network congestions or because not all the available bandwidth was used.

3 Communication metrics

The network communication performance has been evaluated at application level, using two metrics:

- Round Trip Time (RTT), computed as the time in seconds, for a message, to go back and forth from

a client to the database. This time sums up the propagation time of the message in the water and the time required to get through all the network layers, both at the client and at the database.

- Packet Loss (PL), computed as number of packets sent by a client and received by the database, and vice-versa. Note that the PL could differ from the packet loss at physical level, as each acoustic packet can be transmitted up to three times by the modems, if a reception acknowledgement is not received.

4 Results

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.

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 11 and 12 show Sound Speed Profiles (SSP) and salinity profiles, during three days of experiment, between 25 May and 27 May 2011, taken at various hours of the day. It is visible the presence of more fresh water in the upper layers.

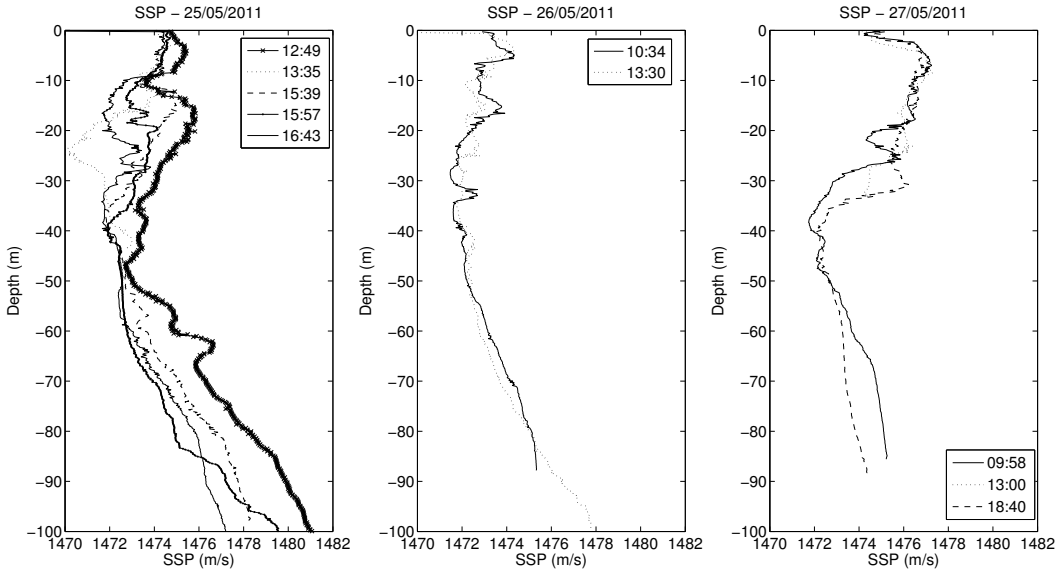

Figure 11: Sound speed profiles measured between 25 May and 27 May 2011.

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.

Between 25 May and 26 May 2011 the IS-MOOS system was used continuously, as shown in Figure 13

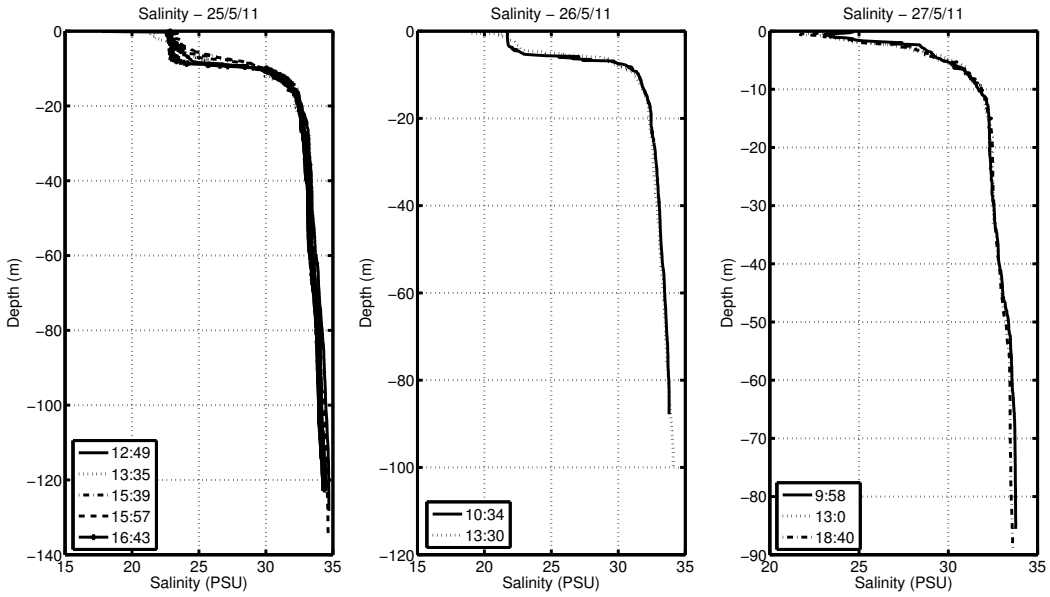

Figure 12: Salinity profiles measured between 25 May and 27 May 2011.

in terms of Packet Reception Ratio (PRR) at middleware level. From the figure, which represents the messages transmitted back and forth from the FNO2 to the MOOSDB, it is clearly visible the variation in the communication performance. Such behaviour was related both to the changes in the acoustic channel, and to periods of network overload with message drops due to too many messages transmitted with respect to the available bandwidth. It must be pointed out that such effects are, however, correlated and, at the current state, it is difficult to separate the two contributions. A decrease in the acoustic channel may easily cause network congestions which last as long as the network itself is not able to adapt to the new conditions (e.g. acoustic modem SL increase; decrease of the transmission bit rate; modification in the network topology to improve the communication). Network security was activated on 26 May 2011, at 3.14pm and left on from that moment on. On 26 May, FNO2 was left in non secure modality in order to verify the overall behavior of the security mechanisms implemented. For this reason, all the packets received by the DB and coming from FNO2 were considered as coming from an intruder and consequently dropped (and not shown in the figure). On 27 May, all the nodes (including FNO2) were in secure communication and the PRR in the link between FNO2 and the MOOSDB is shown in Figure 14. The first part of the day was devoted to low level communication tests and hence no packets were received at middleware level. Figure 15 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:

- The message expansion caused by the authenticator which in turn increases the probability of packet loss.
- 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.

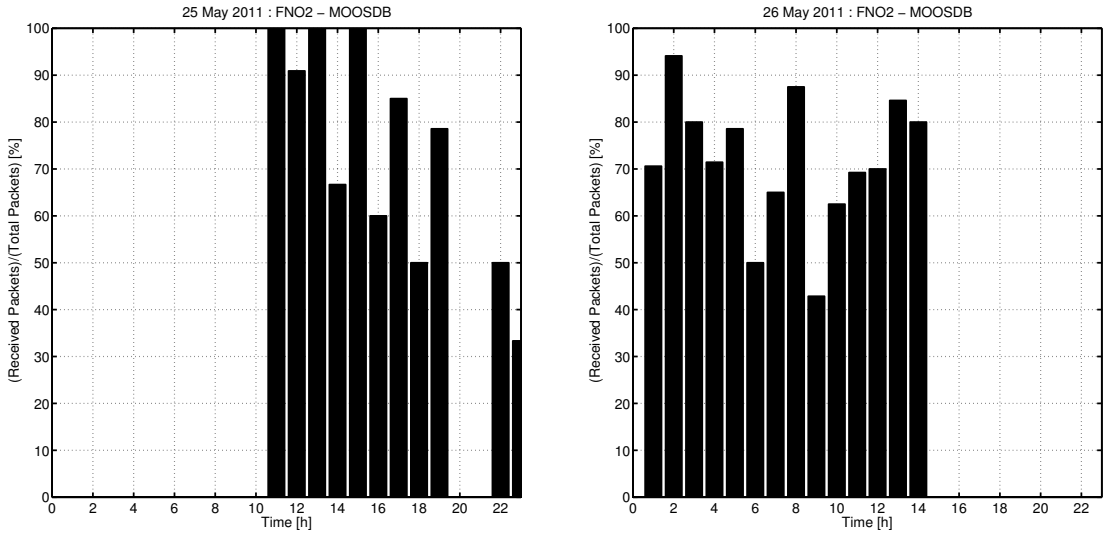

Figure 13: Packet reception ratio recorded on 25 and 26 May, 2011 along the link FNO2 - MOOSDB. It is clearly visible the variation in the communication performance during the operation days. Network security was kept off for most of the period and activated on 26 May 2011 at 15.14pm. From the moment on FNO2 was maintained out of the network by the DB as the node was not switched to the secure communication mode, and hence considered as an intruder. It re-entered into the UAN on 27 May 2011 when it was switched to the secure IS-MOOS (see Figure 14).

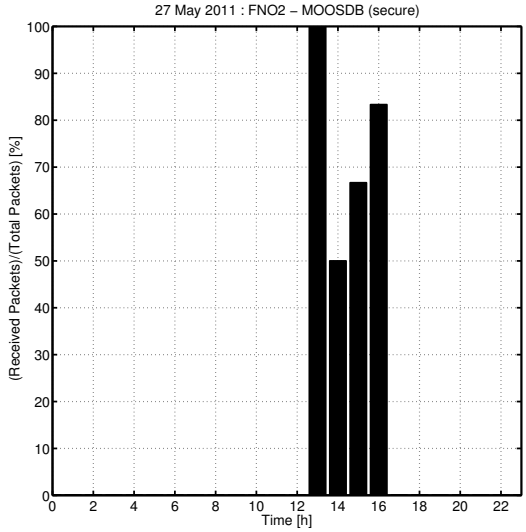

Figure 14: Packet reception ratio recorded on 17 May, 2011 along the link FNO2 - MOOSDB. Network security services were activated. Variations in communication performance are clearly visible.

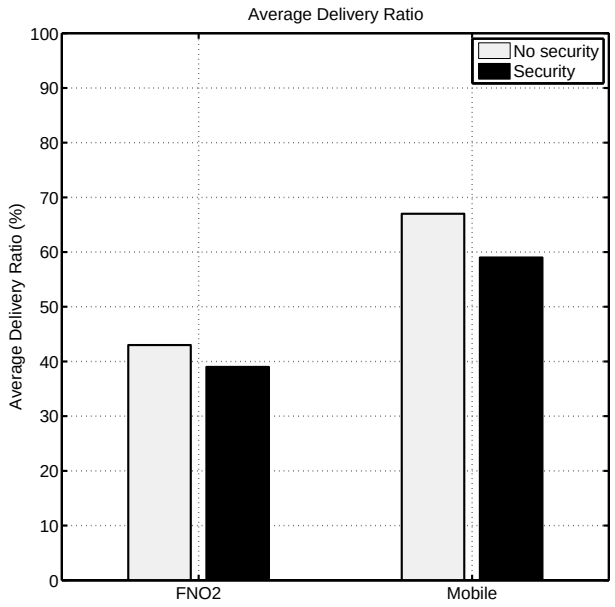

Figure 15: Average Delivery Ratio (ADR) performance. When the security was activated there was a decrease of 8% in the ADR. The decrease was due to two concurrent conditions: a decrease in the acoustic channel and in the message expansion due to the authenticator. Even though, at the current stage, we 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.

A global overview of the middleware performance is given in Tables 5 and 6 in terms of average packet loss for each node of the network, and in terms of average Round Trip Time (RTT). Except the STU, which was always operative, not all the nodes were in the water at the same time, and the network had often to change topology to adapt to the varying oceanic conditions, and to route the messages via the best communication path. On May 23 the network was composed by the STU with direct hops to the fixed nodes, which were located close the pier, in very shallow water. On May 23 and May 24, the IS-MOOS system was up for less than 4 hours the first day, and only for one hour the second day. Only few messages were exchanged and thus the corresponding statistics might be less accurate. Note also that, due to the loss of the node, RTT statistics for FNO1 on 23 and 24 May are currently not available, even though the node was operative. On May 25 one Folaga was used in the morning as a bridge to reach FNO2 from the STU, while in the afternoon FNO2 was routed directly, with a single hop. On May 26, FNO1 was substituted by FNO3 which was used to relay FNO2.

Finally, on 27 May 2011, the protection system was tested completely, including above water and underwater sensors. The two mobile nodes were used as active surveillance assets, and kept mostly on surface, but with just acoustic communication available for messaging with C^2. Figures 16, and 17, show the vehicles trajectories, in the morning and in the afternoon, respectively. In particular, in the afternoon of May 27, a complete anti-intrusion demonstration was carried out. With reference to Figure 17, 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 $OBJ_1 = (63, 44891470; 10, 71229367)$, and communicated via UAN to the C^2. As a response, the C^2 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 (red line pointing towards the STU in Figure 17) 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).

Date	*Node*	*Average Paket Loss (%)*
23 May 2011	FNO1	0
	FNO2	29.37
24 May 2011	FNO1	11.11
25 May 2011	FNO2	58.75
26 May 2011	R/V	32.76
	FNO2	54.76
27 May 2011	Folaga1	18.31 (until 2.00 pm)
	Folaga2	49.64 (after 3.00 pm)
	R/V	40.58
	FNO2	68.38

Table 5: Packet loss per day per each node in the water at middleware level. Note that the STU was always operative. Statistics collected on May 23 and May 24, 2011 are not very accurate as the IS-MOOS system was activated only for few hours of operation.

Date	*Node*	*Average RTT (s)*
23 May 2011	FNO2	17.39
25 May 2011	FNO2	58.71
26 May 2011	R/V	248.91
	FNO2	54.39
27 May 2011	Folaga1	38.81 (up to 2.00 pm)
	Folaga2	112.95 (after 3.00 pm)
	R/V	35.28
	FNO2	107.42

Table 6: Round Trip Time per day per each node in the water at middleware level. Note that the STU was always operative. Statistics on May 23 and May 24, 2011 might be less accurate as the IS-MOOS system was activated only for few hours of operation. Note that, due to the loss of the node, RTT statistics for FNO1 on 23 and 24 May are currently not available, even though the node was operative.

5 Conclusions

This work described the implementation at sea of an underwater acoustic network composed of fixed and mobile nodes, which included multi-hop capabilities, and able to work continuously. The network showed a quite impressive level of robustness and it was able to tackle variation in its structure, with nodes routinely added and removed, e.g., for battery recharging, and to adapt to the modification of the oceanic environment. To the best of our knowledge this was the first time that such a complex UAN was deployed and successfully operated.

The paper reports details on the performance of the acoustic communication, evaluated in terms of round trip time and packet loss. The data gathered during the experimental activities shows that the communication performance was poor with large and variable delays and packet loss, depending on day and network configuration.

The mobile nodes of the UAN were implemented on eFolaga AUVs, and they were used: as communication nodes and movable relays to reach fixed nodes with poor acoustic connectivity; to autonomously adapt in response to variation of the network performance; as surveillance assets of the UAN wide area protection system, acoustically controlled by the C^2.

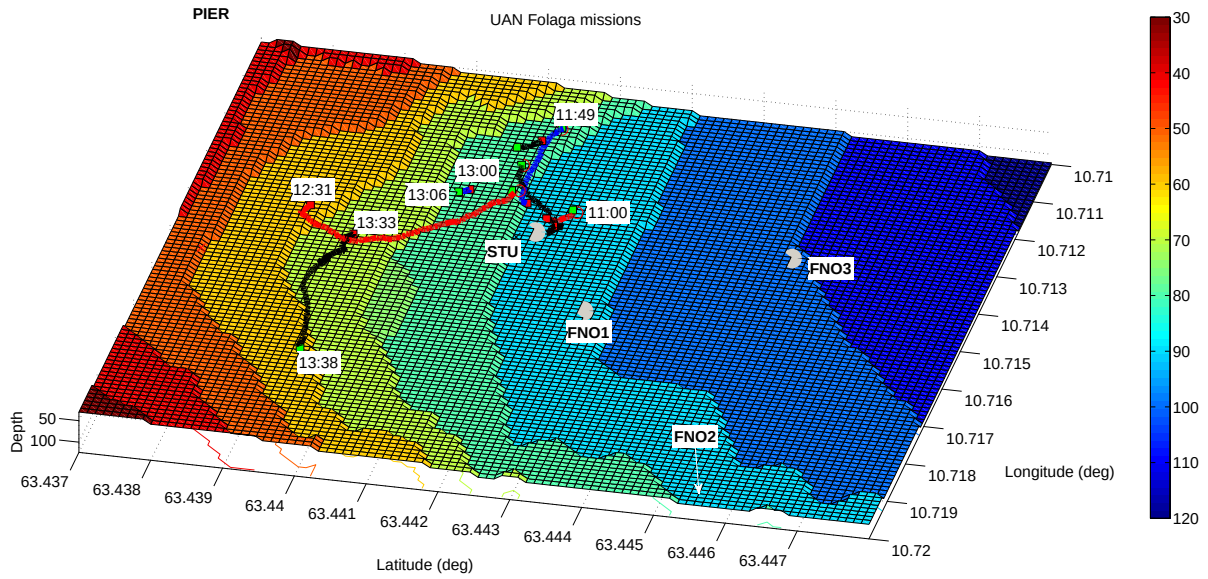

Figure 16: Folaga AUVs path during the experimental activity on May 27. In the first part of the day the vehicle in the water was acoustically controlled by the UAN command and control center to perform several missions (each line represent a different mission).

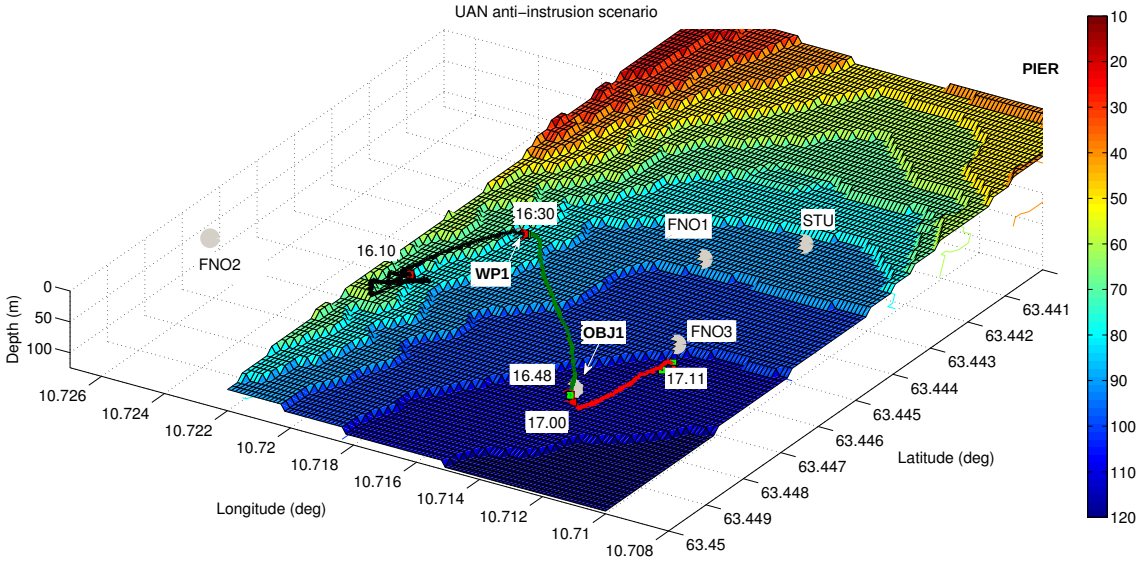

Figure 17: In the afternoon of 27 May 2011, the vehicle was used as a surveillance asset. The C^2 sent the AUV in an area of possible intrusion (OBJ_1) to proceed to further investigation. Once on location the AUV found itself out of the network. According to the behavior described in Section 2.3 the mission supervisor autonomously planned a new mission to move towards the high value asset (the UAN base station) where it could re-enter the network.

The UAN network was also equipped with network security features (IS-MOOS) to guarantee the confidentiality, authenticity and integrity of the exchanged messages. This is of paramount importance in the context of underwater harbour protection where the communication channel is open and often easily accessible. The UAN11 sea trial demonstrated that, as long as the security features are tailored for the limitation of the communication medium, the inclusion of network security is indeed feasible even with the bandwidth and capacity constraints that characterize the underwater environment. The recorded data shows that the security overhead does not worsen so much the performance of the network, especially when compared to the communication degradation due to the acoustic channel itself.

6 Future research and lessons learned

On the basis of the UAN11 results several lessons can be drawn. The UAN project demonstrated the feasibility of the operation at sea of an underwater acoustic network composed by fixed and mobile sensors. However, given the variability and the limitation of the communication, the autonomy of the nodes becomes critical. Each node must be able to take autonomous decisions to perform its tasks without continuous supervision by the command and control, and often even disconnected from the rest of the network for quite long periods of time. Furthermore, delays and packet loss are so high that cooperation algorithms with the need for a great deal of message exchange, such as consensus-based methods, become operatively infeasible.

Since the achievable communication performance is so limited, it becomes important to reduce as much as possible the network communication overhead (e.g. signaling traffic, etc.) so to leave the bandwidth available for the applications. In this sense, the ideas described in this paper in the case of the IS-MOOS to reduce the traffic at middleware level could be pushed further. The use of a centralized pub/sub system has the advantage of concentrate in a single node all the information exchanged within the network. While this is useful in the case of protection of critical infrastructures, where the C^2 needs the complete control of the system, it creates an addition communication burden and may limit the network scalability. It is hence foreseeable that in other applications more suited middleware may be utilized. For example, it is a current research field in terrestrial networks the deployment of distributed pub/subs, which would also have the advantage of reducing the number of messages exchanged. Similar approaches can also be extended to other network layers. Finally, we have learnt that using a unified programming model, namely publish-subscribe, and a unified middleware layer, namely IS-MOOS, both for intra- and inter-vehicle communication simplifies the development of secure and reliable applications in underwater acoustic networks.

Acknowledgments

This work was supported in part by European Union, 7th Framework Programme, Project UAN - Underwater Acoustic Network under Grant no. 225669.

References

Akyildiz, I. F., Pompili, D., and Melodia, T. (2005). Underwater acoustic sensor networks: research challenges. *Ad Hoc Networks*, 3(3):257–279.

Balasuriya, A., Schmidt, H., and Benjamin, M. (2009). Nested distributed autonomy architecture for undersea sensor networks. In *Proc. IEEE/MTS Oceans*.

Becker, K. M., Zucker, M. L., and Bradley, D. L. (2008). Characterization of harbour and ports for acoustic defence systems. In *Proc. Water Side Security Conference*.

Benjamin, M., Schmidt, H., Newman, P., and Leonard, J. (2010). Nested autonomy for unmanned marine vehicles with moos-ivp. *Journal of Field Robotics*, 27(1):834–875.

Benjamin, M. R., Leonard, J. J., Schmidt, H., and Newman, P. M. (2009). An overview of moos-ivp and a brief users guide to the ivp helm autonomy software. Tech. rep., Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA. Available at http://hdl.handle.net/1721.1/45569.

Bernstein, P. A. (1993). Middleware an architecture for distributed system services. *Communications of the ACM*, 39:86–98.

Caffaz, A., Caiti, A., Casalino, G., and Turetta, A. (2010). The hybrid auv/glider folaga: Field experience at the glint'08 experiment. *IEEE Robotics and Automation Magazine*, 17(1):31–44.

Caiti, A., Calabro, V., Dini, G., Lo Duca, A., and Munafò, A. (2012a). Secure Cooperation of Autonomous Mobile Sensors Using an Underwater Acoustic Network. *Sensors*, 12(2):1967–1989.

Caiti, A., Crisostomi, E., and Munafò, A. (2010). Physical characterization of acoustic communication channel properties in underwater mobile sensor networks. In Hailes, S., Sicari, S., and Roussos, G., editors, *Sensor Systems and Software*, volume 24 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 111–126. Springer Berlin Heidelberg.

Caiti, A., Munafò, A., and Vettori, G. (2012b). A geographical information system (gis)-based simulation tool to assess civilian harbor protection levels. *IEEE Journal of Oceanic Engineering*, 37(1):85–102.

Casalino, G., Cresta, M., Storti, E., and Simetti, E. (2010). Archimede - integrated network-centric harbour protection system. In *Water Side Security Conference*.

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

Eickstedt, D. and Sideleau, S. (2008). The backseat control architecture for autonomous robotic vehicles: A case study with the iver2 auv. In *Proc. IEEE Oceans Pacific*.

Hamilton, M. J., Kemna, S., and Hughes, D. (2010). Antisubmarine warfare applications for autonomous underwater vehicles: The glint09 sea trial results. *Journal of field robotics*, 27(6).

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

Marques, E., Gonçalves, G., and Sousa, J. (2006a). The use of real-time publish-subscribe middleware in networked vehicle systems. In *Proceedings of the 1st IFAC Workshop on Multivehicle Systems (MVS 2006)*, volume 1 (PART 1), pages 108–113, Salvador, BA.

Marques, E. R. B., Goncalves, G. M., and Sousa, J. B. (2006b). Seaware: a publish/subscribe based middleware for networked vehicle systems. In *Proc. of the 7th IFAC Conference of Manoeuvring and Control of Marine Craft*.

Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.

Munafò, A., Simetti, E., Turetta, A., Caiti, A., and Casalino, G. (2011). Autonomous underwater vehicle teams for adaptive ocean sampling: a data-driven approach. *Ocean Dynamics*, 61(11).

Newman, P. (2012). The moos cross platform software for robotics research. "Retrieved January 12, 2012, from http://www.robots.ox.ac.uk/ mobile/MOOS/wiki/pmwiki.php".

Oxford Mobile Robotics Group (2012). The moos cross platform software for robotics research. Retrieved, February 24, 2012, from http://www.robots.ox.ac.uk/ mobile/MOOS/wiki/pmwiki.php/Main/Documentation.

Pompili, D. and Akyildiz, I. F. (2009). Overview of Networking Protocols for Underwater Wireless Communications. *IEEE Communication Magazine*, pages 1–6.

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

Schneider, T. and Schmidt, H. (2010). The dynamic compact control language: A compact marshalling scheme for acoustic communications. In *Proceedings of IEEE OCEANS 2010*, Sidney, NSW. cited By (since 1996) 0.

Schneier, B. (1995). *Applied cryptography: protocols, algorithms, and source code in C*, pages 191 – 195. Wiley, 2nd ed. edition.

Stojanovic, M. (2007). On the relationship between capacity and distance in an underwater acoustic communication channel. *ACM Sigmobile Mobile Computing and Communications Review (MC2R)*, 11(4):34–43.

UAN (2011). The uan underwater acoustic network - project web site. "Retrieved December 12, 2011, from http://www.ua-net.eu".

Zabel, F., Martins, C., and Silva, A. (2011). Design of a uan node capable of high-data rate transmission. *Sea Technology*, 52(3):32–36.