PROJECT PERIODIC REPORT

Grant Agreement number: 225669

Project acronym: UAN

Project title: UNDERWATER ACOUSTIC NETWORK

Funding Scheme: STREP - Cooperation

Date of latest version of Annex I against which the assessment will be made: 09/Feb/2009

Periodic report: 1st 2nd 3rd X 4th □

Period covered: from 01/October/2010 to 30/September/2011

Name, title and organisation of the scientific representative of the project's coordinator:
Sergio M. Jesus, Prof., CINTAL

Tel: +351289800951

Fax: +351289864258

E-mail: sjesus@ualg.pt

Project website address: www.ua-net.eu

Declaration by the scientific representative of the project coordinator

I, as scientific representative of the coordinator of this project and in line with the obligations as stated in Article II.2.3 of the Grant Agreement declare that:

- The attached periodic report represents an accurate description of the work carried out in this project for this reporting period;

- The project (tick as appropriate):

  X has fully achieved its objectives and technical goals for the period;

  □ has achieved most of its objectives and technical goals for the period with relatively minor deviations[1];

  □ has failed to achieve critical objectives and/or is not at all on schedule[2].

- The public website is up to date, if applicable.

- To my best knowledge, the financial statements which are being submitted as part of this report are in line with the actual work carried out and are consistent with the report on the resources used for the project (section 6) and if applicable with the certificate on financial statement.

- All beneficiaries, in particular non-profit public bodies, secondary and higher education establishments, research organisations and SMEs, have declared to have verified their legal status. Any changes have been reported under section 5 (Project Management) in accordance with Article II.3.f of the Grant Agreement.

Name of scientific representative of the Coordinator: ..SERGIO M. JESUS..........................

Date: 19 / OCT / 2011

Signature of scientific representative of the Coordinator: ....

[1] If either of these boxes is ticked, the report should reflect these and any remedial actions taken.

[2] If either of these boxes is ticked, the report should reflect these and any remedial actions taken.

1. Publishable summary

The Underwater Acoustic Network (UAN) project aims at conceiving, developing and testing at sea an innovative and operational concept for integrating in a unique system submerged, surface and aerial sensors with the objective of protecting off-shore and coastline critical infrastructures. Critical infrastructures may include, but are not limited to, power plants, off-shore gas or oil platforms, sensitive harbours, economically strategic bays or inlets, airports and coastal military structures. The security plan for such economically vital infrastructures may include land/air as well as underwater sensors and actuators. Information exchange between the various security subsystems requires a communication network with the appropriate bandwidth and resilience time to allow system operation as whole. Underwater sensors and actuators may be advantageously (from the communication point of view) cable connected to shore or to fixed platforms. However, in many other situations where for example sensors are spread over large areas, or there is the need for a rapid or temporary deployment, or sensors are mounted on moving platforms, the only viable and/or cost effective solution is wireless. In this case moving platforms will include Autonomous Underwater Vehicles (AUVs) and Gliders which are becoming off the shelf sophisticated systems that can considerably extend the capabilities of security systems.

The main objective of the UAN project is to fill the technological gap and specifically to define methodologies, technologies and procedures for the implementation of underwater acoustic communication networks to be integrated as a component of a multi-media network for surveillance and monitoring of critical at sea infrastructures. More specifically network efficiency will require:

(a) *the performance evaluation of digital transmission* over the acoustic underwater channel as a function of frequency, signal modulation and specially environmental characteristic parameters;

(b) the specification of design methodologies, system requirements and algorithms for implementing a generic and secure underwater ad-hoc mobile acoustic network (MANET) consisting of fixed and mobile nodes, where the *mobile nodes will be able to adapt to the network geometry to* obtain a near optimal communication performance according to the predictions obtained from (a);

(c) *the integration of MANET into the overall security system* through dedicated underwater gateways allowing for a sustained asymmetric flow of data and commands to and from shore, and

(d) *the experimental verification and validation* of the proposed methodologies, algorithms and developed hardware that can adapt to the end user requirements.

As a first step toward detailed performance specifications of the underwater acoustic network, a *threat scenario* has been defined and analysed. Threats can be subdivided into two main categories: underwater intrusion threats to the critical infrastructure and threats to the network itself. In addition to the threat scenario, an associated *environmental scenario* has been set up. The underwater acoustic network must be able to cope with the variability of the acoustic channel characteristics due to environmental changes (e.g., temperature) to guarantee the Quality of Service (QoS) both in terms of networking performance and of the ultimate goal of the deployed assets, i.e., the security of the infrastructure. As a final activity for scenario definition, shallow water areas in the Mediterranean (Tuscan Archipelago) and in the North Sea (Trondheim Fjord) were identified.

The objective of performance evaluation methodologies is to develop methods and software for predicting the communication network performance in terms of achievable stable communication rates, given the environmental conditions, the node positions, speed parameters of the mobile nodes and the encoding/decoding schemes. The performance evaluation methodology developed is based on the simulation of acoustic communication in realistic underwater environments, with careful modelling of effects with significant influence on communication performance, in particular transmission loss, ambient noise, reverberation and multiple propagation paths with individual time-variable Doppler shifts due to movement of communication nodes, water surface and/or water body. A significant project milestone was attained with the assessment of the performance prediction methodology based on the COMLAB software tool against experimentally observed communication performance.

Other requirements for the set up of a MANET network encompass the development and testing of specific hardware tools. A set of generic purpose acoustic modems was adapted to UAN requirements so as to be able to cope with message handling to/from the various network nodes, routing operation and variable data rate switching for asymmetric communication. Each underwater node is formed by a sensor capable platform coupled with a generic UAN modem. The sensor platform, fixed or mobile, will handle the messaging and routing while the modem will provide medium access capabilities. During this final year extensive testing of modem pairs has been performed both during project integration tests and during the final project sea trial. The UAN class modem is now a robust working platform for underwater acoustic networking.

The seamless integration of the underwater acoustic network into the global net requires appropriate cabled or radio linked gateways being able to cope with an asymmetric data flow that is normally much higher from underwater to shore than in the reverse direction. The solution adopted in UAN was to develop a bottom moored and shore connected communication node - *the base station*. The base station is a highly complex network node including a vertical line array with 16 acoustic sensors, a UAN class modem and the appropriate electronics for signal real time transmission to shore. The base station is now a fully operational system tested both under controlled conditions and in several open sea operations. Due to its particular configuration, the base station acts as a particular network node in a single-input-multiple-output (SIMO) configuration in respect to the other network nodes. During sea testing it was shown that coherent transmissions, either from dedicated modems or from sound sources, in various geometric configurations (depths and ranges), static or moving, showed an achievable one-way data rate much higher than that provided by individual network modem communications. Another important result is the degree of robustness of the communication performance both to geometric changes between source and receiver (which includes moving nodes) and to environmental variability. In this context environmental variability relates to water column short and long term changes and to bottom structure variations due to source movement during transmissions. Transmissions included signals for covert communication, which is an important component for network self security and for reliable security operations in general. This was demonstrated during the final project sea trial where simulated threat images could be sent from any network node directly to the base station at the Command and Control operator request.

The UAN network demonstrator included the set up of a full OSI communication model, which layers were individually tested and configured both at the hardware and software (driver) level. The physical and logical network layer encompasses the modems' operation, which includes point-to-point and multi-hop inter-modem links using the low-level modem embedded protocol. The network IP layer runs in a star-shaped network in which the base station is the central node and through which each client node exchanges data independently of its lower level configuration. This level of abstraction makes it possible for any client node to establish point-to-point IP connections with the master where IP forwarding is performed. The MOOS middleware runs at the IP layer level and is composed of the base station MOOS-DB database with MOOS clients on each network node. The high data rate secure layer has also a star configuration where each slave node transmits signals received at the base station gateway node equipped with a multi-hydrophone vertical array. The application layer runs on top of MOOS through which Command and Control (C2) directives as well as network transparent high data rate messages, are transmitted and received.

The UAN system was deployed on the Trondheim Fjord in a 5x5 km area with varying water depth between 30 and 150 m. The 5-node network was composed of two mobile nodes, two fixed nodes and one base station node. The base station was connected to shore, where data processing and the C2 were installed. During several days the system was operated in simulated threat scenarios with AUV patrolling the area and performing interception missions. C2 was receiving information and sending commands to any asset in the field executing the requests: receiving environmental data from fixed nodes, moving mobile nodes and integrating performance predictions. To our knowledge this is the first time ever that a fully functioning network was deployed and demonstrated to be operational at sea, representing a landmark in underwater communication functionality in general and for security applications in particular.

It is now clear that all project objectives were attained where the underwater network appears to be just a seamless extension of a local area network. The impact of this achievement will likely foster other applications and discoveries. To obtain more information on UAN activities, achievements and partnerships please contact the consortium at info@ua-net.eu or consult the UAN website www.ua-net.eu .To be kept informed subscribe the UAN newsletter .

2. Project objectives for the period

UAN overall objectives are set forth in section B.1.1 of Annex I (pages 7 and 8). Specific objectives per project year can be drawn from the work package and deliverables lists (B.1.3.3 and B.1.3.4) and timing chart (B.1.3.5 and fig.2 of Annex I, respectively). Integrating the information from these various sources the third project year objectives of UAN were centred in the following topics:

- to terminate the simulated data testing of the communication performance prediction tools and evaluate its performance against field data;
- to field test the various network components (Folagas, modems, fixed nodes and gateway node) and make sure of their compatibility and performance in real world conditions;
- to validate the communication network architecture, including inter element drivers and middle ware components,
- to perform a full size sea trial with all the system components, network layers and threat scenario, so as to test full system integration.

The third interim progress report was submitted on the completion of the project 30 months. This third year included the completion of various deliverables as well as reaching five project milestones. These milestones were related to: the completion of achieving a prediction of communication network performance on benchmarking (M2.2), the completion of a working modem pair and testing at sea (M3.2), the conclusion of field testing of system integration on Folaga vehicles (M4.2 – M5.2) and finally that related to the conclusion of the main project sea trial (M6.1). There was a slight delay on the conclusion of the M3.2 which had a minor impact on the completion of M5.2. This impact was minimized by two additional system testing workshops one held in Faro (Portugal) in March, and one held in Trondheim (Norway), prior to the sea trial, leading to a timely completion of all the other milestones, including the main project sea trial (M6.1).

3. Work progress and achievements during the period

WP2 – Scenario development and performance evaluation

Summary of progress

Task 2.4 *Validation of predicted performance against field data* was active during this period. The goal of Task 2.4 and the preceding Task 2.3 *Performance evaluation prediction* is to demonstrate the performance prediction methodology and the COMLAB software developed in Task 2.2 by applying it on communication under environmental conditions characteristic of the UAN application scenarios, and validate the predictions against experimental data.

The objectives of both tasks 2.3 and 2.3 have been reached, as reported in deliverables D2.3 and D2.4 (both delivered in Y3). The scenarios studied were selected from those of the P2P communication tests at the UAN10 trials at Pianosa I. (Italy) in September 2010.

Main achievements

The main achievement in WP2 in this period is a first assessment of the performance prediction methodology and the COMLAB software tool against experimentally observed communication performance. A summary of the results of the assessment is found in tables 3 and 4 below, showing the predicted and the experimentally observed frame error rates as function of source position and modulation format using all 8 receivers and a single receiver, respectively.

A second important achievement in WP2 in this period is the development of a technique for estimating seabed parameters by using the communication signals for acoustic inversion. Such techniques are important for accurate modelling of the effects of seabed interactions on the communication signals and the influences of such interactions on communication performance.

Brief summaries of the technique for seabed parameter inversion and the validation of the performance prediction method are given below. Further details can be found in the D2.4 report [3] and the conference papers [6] (Oceans'11), and [4, 5] (UAM 2011).

Environmental model of the Pianosa I. Site

In COMLAB the environment is modelled as a water layer above a seabed consisting of a single infinitely thick layer of fluid or solid material. The geometry is three-dimensional, i.e. the water depth h may vary with the horizontal coordinates (x, y) and the sound speed c in water may vary with all three spatial coordinates (x, y, z). h(x, y) and c(x, y, z) are smooth functions, represented by B-spline expansions. Modules for computation of the coefficients of the B-spline expansions from input (measurement) data given at arbitrary spatial points are included, see [1, Sec. 3.1].

Bathymetry, network geometry and sound speed

The left frame of Figure 1 shows the bathymetry and the source and receiver positions at the site of the stationary-source P2P tests. The bathymetry data were obtained by combining two sources (i) digitization of a navigation map of the experimental area [12, p. 10], and (ii) a multibeam survey of the experimental area conducted by NURC in September 2010. The black dots marked S1, S2, S3, S4 and VA are locations of the source nodes and the vertical receiver array, respectively, in the stationary-source P2P tests on September 20, 2010. The water depth varies from ca 2 m at the pier to ca 58 m at the vertical array.

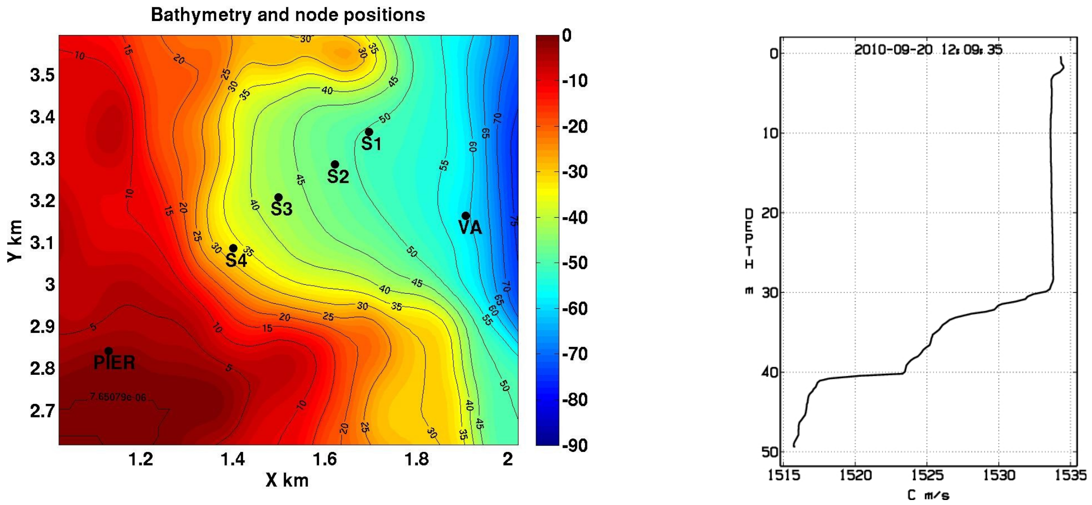


Figure 1. Left: Bathymetry and positions of source (S1-S4) and receiver (VLA) at the stationary-source P2P tests at Pianosa. Right: Sound speed profile recorded at the receiver.

The sound speed was modelled as range independent, with the depth dependence shown in the right frame of figure 1, recorded near the VLA on the day of the P2P tests.

Seabed parameters

The seabed is modelled as a fluid under a smooth non-reverberant seafloor. The geoacoustic parameters of the seabed model were determined by a 'through-the-sensor' inversion technique applied to the HFM probe pulses embedded in the P2P communication data. A brief description of the inversion technique follows.

Data used for seabed parameter inversion

The data used for geoacoustic inversion were obtained from the communication signals transmitted from the stations S2 and S4 and received on a moored vertical line array (VLA). An example of the measurement scenario is displayed in figure 2. There are four ray paths with a single bottom bounce (depicted in green and red colours in figure 2), which carry information on the reflectivity of the bottom.

Figure 3 is a display of recordings of 43 time traces of signal envelopes (magnitude squared of complex pressure) that were sent repetitively in time gaps of some 7 s. The bandwidth of the HFM pulse was 8-12 kHz, which implies that the pulse width after match filtering is some 0.25 ms. Arrival times and amplitudes are normalized w r t the direct arrival (D). The surface reflections (S), which follow after a delay of 1.3 ms, exhibit fluctuations which amount to some 2 dB on average. There are four arrivals with a single bottom bounce. The first one (B) is hardly discerned at a delay of 5 ms. Then follow the surface-bottom arrival (SB), the bottom-surface (BS) and surface-bottom-surface (SBS) arrivals at delays of 8, 18 and 23 ms respectively. On average their amplitudes are less than -17 dB. Four arrivals with exactly two bottom bounces are expected to appear in the time window 25-62 ms. Apparently they are obscured by a background field (-35 dB), which presumably emanates from surface and bottom scattering (reverberation).

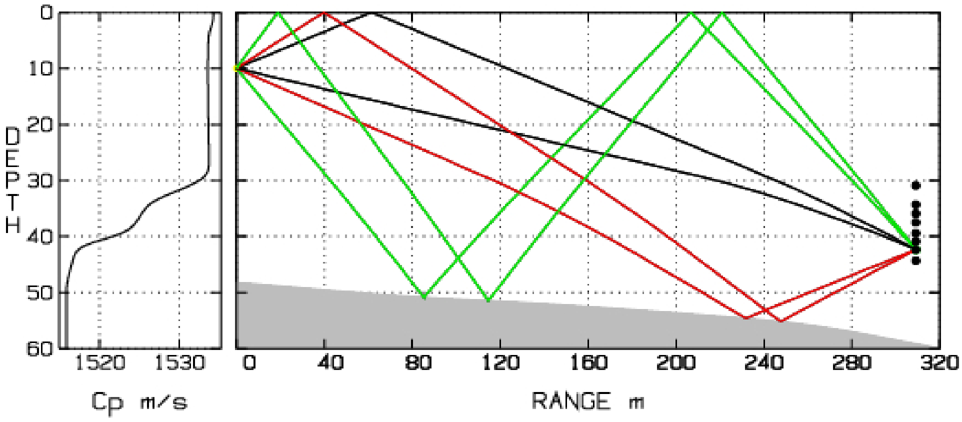


Figure 2. Left: Sound speed profile at the time of the experiment (Sept 20 2010).Right: Bathymetry in the transect from S2 to VLA and ray paths of the first six arrivals at hydrophone R7.

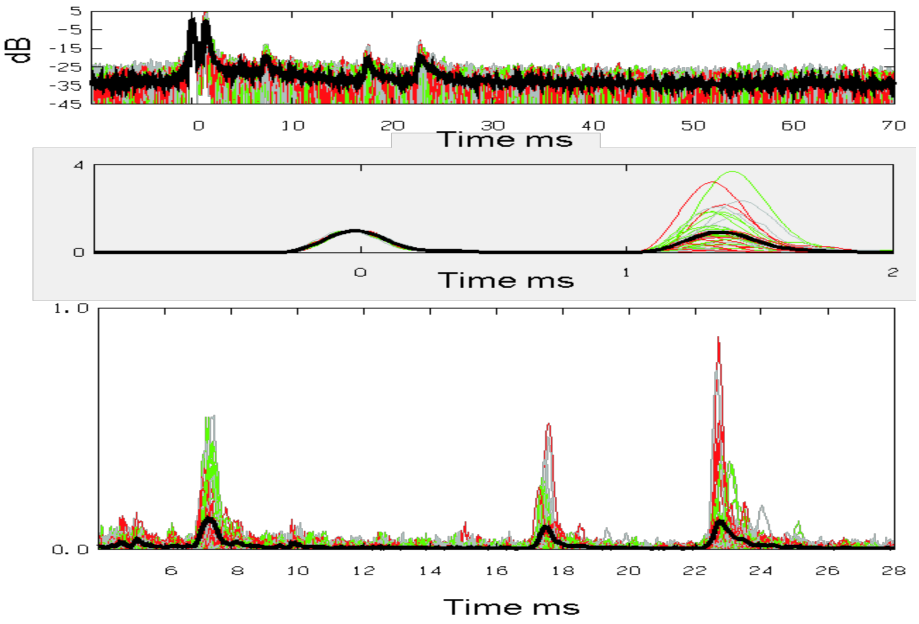


Figure 3. Time traces of 43 pings at S2-R7 and their average (solid black). The top frame shows the envelope signals in dB-scale in time interval [-10,70] ms, the middle frame shows merely the D and S arrivals, and the bottom frame is an expanded view of the B, SB, BS and SBS arrivals in time interval [4-28] ms.

Seabed parameter inversion results

For the inversion a conventional matched field technique is applied. The modelled time-series is composed of three parts, propagation along the B, SB, BS and SBS ray paths, reverberation from a randomly rough water/sediment interface, and ambient noise. The contributions from bottom reflections and reverberation were generated by a ray model, while ambient noise was taken from a suitable time slice of measured data. The inversion is made for two parameters, the mean grain size M_z (in ø units) and rms bottom roughness height h. The mean grain size is used as a substitute for fluid sediment parameters $(c\ \rho,\ \alpha)$ by the use of empirical relationships obtained from regression fits to measurements on core samples [7], [9]. The rms roughness height h is related to the spectral strength parameter w_2 in a statistical description of bottom roughness by an isotropic power law, in which the spectral exponent γ_2 is held fixed at a typical value of $\gamma_2 = 3.25$ [10]. The fitness function, which measures the mismatch between modelled and measured time series of signal envelopes, was formulated as an average in dB over time samples and the number of hydrophones being used. The minimization of the fitness function was done over a uniform grid of 21 x 21 points in the space

$$\left\{(M_z\right\},h),\ |\ 0\le M_z\le 10\,\varphi,\ 0\le h\le 10\,c\left(m\right) \qquad (1)$$

by an exhaustive search. Figure 4 shows a level plot of the fitness function over the search space (1) using data from two hydrophones, S2-R1 and S2-R7.

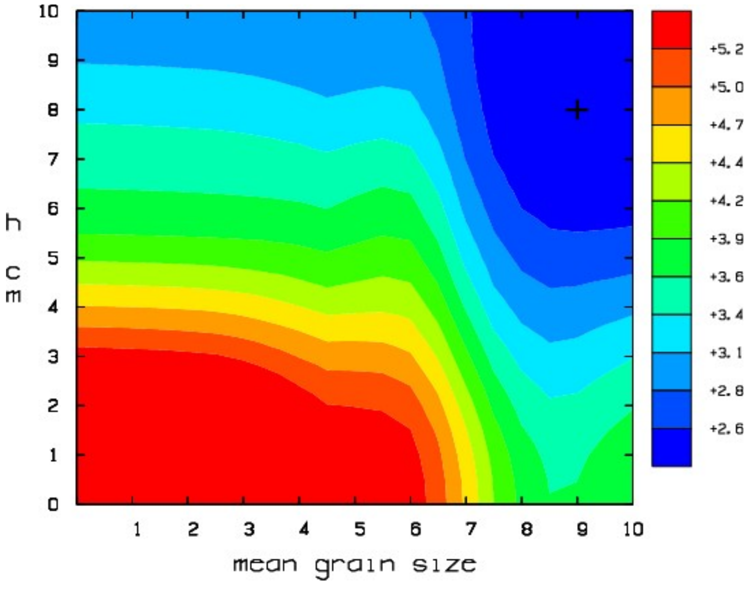


Figure 4. Level plot in dB of the fitness function as function of mean grain size (-units) and rms roughness height (cm). The minimum point is marked by a cross.

The best fitness of 2.3 dB was obtained for M_z=9.0 ø, (or c=1497 m/s, =1386 g/cm^3, α=0.08 dB/λ), h=8.0 cm. The fitness function is rather shallow in a large domain around the minimum point as can be noted in figure 3. It indicates that there is an ambiguity between coherent and incoherent contributions, the sum of which is approximately energy conserving by the underlying scattering theory of modelled time series. Roughly it means that the weak coherent bottom reflections, as evidenced by data in figures 2, can be explained by both a hard and rough bottom or a soft and smooth bottom. The ambiguity is mostly pronounced along horizontal and vertical zones through the optimal point at =9.0 *ø* and h=8 cm. The behavior of the fitness function of the bottom line corresponds to an inversion made for a smooth surface without reverberation. When reverberation modelling is omitted in the above inversion the run time is reduced from hours to seconds. The large computational burden of modelling seafloor scattering is explained by the necessity to include scattering returns from all conceivable azimuthal and vertical angles at both incidence on and reflections off the seafloor. The footprint area on the seafloor must be large enough to cover scattering that arrives within the time window being used for inversion. Since the reverberation at short range is markedly bistatic the first-order small-slope approximation (SSA) [11] for scattering of a rough surface was used.

The computation of scattering strength of SSA is demanding as it involves a double integral of an highly oscillatory function [8]. A topic for future work is to develop more efficient computational techniques to deal with short range reverberation. Fortunately in the present case, the inversion result for a flat bottom does not deviate too much from the optimal one. Fitness of inversion for the flat bottom case is displayed at the bottom line of figure 3. As can be seen the resolution in terms of M_z is good with an optimal value around $M_{z\approx}$ (c=1504 m/s, ρ = 1411 kg/m^3, α = 0.08 db/λ), corresponding to a sediment of fine silt. This is in clear disagreement with the harder sand and coastal debris materials in the seabottom map of the Tuscan Archipelago in [12, Figures 4.9 and 4.10]. Noting that both the sediment density ρ and sound speed c decrease as function of mean grain size Mz [7], i.e. hard seabed materials correspond to small values of Mz in φ-units, fig 3 shows that harder seabed materials provide good fits to the observed bottom reflection loss only if combined with a rough seafloor. Without accounting for roughness-induced reflection losses, a harder seabed model will overestimate the coherent bottom reflection coefficient and thus the impulse response length, causing misleading estimates of the communication performance.

Predicted vs observed communication performance

Predictions of communication performance at the UAN10 P2P tests were carried out by COMLAB simulations, using the environmental model described above. The emitted signals in the simulations were computer-generated random messages with the same parameters and encoding formats as those of the FOI signals used in the trial. The source at the P2P tests was the Portable Acoustic Source Unit (PASU) [12, p. 22], deployed at depth ca 10 m. The source and encoding parameters are listed in table 1. The corresponding total and net bit rates in kbits/sec are shown in table 2.

For each source position S1,...,S4 the performance of communication to the receiver (VA in figure 1) was predicted by COMLAB simulations of ten cases. Each case corresponded to one of the five modulation formats using one of two receiver subsets (all 8 receivers and the top receiver only, respectively) in the decoder.

source level	155 dB rel 1µPa
carrier frequency	10 kHz
symbol frequency	3.5 kHz
modulation format	04QAM, 16QAM, M32QAM, M64QAM, 128QAM
interleaver size	644 if 128QAM, else 640
number of training symbols	255
code rate	1/3
number of frames in message	15

Table 1: Source parameters and encoding formats for computer generated random messages used in the simulations.

	04QAM	16QAM	M32QAM	M64QAM	128QAM
Total bitrate	7.00	14.00	17.50	21.00	24.50
Net bitrate	1.78	2.93	3.36	3.72	4.05

Table 2: Total and net bitrates (kbits/sec) in the P2P communication tests

The signal to noise ratio in the experimental data was found to disagree significantly with model predictions, by showing strong irregular variations with source position, receiver number and time. Therefore, to prevent effects of grossly erroneous SNR from influencing the validation results, the communication performance predictions were carried out with the SNR values at the receivers set to those in the experimental data.

The validation results are summarized in tables 3 and 4 showing the predicted and the experimentally observed frame error rate (FER) in percent as function of source position and modulation format. The table entries are colour coded according to their values, green for FER = 0, blue for 0 < FER ≤ 25 and black for 25 < FER ≤ 100.

	Predicted				Observed			
Modulation	S1	S2	S3	S4	S1	S2	S3	S4
04QAM	0	0	0	0	0	0	0	0
16QAM	0	0	0	0	0	0	8.9	0
M32QAM	0	0	6.7	0	3.3	0	24.4	0
M64QAM	0	100	0	0	6.7	1.3	2.2	0
128QAM	100	26.7	100	0	70.0	37.3	94.4	1.9

Table 3: Predicted and experimentally observed frame error rates (percent) using all 8 receivers.

	Predicted				Observed			
Modulation	S1	S2	S3	S4	S1	S2	S3	S4
04QAM	0	0	0	0	0	1.3	0	0
16QAM	0	0	0	0	14.8	4.0	56.7	16.7
M32QAM	0	0	93.3	0	51.9	72.0	95.6	53.3
M64QAM	100	73.3	100	0	90.4	97.3	100	92.2
128QAM	100	100	100	100	100	100	98.9	98.9

Table 4: Predicted and experimentally observed frame error rates (percent) using the top receiver only.

Comments on the validation results

The predicted and the experimentally observed communication performance show a qualitatively similar dependence of (i) using a single vs all receivers of the array for the decoding (ii) modulation format. The predicted communication performance is, however, better than the experimentally observed, by the numbers of (modulation , source position) combinations allowing error-free communication being 27 and 13, respectively.

The difference indicates influences from performance degrading effects not accounted for in the modelling. Such effects include unmodelled environmental influences such as significant amplitude variations of the surface reflected sound induced by surface waves, unmodelled surface-wave induced movement of the transmitter, unmodelled fine-scale spatial and temporal variations of the sound speed, and unknown degradation of the data quality by the transmitter and the receiver hardware.

A second validation of the performance prediction method and the COMLAB software is in progress, against field data from the P2P tests of the UAN11 trials at Trondheim in May 2011. In these tests the communication performance was observed to be significantly better than at Pianosa, promising a model vs. data comparison of the UAN11 trials to provide a valuable complement to the Pianosa results.

Corrections

This task and work package is terminated and no corrections are deemed necessary.

WP3 – Underwater communication physical layer

Summary of progress

Milestone 3.2 *Working modem pair concluded and tested at sea* was achieved in Feb 2011. Verification of the turbo equalizer implementation was done in a dedicated sea trial in Oslofjorden, Norway, were stable communication of up to 1800 m range was demonstrated. The results for the milestone were presented in a paper in April for the IEEE Oceans 2011. Deliverable D2.2 was delayed, but submitted at the very end of the project with no substantial impact on the project.

Main achievements

The overall main achievement in this period was finalizing the implementation of the turbo equalizer on the modem platform. Work in Task 3.3 has progressed with KM doing the coding of the Turbo equalizer on to the modem based on Matlab code supplied by FOI. The coding has been done mainly in C++ (some critical parts in ASM) manually converted from Matlab code. Benchmarking of the C++/ASM implementation towards the Matlab code was done using sea trial data logged in the modem; the modem implementation could be considered bug free when similar performance was experienced in the modem as in the Matlab code (using the same equalizer lengths and other parameters). The modem was concluded and tested at sea in February 2011 reaching milestone M3.3 Working modem pair concluded and tested at sea with a one month delay. After this was the implementation incrementally improved before the engineering test March 2011 in Algarve and the final demonstration in May 2011 in Trondheim.

There has been a close cooperation between FOI and KM in the period, with numerous phone conferences and also a dedicated implementation meeting 2011-01-19 taking place in Stockholm. Modem hardware was brought for hands on collaboration. The focus has been to get the functionality up first, thereafter refining the performance where the effort pays of best.

Sea Trials

Dedicated sea trials for the turbo equalizer implementation have been performed according to the table below. Kongsberg Maritime test vessel Simrad Echo has been used for the testing.

Date	Area	Test objective
2010.08.13	Oslofjorden, Breidangen	First test of turbo decoder
2010.12.09	Oslofjorden, Breidangen	First test of turbo equalizer
2011.01.26	Oslofjorden, Breidangen	Continued test of modem
2011.02.11	Oslofjorden, Breidangen	Verification test of modem
2011.02.24	Horten harbor, Målfrid test barge	Trigger level measurement
2011.05.04	Oslofjorden, Breidangen	Test of improvements
2011.05.10	Oslofjorden, Breidangen	Test of improvements
2011.05.16&18	Horten harbor, Målfrid test barge	Test before final demo

Results from the tests 2011.02.11 and 2011.05.04 are reported in Deliverable 3.3. The results from the February test are also published in a conference paper Oceans 11 with co-authors from KM, FOI and SINTEF. Figure 5 illustrates the success rate for transmission towards a bottom node as a function of communication distance. Relative stable communication is achieved up to 1800 meters range in this particular case.

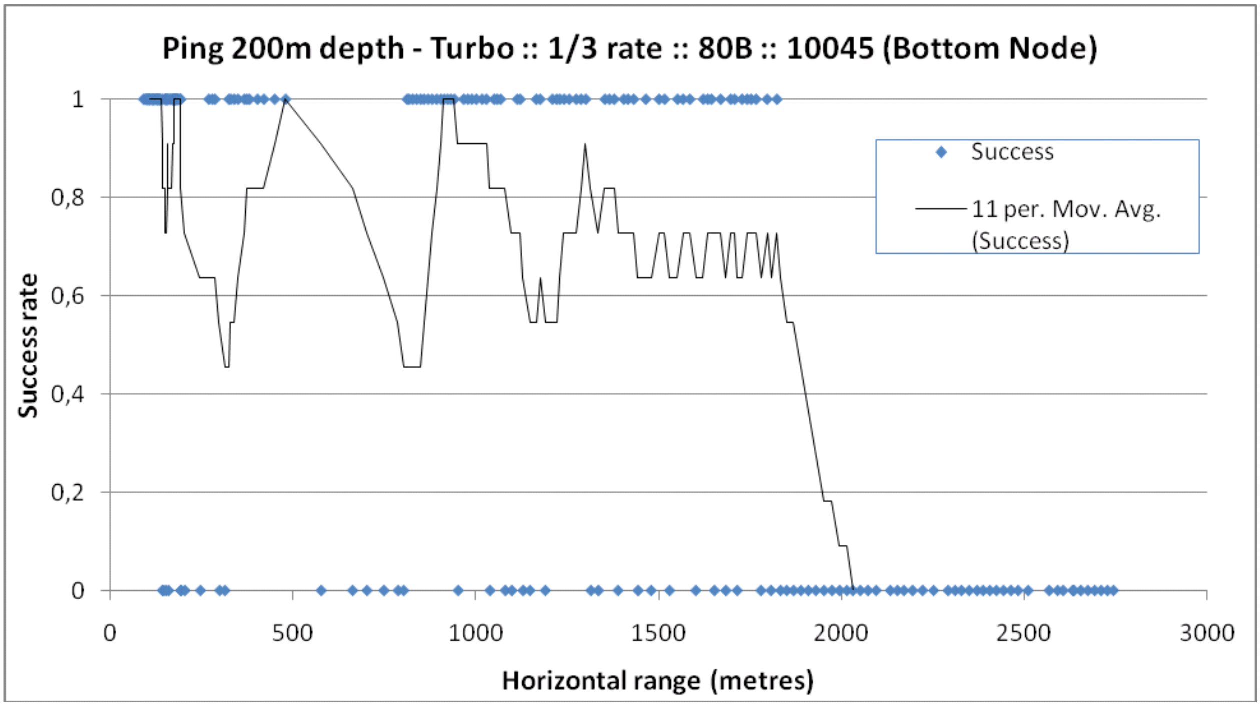


Figure 5: success rate transmissions towards a bottom node as a function of communication distance.

Trondheim demonstration aftermath

The modem implementation of the turbo equalizer did not perform well in Trondheim and a direct sequence spread spectrum signal (DSSS) format with 200 bps was used in the modems for the network tests. The logging of all signals at the vertical array of the STU also captured the initial tests did with the turbo equalizer signals. FOI has analyzed a small set of these signals captured by the hydrophone closest to the master modem, and found that the Matlab model of the turbo equalizer performs well even with short equalizer lengths as in the modem. This indicates that there is room for improvements on the modem implementation.

Corrections

Much work and focus has been spent on optimizing the turbo equalizer implementation and also preparing the upper layer functionalities of the modem for the final demonstration in May. After completing milestone M3.3 Working modem pair concluded and tested at sea in

February, the writing of deliverable D3.3 was not prioritized. The main results of D3.3 were presented in the Oceans 2011 paper submitted in April. D3.3 was delivered at the very end of the project with no impact on other project work packages.

WP4 – Acoustic communications and environmental-based optimization

Summary of progress

Under WP4, only Tasks 4.3 and 4.4 were active during this third year and only during the first six months. Regarding the hardware development in Task 4.2 (already terminated), an article discussing the design of UAN nodes was published in Sea Technology [13]. Moreover, due to equipment damage during the UAN’10 sea trial, the STU repair was carried out in preparation for the upcoming project main sea trial. Furthermore, in March 2011, an integration workshop was organized to bring people involved in the hardware development and configuration of the various work packages to implement and/or define the final version of the functional UAN network for the UAN’11 final demonstration experiment foreseen for the end of May 2011.

Task 4.3 dealing with environmental equalization algorithm implementation has terminated during this period. The performance of the developed algorithm was shown using simulated data from the Time-Variable Acoustic Propagation Model (developed in Task 4.1) and data collected during the UAN’10 experiment as well as that collected previously from RADAR'07 sea trial (conducted off Setubal (Portugal) in 2007, under project RADAR, contract POCTI/CTA/47719/2002, funded under POCTI program from FCT (Portugal)). Moreover, the performance of the new environmental equalizer was evaluated in face of environmental and geometric variations. The attained performance was compared with those of the current state of the art equalizers. The work developed for this task was reported in Deliverable 4.5.

Task 4.4 dealing with the spread-spectrum communications was terminated during this period. The data collected during UAN’10 engineering test was used to evaluate the performance of the processing scheme and the results were reported in Deliverable 4.6.

Main achievements

During project UAN 3rd year, the major contributions of WP4 were: (i) in Task 4.3 the development and implementation of an high data rate link for the UAN-network, and (ii) in Task 4.4 the development of an high secure spread spectrum data link.

In Task 4.3, a combined geometry-adapted passive Time Reversal (pTR) and Decision Feedback Equalizer (DFE) technique for time-variant underwater communications, was proposed. High data-rate and sustainable communications for moving source (implying geometry changes) are considered. Such changes can be compensated by employing a frequency shift on probe impulse response in pTR processing. The geometry-adapted pTR is referred to as Frequency Shift pTR (FSpTR). In practice, the FSpTR can not completely eliminate Inter-Symbol Interference (ISI). Hence, a DFE is applied to mitigate a residual ISI (caused also by environmental changes), and the technique is called FSpTR-DFE. Two experimental data (from RADAR'07 and UAN'10 sea trials) and simulated data (from the acoustic channel model developed in Task 4.1). Temporal coherence is shown to be a key factor, determining the performance of pTR-based techniques. Since the FSpTR improves the coherence over the pTR, the FSpTR-DFE outperforms the pTR-DFE. Without explicit channel tracking, the FSpTR-DFE exhibits a sustainable performance upto 50s in 1.4 m/s source speed. The FSpTR-DFE results are also compared with MultiChannel DFE (MC-DFE) scheme, where the MC-DFE is more sensitive to synchronization and Doppler estimation, although its performance can be superior. Moreover, the simulation studies of the effects of environmental and geometry changes, as well as signal frequency on the coherence are carried out to explain the experimental results.

The main objective of task 4.4 was to investigate and implement spread spectrum techniques for the underwater acoustic communication able to guarantee a good level of message privacy and to reduce the probability-of-intercept. Within the third year of project, the work of the task 4.4 focused on the evaluation of the spread spectrum techniques developed in WP4 on the basis of the data acquired during the UAN10 engineering sea trial in Pianosa island, Italy. The results of the analysis were reported in details in the project Deliverable 4.6, “Evaluation of the Spread Spectrum Technique”. The analysis of field data is briefly summarized in the following of the section. The main conclusion is that the proposed method allows one to perform a point to point underwater acoustic communication able to guarantee a good level of privacy and covertness. The chosen method, based on a direct sequence spread spectrum approach and differential PSK modulation, can be considered a good trade-off between performances and simplicity: it allows to overcome the problems connected to a perfect knowledge of the signal phase offering anyway good performances in terms of error probability. In reception, a rake receiver that takes advantage of the multiple propagation paths together with an adaptive Doppler tracking procedure that corrects the instantaneous Doppler shift has been devised and tested. The analysis of the received data during the UAN10 engineering test showed that the developed communication algorithm is able to handle the multipath phenomenon and variability of the underwater channel, allowing one to achieve the expected performance at a bit rate equal to 133 bits/s. Analysis of experimental data has shown that problems may occur for some blocks of bits when only one channel is considered in the decoding procedure, due to synchronization issues, and possibly for the lack of the postamble in the transmitted sequences. The problem has been faced considering more than one channel in the decoding process, exploiting the information on the number of energetic paths for each bit given by the Rake receiver for multiple channels.

Task 4.3 – Environmental equalization algorithm implementation

For high rate coherent communications, underwater channels are very challenging due to their complex multipath structure, rapidly time-varying fading and large Doppler. The large multipath delay spread causes a severe ISI. The time-variant fading and Doppler shift caused by surface waves and the relative motion between a source and a receiver are inevitable, and more prominent for a fast moving source/receiver, such as when autonomous underwater vehicles are employed. To combat such severe conditions, a receiver array providing spatial diversity is usually required in practice, and also considered in this project at the base station to make possible the transmission of images of potential threats in the UAN network.

In this work, a passive time reversal technique which is a one-way communication from a source to a receive-only array, is considered. In a pTR communication system, the source first transmits a probe signal to sample the multipath characteristics of the channels. Then, a data-bearing signal is transmitted. At the receiver, the array of received data signals is cross-correlated with the corresponding array of time-reversed received probe signals and spatially combined to provide the pTR output. With a dense and long receiver array and static channels, the pTR technique having the pulse compression (focusing) property can eliminate the ISI problem. However, in practice, such ideal conditions are never realized and a residual ISI always exists. To address the time-varying channel problem, caused by a moving source/receiver, the geometry-adapted pTR technique was considered. It was shown that by employing a frequency shifted version of the estimated channel impulse response in the pTR processing, the focusing property of the pTR can be partially restored over time-variant channels. Such technique is referred to as FSpTR. Although the FSpTR-technique can mitigate the ISI problem, an equalizer is required to eliminate the residual ISI as well as to cope with channel variability caused by environmental changes. Hence, the performance improvement of the FSpTR-technique using an adaptive DFE, termed FSpTR-DFE, was proposed. For the FSpTR-DFE implementation, a slot-based processing is performed where frequency shifts applied to the IRs can change over slots to compensate for geometry changes over time. The FSpTR output is the concatenation of slots of the processed signals. With different frequency shifts for consecutive slots, there are phase jumps in the FSpTR output. WP4, Task 4.3 addresses the phase jump problem and proposes two compensation methods so that a standard PLL can be used for phase synchronization and the DFE can be applied to further eliminate residual ISI (from the FspTR).

To demonstrate the performance of the pTR-DFE and FSpTR-DFE techniques, simulated data obtained from the TVAPM (reported in Deliverable 4.1 and available in the UAN web page http://www.ua-net.eu/projects/simulator/) , as well as, experimental data from the RADAR’07 and UAN’10 experiments were used. During the UAN’10 experiment, BPSK modulates singals were sent from Portable Acoustic Source Unit (PASU) (see Deliverables 4.1 and 4.5), with user-defined bit rates, frequency bands, powers and geometries. Moreover, QPSK modulated signals were transmitted from the KM-modem (in transparent mode, see Deliverables 3.1, 3.2 and 4.5) with the pre-defined powers, bite rates and frequency band.

During those transmissions, environmental data was collected for futher analysis of the influence of environmental variability on the equalizers' performance. Figure 6 shows a performance comparison between the pTR-DFE and FSpTR-DFE, using UAN'10 data. It is observed that the performance loss of pTR-DFE (a) in face of geometric change and environmental variability, showing by the increase of Mean Square Error (MSE) over time, whereas the FSpTR-DFE is more stable (b). Figure 6 (c) and (d) shows the resulting constellations, associated with pTR-DFE and FspTR-DFE, respectively.

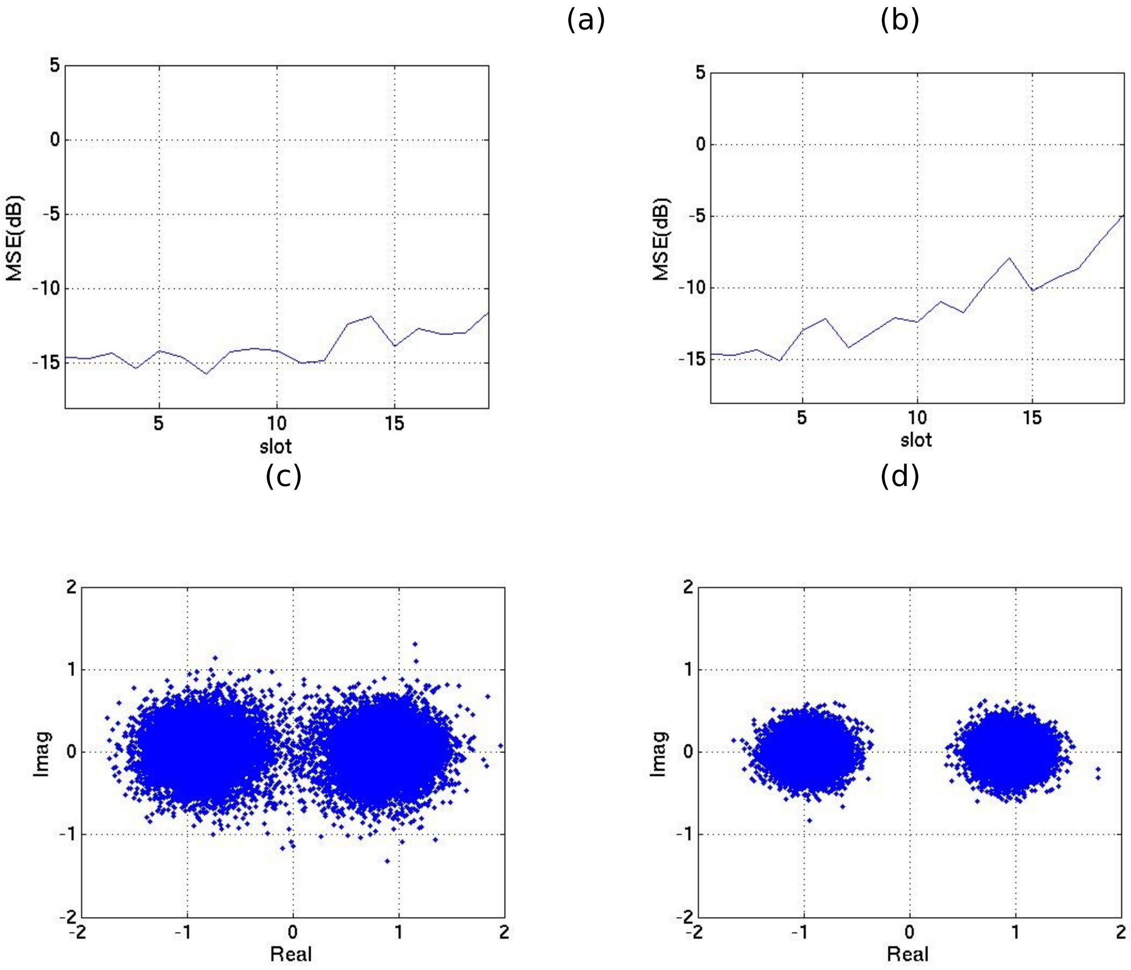


Figure 6: Performance of pTR-DFE and FSpTR-DFE schemes obtained with UAN’10 data: MSE of pTR-DFE (a), MSE of FSpTR-DFE (b), Demodulated BPSK constellation for pTR-DFE (c), and Demodulated BPSK constellation for FSpTR-DFE (d).

The FSpTR-DFE provides a performance gain over the pTR-DFE, and an error-free communication is achieved. Temporal coherence is shown to be a key factor, determining the performance of pTR-based techniques. The benefit of the FspTR over the pTR is to improve the channel temporal coherence, under geometric changes, and a much longer channel coherence time is obtained for the FSpTR as compared to the pTR, resulting in a performance gain. The performance of the FSpTR-DFE technique was also compared with the bench marking MC-DFE scheme. The results show that the MC-DFE can provide a better performance than pTR-based techniques, but requires a longer training sequence and is more complex and more sensitive to synchronization problems (that can cause the MC-DFE malfunctioning). Deliverable 4.5 reports these results in details.

The influences of the channel temporal coherence on the pTR-based communication systems observed in this work lead to the simulation studies of the effects of wind-induced surface waves, geometry changes (range and depth changes) as well as signal carrier frequencies on the channel coherence. We observe that the channel temporal coherence drops rapidly as wind speed, source speed and acoustic signal carrier frequency increase, showing that environmental parameters have a strong impact on the channel temporal coherence, and in turn determine the performance of pTR-based techniques. It was also observed that FSpTR technique can improve the temporal coherence dropped due to geometric changes. Hence, the FspTR combined with DFE to further cope with other environmental changes, could be a candidate scheme for high data rate, sustainable and reliable point-to-point communications over time-varying underwater channels that satisfies the objective of the WP 4, Task 4.3. The compensation for the temporal coherence loss caused by surface waves would be an interesting topic for future work. The work conducted in Task 4.3 results in the implementation of the acoustic Uni-SIMO data links of the overall UAN-network. During the UAN’11 experiment, the high data rate (upto 8000 bps) with low error rate Uni-SIMO links offered the successful transmission of potential threat images from the remote nodes to the Command and Control. Figure 7 shows an example of a simulated threat image. In the third year of UAN project, this work in Task 4.3 was published in two papers in the OCEANS’11 conference [14,15,16] and was submitted for publication in IEEE Journal of Oceanic Engineering [17].

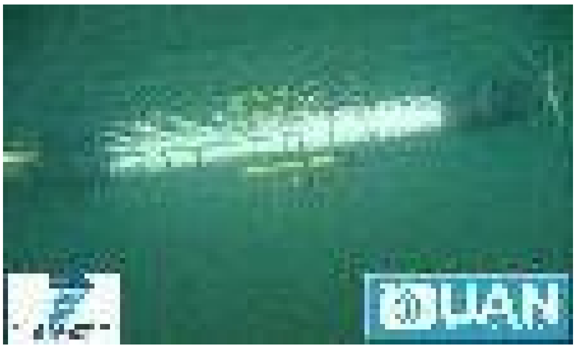


Figure 7: Simulated threat image transmitted during UAN’11.

Task 4.4 – Development of spread spectrum transmission schemes

The main objective of task 4.4 was to investigate and implement spread spectrum techniques for the underwater acoustic communication able to guarantee a good level of message privacy and to reduce the probability-of-intercept. All the technical details of the chosen methodology have been reported in detail in the project Deliverable 4.4 "Spread Spectrum Transmission Algorithm" and we only report here some of the main features and characteristics of the method:

- The developed scheme is based on a PSK direct sequence spread spectrum.
- The choice of pseudo noise sequences allows one to reduce narrowband interference arising from other users and self-interference due to multipath propagation.
- The solution employs differentially coherent modulation and it is based on the assumption that the channel does not vary significantly during two bits intervals. On the receiver side, a Rake receiver can be used to exploit the energy present in multiple propagation paths.
- A step of synchronization and parameter estimation necessary for Doppler and compensation is performed before the decoding operation. Moreover a tracking procedure that allows an adaptation to the instantaneous Doppler shift has been devised and tested.

After the validation on simulated data, SS-ISME signals have been tested on real data acquired during the UAN10 engineering tests. Table 1 reports the parameters characterizing the specific transmission:

Technique	Direct Sequence Spread Spectrum
Modulation type	BPSK with differential encoding
Bit rate (information rate)	133.3 bit/s
Chip rate	2000 chip/s
Spreading factor	15
Radio-frequency bandwidth	< 4 kHz

Table I: Transmission Parameters

The single transmitted signal has a specific data format:

Duration:	0.19 s	25 s	0.19 s
Signal:	Known preamble	Message (1 s × 25)	Known postamble

where:

- The preamble is made of six periods of a Gold pseudo noise sequence.
- The Gold sequence period is composed of 63 chips.
- The postamble is equal to the preamble.

The information bits are differentially encoded. The bits relative to 1 second of transmission are repeated 25 times. Each bit is multiplied by a Gold sequence made of 15 chips. The final chip rate is equal to 2000 chips/s.

Signals were transmitted using the KM modem transducer as source. The master KM modem was operated at 10 m depth. The signals have been received by the Vertical Array (VA) composed of 8 hydrophones. Unfortunately, due to technical problems, only a portion of the entire signal has been transmitted; in particular the known postamble is not present in the received signals preventing a further check of synchronization and Doppler shift at the end of the Rake receiver procedure. The system configuration used is shown in Figure 8.

For each run the signals received from the vertical array (8 hydrophones) have been recorded. The carrier frequency is equal to 25600 Hz; the sampling frequency is equal to 60000 Hz. The acoustic data here reported have been recorded on September 21, 2010 and refer to one hour and half of transmission.

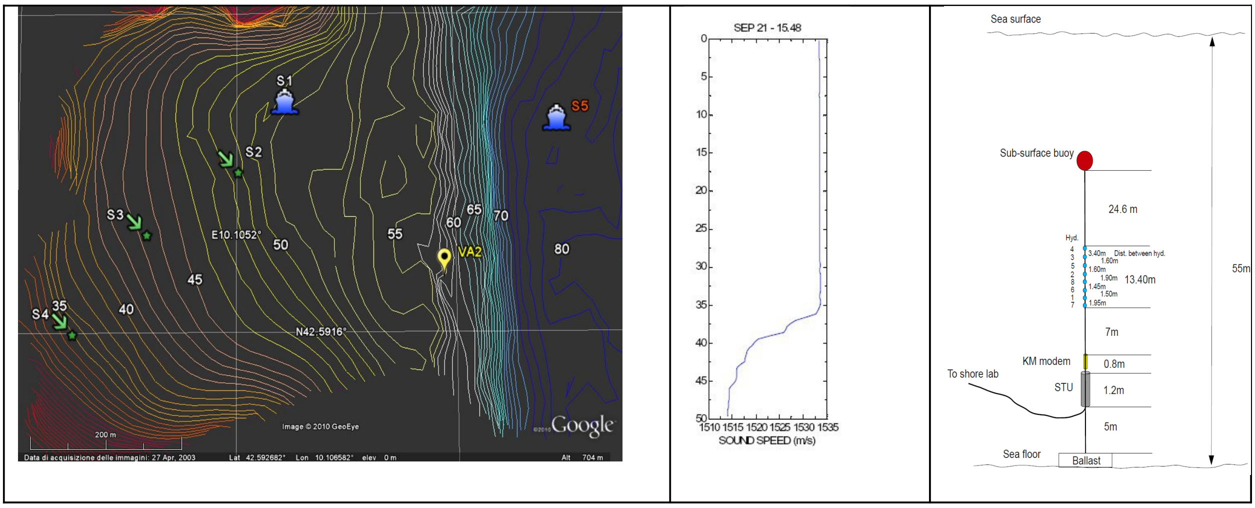


Figure 8. Left: Bathymetry in the region; Middle: measured sound speed profile; Right: VA configuration. Note that the water depth reported is the nominal water depth at deployment; indeed, from the bathymetric data it results that the ballast was at 58 m depth.

A blind decoding (with no information about environmental data) has been performed. For each analyzed received signal the following steps have been performed:

- Doppler estimation (ambiguity function);
- Synchronization
- Rake receiver with Doppler compensation.

The system parameters used are as follows:

- Block size for the Doppler tracking procedure: 5 bits;
- Rake receiver fingers: 5.

Without entering into the analysis details (see D4.6 for more information), it is worth noticing here that thanks to the complementary behavior of the two vectors at the Rake receiver it is possible to recover incorrectly decoded bits. Finally, the algorithm is able to exploit the information received by another hydrophone to provide a better estimation of the message: by merging the information relative to both channels, thanks to the evaluation of the multipath counters vectors provided by the rake receiver it is possible to improve the overall result.

WP5 – Mobile ad-hoc network coordination and implementation

Summary of progress

WP5 was almost concluded at the end of year 2. The remaining part of the work to be concluded in Year 3 consisted in completing the reporting of the UAN10 engineering test in Pianosa Island, concluded at the very end of Year 2. Conclusion of the field data report (Deliverable 5.3) took longer than planned, due to the wealth and richness of activities that the Project team was able to pursue during the UAN10 Pianosa test. The delay in the delivery of the final version of the report did not affect the other activities in the project.

Corrections

As a consequence of the Reviewers' comments at the second year project review, the security suite designed within Task 5.3 had to be upgraded. As agreed, the upgrading has been moved to WP 6, in particular within Task 6.2 (see also “Corrections” in WP6 section)

WP6 – Systems integration, experimentation and validation

Summary of progress

The main WP6-activities in year 3 were carried out under Task 6.2 (T6.2), *Integration*, and Task 6.3 (T6.3), *Experimentation and validation*. In addition, under Task 6.1 (T6.1), Communication and Networking, the final implementation of an IP interface between PCs and acoustic modems was completed.

T6.2, led by Selex, has integrated the underwater network into a complete wide area surveillance system. The task is completed by submission of the corresponding deliverable, D6.2. T6.3 , led by SINTEF, has prepared and executed the final Project Sea Trial. The sea trial is denoted UAN'11 in the following. The task too is completed by submission of its deliverable, D6.3. In total it is fair to claim that the overall goal of WP6 has been achieved through UAN'11. An integrated UAN system has been tested and demonstrated. This includes also the underlying tests of the key system components.

An upgraded version of the security suite devised for the MOOS pub/sub system has been implemented, integrated within the Selex SI system and tested at two additional engineering test (Faro and Genova).

During the final UAN10 sea trial, the UAN system has been tested with all its layers, including MOOS at first in its non-secure form and then activating all the network security features. The whole MOOS middleware, both in its non-secure and secure form, behaved as expected showing robustness during all the different phases of the communication. Interruption of any of the underneath network layers did not cause any problem and both the clients and the database were always able to adapt to the communication conditions correctly. The modifications implemented in order to simplify the handshake phase and to adapt the application layer to the constraints of the other layers of the network, which were required after the analysis of the Pianosa data, gave very good results allowing for a quick establishment of the client-server connection with a reduced communication overhead. MOOS was used during the whole experiment using UDP as transport protocol without any problem in the data received and transmitted. Mission control acoustic commands from the C2 were received, acknowledged and successfully accomplished. According to the adaptive cooperative algorithm described in deliverable D5.1, Folagas were able to identify, from an application level point of view, abrupt interruption in the communication. In particular, the Folaga were able to identify its moving in an area were the acoustic communication was lost (no MOOS messages were received for more than 15 minutes) and autonomously started to move towards the vertical array where the communication could have been re-established.

Main achievements

Task 6.1 – Communication and networking

The integration of acoustic modem (KM modem) and middleware host was done using a Linux host for the middleware, and connecting physically these components using legacy serial line (RS-232). Since the MOOS middleware was implemented using IP-sockets, the modems were given an IP interface using the PPP protocol. The first version used a kernel driver in order to have tight latency control. Due to lack of flexibility during testing, the kernel driver was exchanged with a user mode operated PPP. In the last period before UAN'11, the PPP was exchanged with a TUN/TAP interface to improve flexibility and p2p connection time. Any of these technologies provided one IP interface per slave modem on the master, and one IP interface in each slave modem. The underwater hop-by-hop routing and MAC protocol was still controlled directly in the modems.

Task 6.2 – Integration

Upgraded Secure MOOS

In this section we describe the details of the cryptographic suite conceived to add security to underwater network communication while limiting the ensuing overhead. In particular, we focus on the middleware layer, and use the cryptographic suite to extend the MOOS (Mission Oriented Operating Suite) publish/subscribe system to provide confidentiality, integrity and authenticity of messages. We call Secure MOOS (SecMOOS) the resulting system. A first version of the suite has been described in the UAN Deliverable 5.3 (Ref. 3), including implementation details. While most of the implementation aspects remain unchanged, in this chapter we report on the rationale and choices for the selection of upgraded security primitives. Moreover, this chapter has a final subsection with dedicated bibliography; citations within the chapter are referred to the dedicated bibliography section.
In any network scenario similar to that of the UAN project, communication bandwidth is limited, propagation time is very long, and vehicles have limited energy resources as they are battery operated. It follows that cryptographic algorithms and protocols for underwater acoustic network must be communication efficient in terms of number and size of messages. Applying traditional techniques such as ciphers, digests and digital signatures requires particular attention because they make message expand so introducing an amount of overhead that is often comparable to or, even, larger than the payload itself. For these reasons, we propose the use of a cryptographic suite that provides confidentiality, integrity and authenticity while keeping at minimum message expansion. Such a suite was presented at the 16th IEEE International Symposium on Computers and Communications (ISCC 2011) [18].

The MOOS (Mission Oriented Operating Suite) framework is a centralized publish/subscribe system, composed of a central server, called the MOOS-DB, and multiple clients, i.e., the underwater fixed and mobile nodes. Publish/subscribe is a communication paradigm that supports dynamic, asynchronous, many-to-many communication. Every client can act as both a publisher and subscriber. A publisher is a client which sends messages, while a subscriber is a client which receives messages. The MOOS-DB is responsible for routing messages from publishers to subscribers. Messages are routed based on their topics, an information descriptor contained in the messages themselves. Subscribers have to declare their interests in specific topics by issuing subscriptions to the MOOS-DB. In order to avoid bursts of short messages, these are grouped in packets. A packet can contain messages having different topics.

We assume an external adversary, equipped with an acoustic modem and thus able to perform snooping and spoofing attacks. The snooping attack is a passive attack aimed at the unauthorized interception of information. In a UAN, an adversary performing snooping could have full access to environment measures or statistics and could use them to prepare other kinds of attacks. The spoofing attack is an active attack aimed at the impersonation of a legitimate node of the network. In the UAN scenario, an adversary performing the spoofing attack could impersonate a legitimate node by injecting wrong measures and data. This could lead to wrong results or even to the violation of the system integrity.

In order to protect the network from the described threats, we organize the vehicles and the MOOS-DB in a secure group. All the members of the group share two symmetric keys: the Integrity Key (IK) and the Encryption Key (EK). The Integrity Key IK is used to authenticate message, while the Encryption Key EK is used to encrypt/decrypt messages. A cryptographic suite for UAN must take into considerations the severe limitations of the underwater networking environment in terms of very high message propagation delay, very low bandwidth, and high energy consumption for communication. Limitation in the message size is hence of paramount importance in order to reduce transmission time and battery consumption in AUVs. In the reminder of the section we describe the technical solution we have adopted to limit message expansion due to cryptography.

The MOOS-DB implements the cryptographic suite, used to provide both confidentiality, integrity and authenticity of messages. Confidentiality of messages is achieved by encrypting messages. Encryption is achieved by splitting clear text in blocks of fixed, predefined bit-length and encrypting each single block. In the most general case, clear text length is not a multiple of the cipher block. Thus padding is necessary. However, padding has the negative effect that the cipher text may result up to one block longer than the corresponding clear text. This effect is called cipher text expansion. Finally, another form of cipher text expansion derives from the concatenation of an authenticator or a digest for authenticity and integrity purposes. While the effects of cipher text expansion are negligible in a traditional network, they become relevant in a wireless sensor networks (WSN) and, in particular, in underwater acoustic networks. For example, the average payload size of a UAN message is about 78 bytes (see Deliverable 5.2). Therefore, enciphering it with AES requires a 16 bits padding as the AES block size is 128 bits. This implies that security introduces a message expansion that amounts to about 2.5% of the average payload size. Similar considerations can be done in the case of concatenation of an authenticator or a digest. With hash functions the situation gets even worse. As a further example, SHA-256 builds a 256-bit digest that results around 41% of the average payload size. Cipher text expansion has been addressed as follows. In order to completely avoid the cipher text expansion problem due to encryption, we use the Cipher Text Stealing (CTS) method that alters the processing of the last two blocks of plain text, resulting in a reordered transmission of the last two blocks of cipher text and no cipher text expansion [19].

Encryption without authentication is insecure [20]. For example, an adversary may flip bits in unauthenticated cipher text and cause predictable changes in the plain text that receivers are not able to detect. To address this vulnerability, the MOOS-DB 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 [21]. An adversary has 1 in 232 chances to blindly forge a digest. If an adversary repeatedly tries to forge it, he/she needs 231 trials on average. However, the adversary cannot perform trials 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 231 messages in order to successfully forge a single malicious message. In a conventional network this number of trials is not large enough. However, in a underwater acoustic network this may 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 231 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 adversary needs to occupy the acoustic channel for a long time. Fortunately, it is feasible to detect when such a attack is under way. UAN uses a simple heuristic: vehicles could signal the base station when the rate of digest/MAC failures exceeds some predetermined threshold.

In the prototype of SecMOOS, we have opted for an off-line key distribution at pre-deployment time. This choice is mainly motivated by the communication and energy limitations: we want to keep low the number of transmitted messages. For this reason we avoid the overhead of a key distribution protocol. However, if some form of re-keying is necessary, we have proposed to employ S2RP, a group key management protocol originally conceived for wireless sensor networks [18]. S2RP is particularly suited for UAN too because it has a very reduced communication overhead [22]. Actually S2RP requires a number of messages that is logarithmic in the number of nodes. Furthermore, newly distributed keys are self-authenticated by means of key-chains, a well-known mechanism deriving from Lamport’s one-time passwords [23], and thus do not require any form of authenticator, thus avoiding message expansion. SecMOOS has been designed in order to be configurable and support various ciphers and hash functions. The main aim is to accommodate off-the-shelf secure cryptographic algorithms. For this reason SecMOOS is based on the OpenSSL 0.9.8g security library and supports several block ciphers, including AES and Camellia, and hash functions, including MD5, SHA-1, and SHA-2 (SHA-256). The default choices are AES as block cipher and SHA-256 as hash function. This choice has been motivated by the following considerations.

Law et al. have made a survey and a benchmarking of block ciphers [24]. Their main aim consists in identifying and selecting the most suitable ciphers for WSNs in terms of both security and efficiency. Of course they consider computing platforms (i.e., sensor nodes such as Smart dust or Intel Mote) that have severe restrictions in terms of computing power, available storage and available memory. Therefore, their considerations about efficiency may be less stringent for us who use Linux Ubuntu 10 running on a PC104 that is essentially equivalent to a customary personal computer. However, their considerations about security are quite general and thus apply to our case too. Of course, we are not going to repeat these considerations here and refer the interested reader to the paper. We simply recall their conclusions that, according to recommendation of NESSIE [25] and CRYPTREC [26], AES (www.rijndael.com) and Camellia (http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html) can be considered secure and they are good performers on a wide range of platforms.

As to hash functions, MD5 and SHA-1 cannot be considered secure anymore. For instance, the complexity of a recent attack against the collision resistance property of he NIST-approved SHA-1 is 263 [27]. It follows that the strength of SHA-1 against collision attacks is weaker than ideal, namely 280 [20]. For this reason, SHA-1 is considered somewhat flawed [28]. Similar considerations hold for MD5, too. Thus, one should wisely use other hash functions, e.g., RIPEMD-160 [29] or SHA-256, with no known flaws and that use the same basic operations as SHA-1. Furthermore, NIST announced a public competition on November 2, 2007 to develop a new cryptographic hash algorithm [30]. The winning algorithm will be named "SHA-3", and will augment the hash algorithms currently specified in the Federal Information Processing Standard (FIPS) 180-3, Secure Hash Standard. The winner will be definitely selected in late 2012.

Notwithstanding these considerations, it is worthwhile to notice the following observations that allow us to make a somewhat relaxed choice oh the hash algorithm, First, SecMOOS certainly relies on the unique properties of the cryptographic one-way function but, while the most of attacks are against collision resistance, the relevant property for SecMOOS is resistance against preimage attacks. MD5 and SHA-1 are still considered secure against this kind of attacks. Second, SecMOOS requires hash truncation for performance reasons (see Section 3.1) which reduces digest length without any detriment to security.

The MOOS framework originally was thought as a middleware working inside a single vehicle. In particular, it managed communication among modules inside the same vehicle by using the TCP protocol. We have extended MOOS in order to allow communication among vehicles. Due to the many restrictions introduced by the underwater channel, the TCP protocol is not indicated, because of its additional overhead introduced to manage connection. Thus we have implemented a UDP version of MOOS. UDP is a connectionless protocol so that if a packet gets lost, it is not retransmitted. Each MOOS Client is composed of the Security Engine and the Communication Engine. The Security Engine provides the cryptographic suite, and the Communication Engine manages the transport communication between the client and the MOOS-DB.

The Security Engine is implemented as the following C++ class:

```
class SecurityEngine
{
    void encrypt(msg, ciphertext);
    void decrypt(msg, ciphertext);
    void generate(msg,mac);
    bool check(msg,mac);
}
```

The encrypt() and decrypt() methods encrypt and decrypt the message, while the generate() and check() methods generate and check, respectively, the MAC of the message. In particular, the check method returns TRUE if the authenticity verification of the message succeeds and FALSE otherwise. The encryption/decryption and generate/check methods can be applied independently. The Communication Engine is implemented as the following C++ class:

```
class CommunicationEngine
{
    void send(msg);
    void receive(msg);
}
```

The methods send() and receive() send and receive a message msg, respectively.

System Integration Test in Genova

In April 2011 the UAN architecture was tested at sea in a simplified configuration with two acoustic nodes (Folaga vehicles) integrated within a wider land-aerial network which included the UAN gateway to connect the underwater part to the land portion of the entire protection system including the Command and Control (C2) centre. Simulated aerial and land sensors were also included in the system to simulate the complete scenario. The integration test successfully tested the MOOS framework in all its functionalities and security features, verifying its robustness with respect to the unreliability of the acoustic communication. Finally the complete integration of the Folaga vehicles within the overall protection system C2 interface as developed by Selex SI was achieved.

The at-sea engineering test took place on April 28, 2011 in the tourist harbour of the Sapello Yachting and Sport Fishing Association, in a side channel of the main Genova harbour (Italy). Water depth within the channel ranges between 4 and 6 meters. During the experiment, one of the Folaga vehicle (F1) was used as a fixed-node positioned at the sea surface during the whole experiment to allow the use of the wireless antenna (see Figure 9). This vehicle was hence acting both as a node of the network and as the land-station of the UAN scheme. For this reason it was equipped with the KM modem for the acoustic communication and with a traditional radio-frequency link to be integrated into the overall protection system. The other Folaga vehicle (named F2 and shown in Figure 10) was equipped with a KM modem, for acoustic communication, and with a radio modem to be connected and controlled by a remote station located on the pier. This vehicle (F2) was free to move in the area but due to the very shallow water of the experimental area it was always kept on the surface. Both vehicles implemented the entire UAN networking stack with the exception of the routing protocol, which was not necessary because of the particular two-only-nodes configuration.

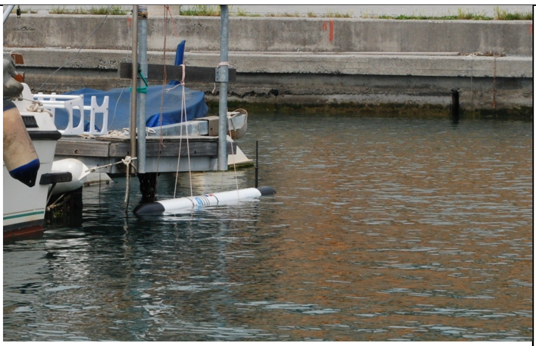


Figure 9: Folaga 1 (F1) moored to the pier. In this configuration the Folaga had the acoustic interface in the water for communication with Folaga 2 (F2) and the wireless antenna always out of the water to communicate with the UAN Gateway and hence with the Command and Control.

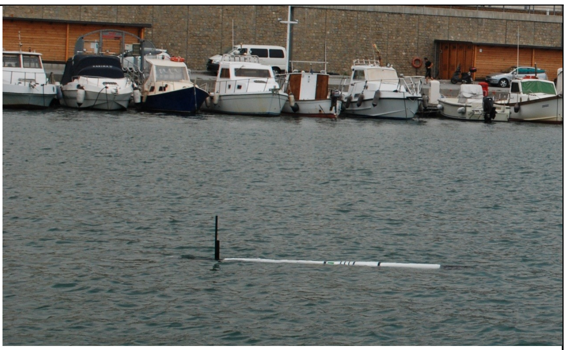


Figure 10: Folaga 2 (F2) in navigation during the test.

The acoustic channel in the area had very poor transmission characteristics, due to the very shallow water and to the presence of several scattering obstructions (the pier itself and the boats), and during the experiment very unfavourable communication conditions were experienced. In particular Folaga 2 was able to establish a reliable acoustic connection only in the small area right in front of the pier entrance (see Figure 11). The Folaga was hence able to establish a first MOOS-DB connection registering to the topics of interest. However, the further it moved from F1 position the worst the communication was with almost 100% of packets lost. In this condition, both the PPP layer and the MOOS clients were disconnected from the corresponding applications located on the master node (F1). However, when the F2 moved back inside the acoustically better area, both the PPP link and the MOOS connection were correctly re-established and the new information and status on the Folaga were showed on the command and control station, thus demonstrating robust behaviour of the tested software.

During the test all the network security services were activated and the following algorithm used:

- Encryption: AES algorithm
- Integrity: SHA2 algorithm
- Authentication: SHA2 algorithm

As expected all the clients, one running on the Folaga 1, one on Folaga 2 and the MOOS client on the UAN gateway, correctly established the MOOS connection and exchanged messages with the command and control and with each other.

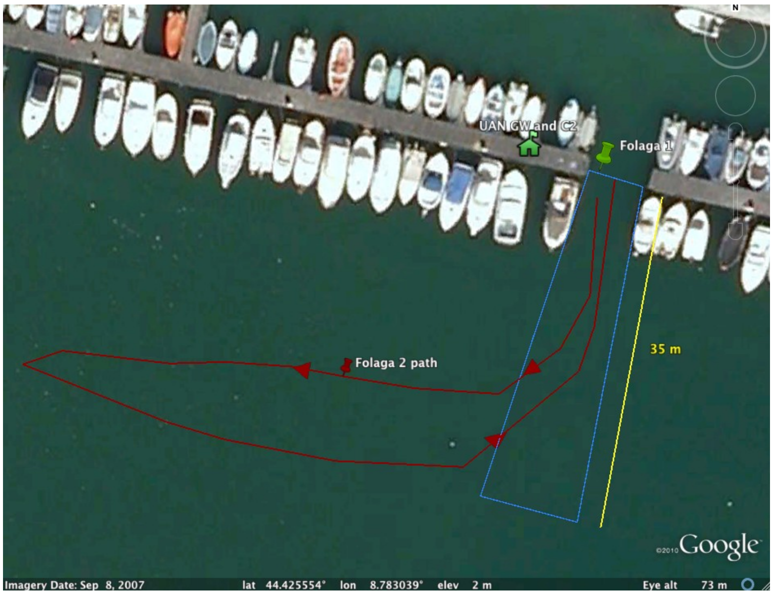

UAN GW and C2
Folaga 1
Folaga 2 path
35 m
©2010 Google
Imagery Date: Sep 8, 2007
lat 44.425554° lon 8.783039° elev 2 m
Eye alt 73 m

Figure 11: Folaga 1 location and Folaga 2 path during the test. The blue rectangle shows the only portion of the area where acoustic communication was acceptable.

Task 6.2 – Wide area integration

The general goal of deliverable 6.2 is to describe wide area scenarios for the UAN and the project of integration in a Critical Infrastructure Protection (CIP) system. More specifically, the Description of Work (DoW) identifies the following subtasks for Task 6.2: Functional analysis, architecture, and interface definition The definition of the threats and of the scenarios (WP2) is the starting point of the functional analysis. The aim of this activity is at first the definition of the dynamic behaviour of the integrated systems and to design system architecture. The functional analysis and the system architecture produce as output the identification of the human computer interface (HCI) and the software computer interface. Design and development of the supervisory command and control and relative man machine interfaces. Based on the previous activity, the design and development of the Command and Control and of the integration projects with HCI included will be performed.

Command and control evaluation

During Trondheim experiment the purpose of Selex-SI was to validate the Command and Control (C2); C2 represents the wide area context network. The validation was done by the use of two operating consoles. Figure 12 shows the integration of the underwater network in the wide area surveillance system (see "Conclusion" paragraph of deliverable 6.2). The integration is performed developing a MOOS client named Network Control Interface able to subscribe all the MOOS topic and to publish the command to the node and the high rate activation message. The client communicates with the C2 through a gateway as all the other integrated system

(RADAR, SONAR, optical system, non lethal weapon, unmanned vehicle). RADAR and optical system integration is demonstrated with the installation of simulators and scenario generator.

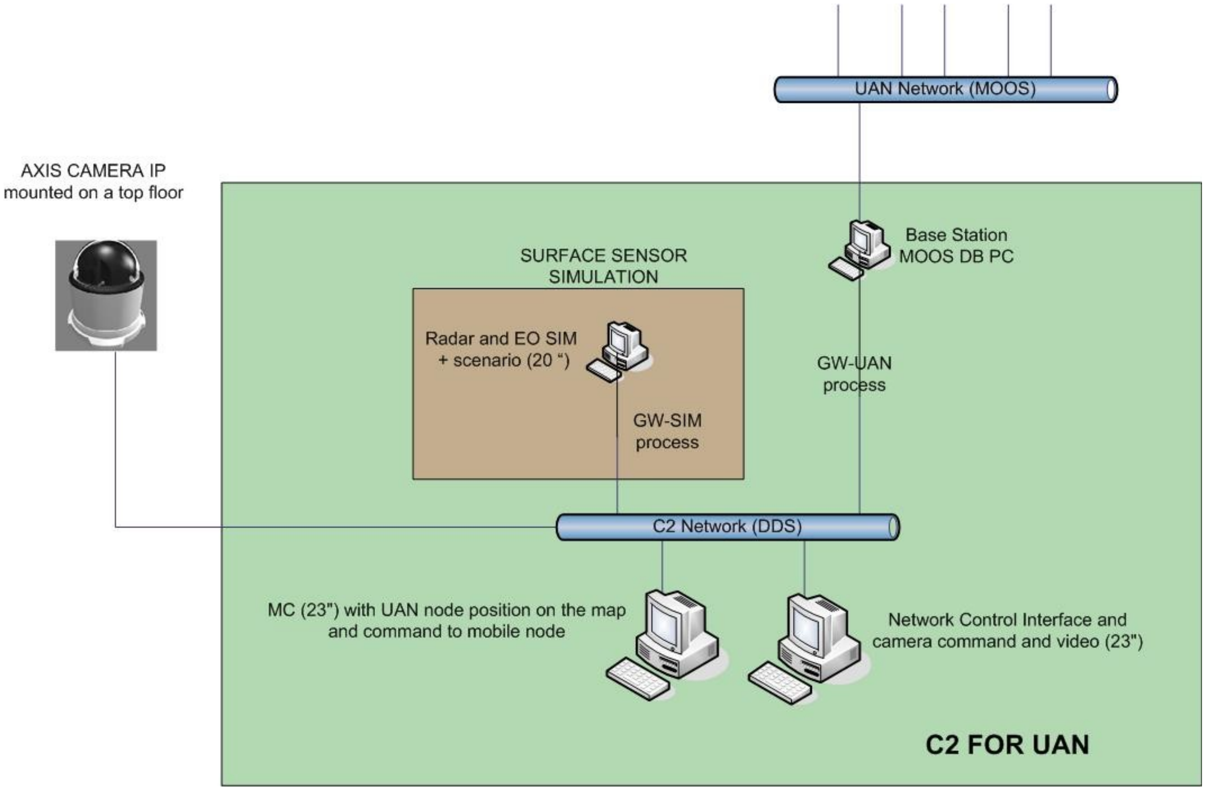
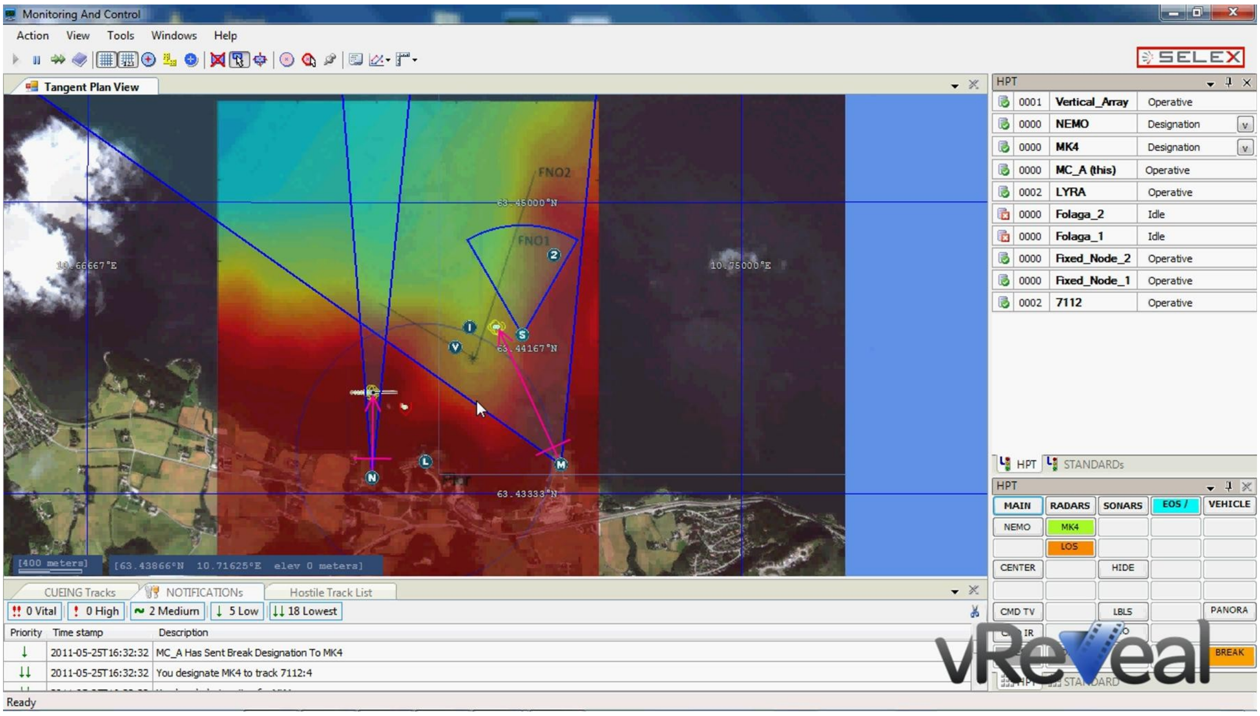


Figure 12: system integration

A scenario is configured in Trondheim area with a ship moving in the area and an underwater target. Figure 13 is a picture of a setup with both underwater and wide area information present at the same time. The list below describes what was validated during UAN'11, with a description of the related key functionalities:

- Receive information about underwater node positions and status
  - Continuous assessment of the node positions and status
- Move unmanned vehicles on a specific position
  - Optimisation of the connectivity based on the channel evaluation performances (the designation point or the depth change is suggested by the acoustic propagation expert)
- Move unmanned vehicles in order to investigate a simulated threat
  - Execution of the intercept mission
- Activate high rate channel in order to receive a pre-charged image from one node

  - o In response to an alarm situation it is requested the transmission of the description of the alarm situation for further analysis
- Integrate in the same console the information from the acoustic channel, from a camera IP and from the surface protection simulation



0001	Vertical_Array	Operative	
0000	NEMO	Designation	v
0000	MK4	Designation	v
0000	MC_A (this)	Operative	
0002	LYRA	Operative	
0000	Folaga_2	Idle	
0000	Folaga_1	Idle	
0000	Fixed_Node_2	Operative	
0000	Fixed_Node_1	Operative	
0002	7112	Operative	

!! 0 Vital | ! 0 High | ~ 2 Medium | ↓ 5 Low | ↓↓ 18 Lowest

Priority	Time stamp	Description
↓	2011-05-25T16:32:32	MC_A Has Sent Break Designation To MK4
↓↓	2011-05-25T16:32:32	You designate MK4 to track 7112:4

Figure 13 : Human Computer Interface

Reproduction of the wide area network by the use of real and simulated components. From the Selex-si point of view, the main objectives were obtained and the experiment was successful, this can be considered true since all the key functionalities of a typical surveillance system were carried out, consequently also the “conceptual validation” was carried out. For development of UAN towards a commercial product it is recommended to establish a Ground Station concept. This corresponds to an interoperability need. In order to give flexibility and re-use of the UAN network in different contexts, it must be defined a unique access point (the ground station) where will be installed all the specific functionalities assigned to the underwater network. These functionalities concern also the underwater sensors that can be included in the underwater structure. For these reasons, the concept of Ground Station should be refined by the use of some addition (payload, automatic channel evaluation and mobile node repositioning) and reallocation (Network Control Interface). Consequently, the Ground Station must preserve the following functionalities (different from C2):

- Collect all the information from the network.

In the experiment, this point is guaranteed by the Base Station by the use of the Moos Database and the High Rate image store and by the Network Control Interface

- Receive surveillance or investigation task from C2
  In the experiment, this point is guaranteed by the Base Station by the use of the Moos Database and by the Network Control Interface
- Receive payload information and share to C2

In a similar way as was done by the use of the High Rate image

- Receive environmental data from the sensor in the network and analyze automatically network
- performance
- Adapt automatically the network to the changing environment condition
- Foresee a local interface in order to configure and monitor the network

Task 6.3 – Experimentation and validation

The fundamental idea behind UAN is that in order to obtain a sustainable gain of performance the whole communication system should be able to adapt itself to the physical acoustic propagation conditions at that particular time and water volume where the system is operating. This includes the use of mobile underwater nodes that can position themselves efficiently for operating as relay nodes in the wireless network. These nodes may also carry intrusion detection payload, and their operation, then, must be a trade-off between the two objectives. The UAN concept also includes fixed nodes, communication networking and data management systems, and finally a Command and Control (C2) subsystem, i.e. integration into a wide area C2 system.

The UAN final sea trial, UAN’11, aimed to test the above key technology components and to demonstrate integration of these into a complete system. UAN’11 was carried out in Trondheim, Norway, on May 23-27 2011, with participation from all project partners. Engineering tests were carried out at the test site in the week before, to prepare for the main experiments.

The sea trials were relatively complex and were carried out to a large extent using lab-prototype components. Furthermore, both underwater and on-shore equipment was included. Together this called for a test location with on-shore lab, reasonably protected waters and efficient ship-support. To meet these criteria, the area around Storsandgård camping in the Trondheim fjord was chosen as test location, with support from R/V Gunnerus of the Norwegian University of Science and Technology.

Figure 14 shows the test area and the ship. On-shore labs were established at the camping, with the fibre cable connection to the STU extending some 900 m out from shore.

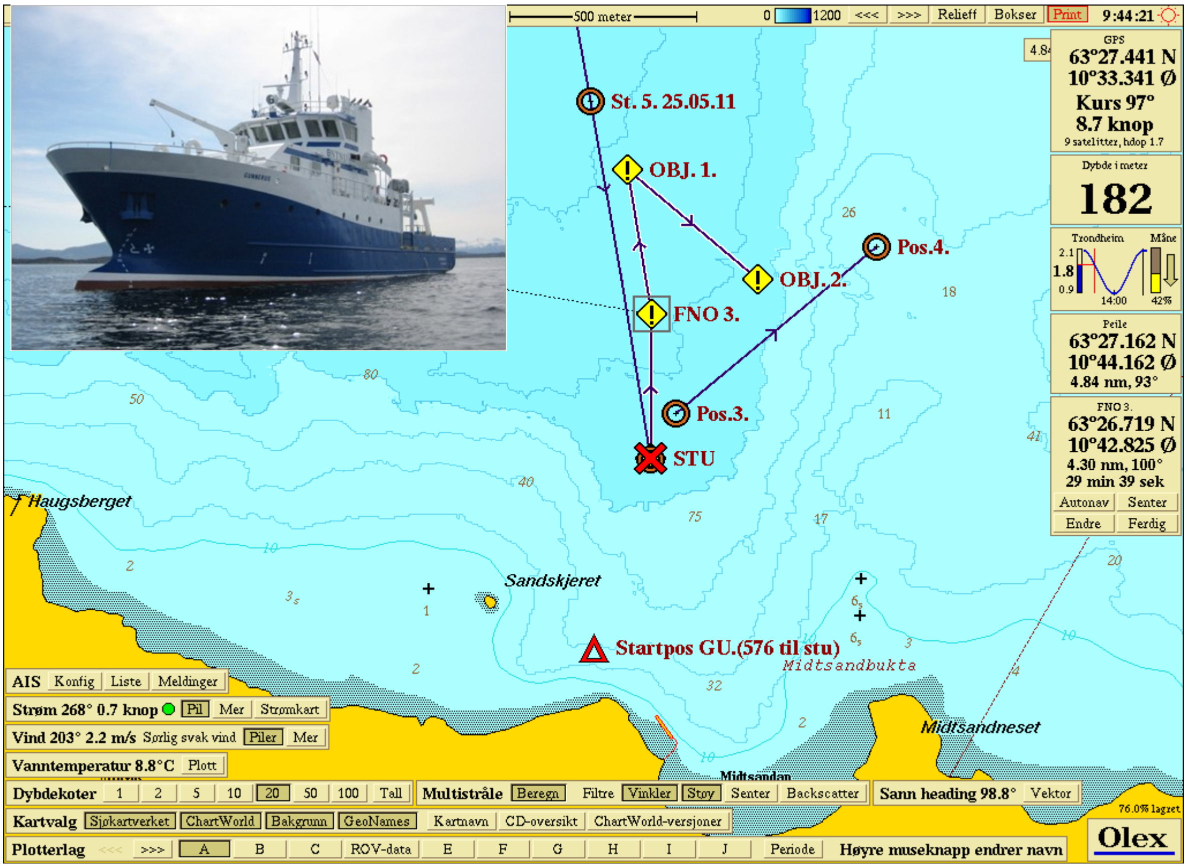

500 meter
0 1200 <<< >>> Relieff Bokser Print 9:44:21
St. 5. 25.05.11
OBJ. 1.
OBJ. 2.
Pos.4.
FNO 3.
Pos.3.
STU
Haugsberget
Sandskjeret
Startpos GU.(576 til stu)
Midtsandbukta
Midtsandneset
Midtsandan
GPS
63°27.441 N
10°33.341 Ø
Kurs 97°
8.7 knop
9 satelitter, hdop 1.7
Dybde i meter
182
Trondheim
Måne
14:00
42%
Peile
63°27.162 N
10°44.162 Ø
4.84 nm, 93°
FNO 3.
63°26.719 N
10°42.825 Ø
4.30 nm, 100°
29 min 39 sek
Autonav Senter
Endre Ferdig
AIS Konfig Liste Meldinger
Strøm 268° 0.7 knop Pil Mer Strømkart
Vind 203° 2.2 m/s Sørlig svak vind Piler Mer
Vanntemperatur 8.8°C Plott
Dybdekoter 1 2 5 10 20 50 100 Tall
Multistråle Beregn Filtre Vinkler Støy Senter Backscatter
Sann heading 98.8° Vektor
Kartvalg Sjøkartverket ChartWorld Bakgrunn GeoNames Kartnavn CD-oversikt ChartWorld-versjoner
Plotterlag <<< >>> A B C ROV-data E F G H I J Periode Høyre museknapp endrer navn
76.0% lagret
Olex

Figure 14 - UAN'11 test area and RV Gunnerus. The geographical distribution of non-mobile nodes is indicated. OBJ 1 and 2 are fictive threats defined for system simulation. The C2 and labs were located on-shore, close to the indicated "Startpos GU".

The physical devices that were integrated in UAN'11 were:

1. Subsurface Telemetry Unit (STU) comprising
   - Underwater acoustic modem from Kongsberg Maritime (KM).
   - Vertical hydrophone array (VA)
   - Vertical chain of thermistors
   - Fibre optical cable connection to shore
   - Underwater industry-PC connected to the above devices.
2. Fixed Nodes (denoted FNOs or FNs), each comprising
   - KM modem as in STU.
   - Vertical chain of thermistors similar to that in the STU
   - Underwater industry-PC unit connected to the KM modems.
3. Mobile Nodes (denoted MNOs or MNs), each comprising
   - Folaga class Autonomous Underwater Vehicle (AUV).
   - KM modem as in the STU and FNOs.

4. Command and Control (C2) system on shore

The UAN11 tests were defined in relation to the key *functions* of the above devices. The functional components and their testing in UAN11 are described as follows:

- **Bidirectional point to point communication** (referred to as SISO-P2P)

This is single input – single output point to point communication between underwater network nodes (FNOs, MNOs, STU), that in sum constitutes the links in a multi-hop underwater acoustic network. The SISO-P2P conveys information over individual network-hops between underwater nodes and the C2 system. The functionality is implemented in real time on KM modems, including both earlier communication algorithms and a new one based on turbo equalization. The latter has been implemented in the project.
Test objective: To test the functionality of new and earlier algorithms in a network environment.
Responsible: Kongsberg Maritime (KM).

- **Unidirectional high capacity point to point communication** (referred to as SIMO-P2P) This is single input – multiple output point to point communication, unidirectionally from remote nodes to the vertical array (VA) of the STU. The VA opens for considerably higher communication capacity than the above SISO-P2P links.

Test objectives: To test (1) the time reversal based SIMO algorithms developed during UAN, and (2) SIMO turbo equalization receiver algorithms. Furthermore (3) to verify transmission of image data to the STU/C2, related to a simulated threat.
Responsible: CINTAL (1 and 3) and FOI (2).

- **Node adaptivity**

Folaga AUVs and KM modems have been integrated in the project, and a remote control system has been developed such that C2 can command the vehicles to move or carry out other actions. Communication between the vehicle and the C2 system is done via the UAN middleware (see below), which uses the acoustic network. When in surface position the vehicle can also be controlled manually over a radio link.
Test objectives: To test the integration of the AUVs in the acoustic network and in the high level middleware and C2 system. Specifically it should be verified that C2 can control the AUV through the middleware and the acoustic network.
Responsible: ISME

- **Network protocols**

Protocols for medium access control (MAC) and multihop routing are necessary to reliably transfer information between source and sink nodes in the acoustical network. Existing MAC and routing protocols have been improved and extended during the project. These protocols have been implemented in the real time processing Digital Signal Processor of the KM modems. To facilitate end-to-end IP connectivity between high level users, an IP interface between the

MAC/routing protocols in the KM modem and the middleware level in the Linux host has been implemented. The PPP protocol was first selected due to the resemblance to old Internet modem usage (e.g. serial connection between KM modem and Linux host), and was used e.g. during the UAN10 sea trial. The PPP was finally exchanged with TUN/TAP protocol due to increased flexibility and faster connection phase. Thus, the TUN/TAP interface was used during the UAN11 sea trial.

Test objectives: (1) to test the implemented acoustical network functionality at sea, for both stationary and mobile nodes. (2) To verify IP interfacing towards high level applications. **Responsible**: SINTEF

- **Middleware - Database and network clients**

The MOOS (http://www.robots.ox.ac.uk/~mobile/MOOS/wiki/pmwiki.php) software was chosen as middleware between the application level and the underwater acoustic network. The middleware hides network, so that the clients see a simple database message exchange system. The clients in this respect are the C2 and the control system of each node, including the AUV control system. The database is centralized and co-located with the C2 on shore. Security features have been added to the standard MOOS software to comply with the overall UAN vision. Specifically these features are integrity, authentication and encryption.

Test objective: To verify the functionality of the middleware in the UAN system, especially in secure mode.

Responsible: ISME

- **System integration - Command and Control**

The UAN concept aims to provide underwater surveillance as an integral part of a wide area surveillance system. Hence, software has been developed for integration of UAN in a C2 environment. For UAN11 the on-shore C2 setup is mainly composed of a Monitoring and Control interface (MC). MC is able to display all the collected information on a map and to send commands to the integrated system. In detail, MC is able to receive data from and to command the underwater network, and to do the same for an on-shore surveillance camera and simulated wide area sensors (RADAR and long range optical system).

Test objectives: To test the integration of all the above functionality into a wide are surveillance system. Specifically this is achieved by demonstrating the following use cases: (1) C2 periodically receives information about node position, status and environmental data. (2) in a simulated threat situation, C2 commands a mobile node to move towards a threat position and the mobile node acknowledges and carries out the command (3) In the same scenario, when the mobile node is near the target, C2 asks the mobile node to provide an image of the target over the high capacity SIMO-P2P link (4) C2 controls the surveillance camera for surface scenario analysis (5) C2 is able to receive tracks from the simulated radar and to send command to the simulated long range optical system.

The SISO P2P network carries all the underwater data traffic (items 1-3), except for the high rate image transfer back to C2.

Responsible: Selex

The overall goal of UAN’11, to demonstrate system integration and thereby the feasibility of the UAN concept, corresponds to the above system integration test objectives. It was necessary for a positive outcome that all of the functional test objectives be fulfilled, with underlying components performing sufficiently to fulfil the demonstration of integration. An overview of the UAN concept as tested in UAN’11 is shown in the following two figures: Figure 15 is an illustration of the underwater physical devices and Figure 16 shows the data and control flow, for the complete on-shore and underwater system.

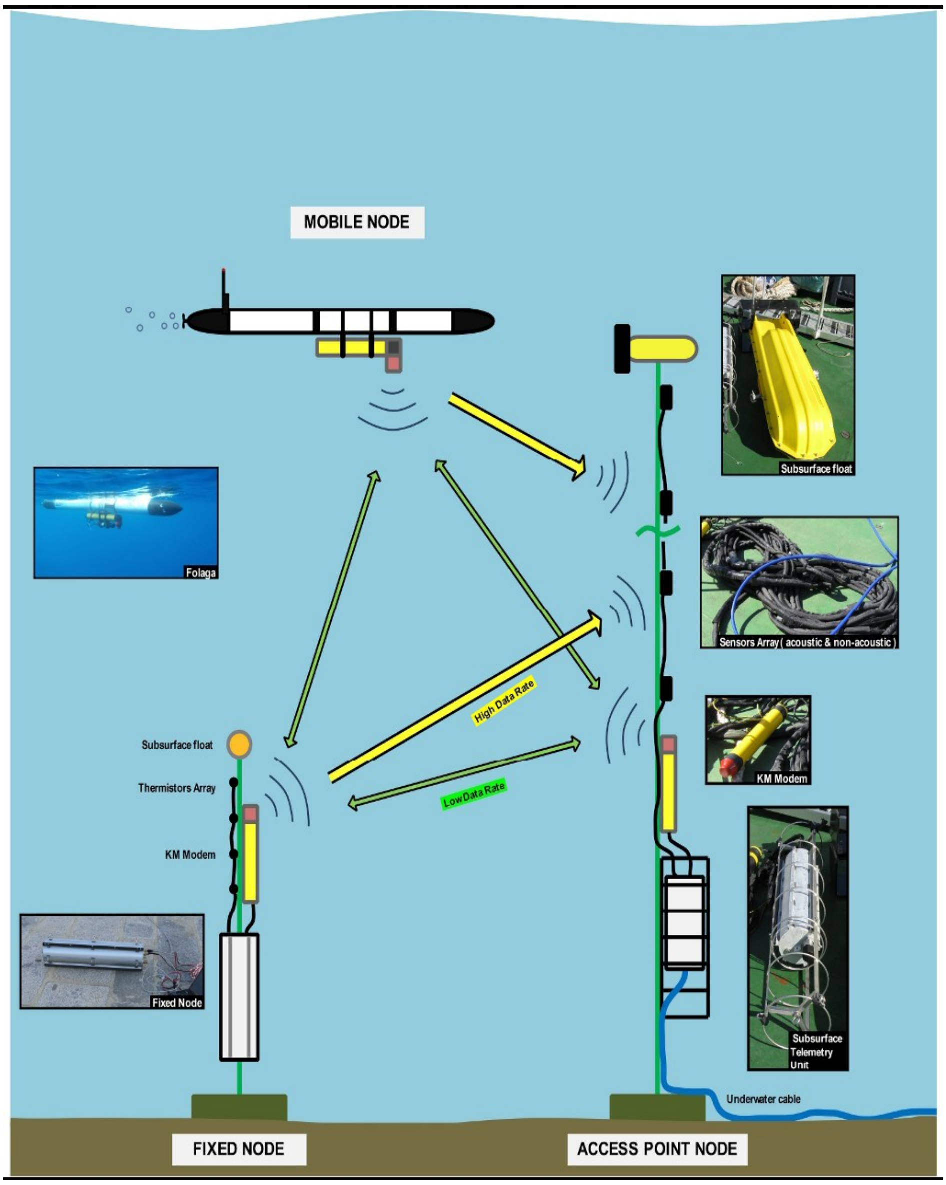


Figure 15 - UAN concept. Underwater components as tested

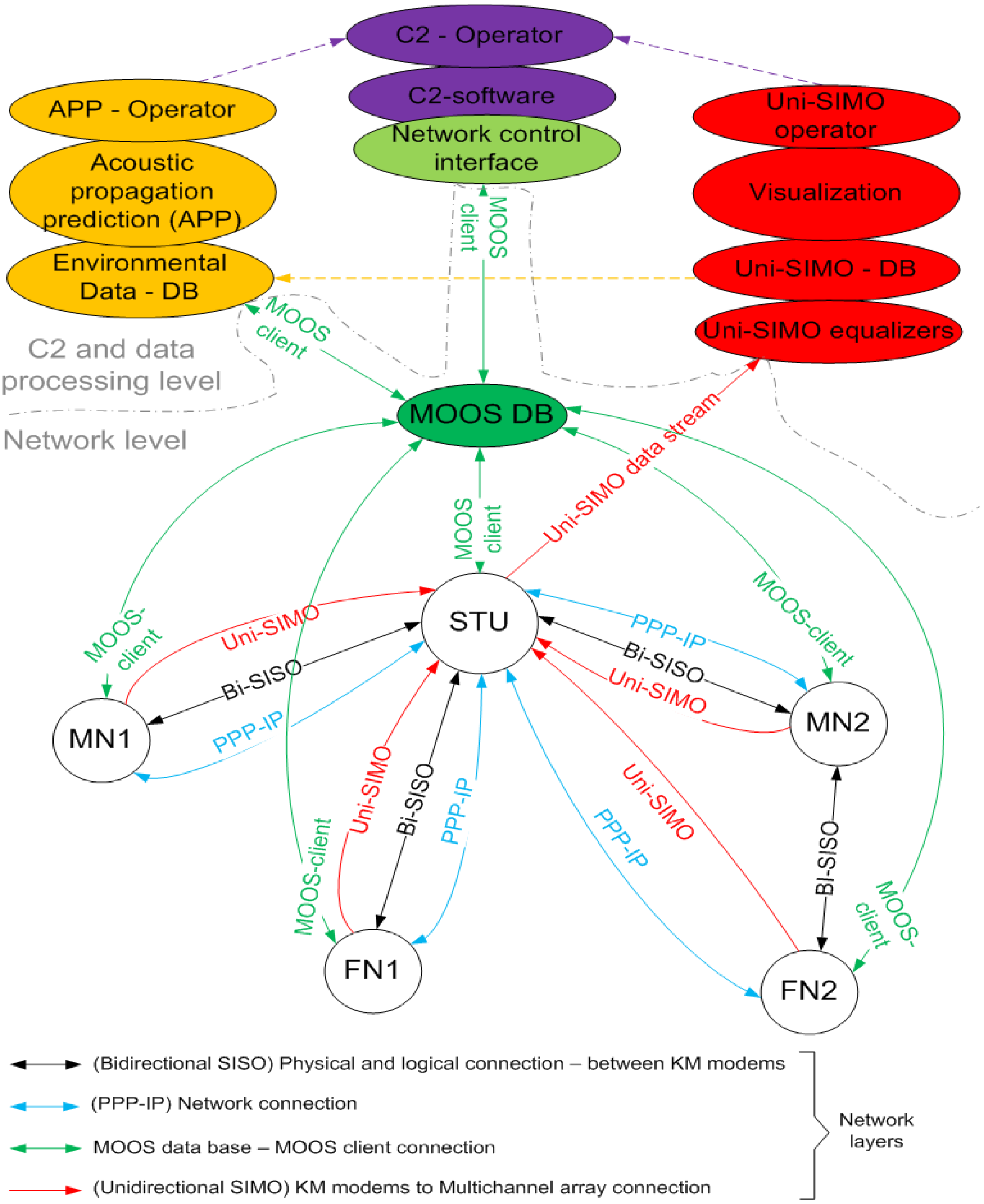

C2 - Operator
C2-software
Network control interface
APP - Operator
Acoustic propagation prediction (APP)
Environmental Data - DB
Uni-SIMO operator
Visualization
Uni-SIMO - DB
Uni-SIMO equalizers
MOOS client
C2 and data processing level
Network level
MOOS DB
Uni-SIMO data stream
STU
MN1
MN2
FN1
FN2
MOOS-client
Uni-SIMO
Bi-SISO
PPP-IP
BI-SISO
(Bidirectional SISO) Physical and logical connection – between KM modems
(PPP-IP) Network connection
MOOS data base – MOOS client connection
(Unidirectional SIMO) KM modems to Multichannel array connection
Network layers

Figure 16 - Diagram of the UAN Project network layers, inter application communications and conceptual data exchange.

Results and evaluation

SIMO P2P communication analyses indicate excellent results even at the longest distance of 11 km. The real time SISO P2P communication in UAN11 was more challenging than experienced during UAN'10 in Pianosa. The Turbo mode (1600 bps) could not operate properly. 500 bps DSSS was used with success especially in the early hours of each day, but 200 bps was sometimes necessary in order to avoid frequent link "outage". In periods significant packet loss was experienced. A possible reason for the challenging and time variable conditions is the presence of fresh water from rivers and rain.

The some times low capacity of P2P communication led to corresponding difficulties at the higher network layers, at times showing long queues and packet losses due to overflow. The network protocols and applications would benefit from refinement and adaptation to be more robust towards such issues, for operation under challenging low capacity conditions.

UAN'11 successfully demonstrated integration of all UAN components into a working system. This includes both controlling data transmission from Fixed nodes and controlling the operation of the Mobile ones, all via the MOOS middleware in secure mode, with the underlying acoustical network invisible to the clients. In total it can be claimed that the validity of the overall UAN concept has been demonstrated, but that improvements (of course) are beneficial on the component level.

ISME equipment in the final UAN10 experiment included two Folaga AUVs with the UAN module mounted at mid-vehicle; the UAN module carried the KM modem and (in one case) also a Valeport CT probe for environmental measurements. Folagas could be controlled via acoustics as mobile nodes of the network and in addition, for setting up the mission and for emergency they could be remotely monitored using a radio link available when the AUVs were on surface. The two vehicles used during the sea trial are shown in Figure 17, and their main technical specifications reported in Table II (See D51 - for more details on Folaga).

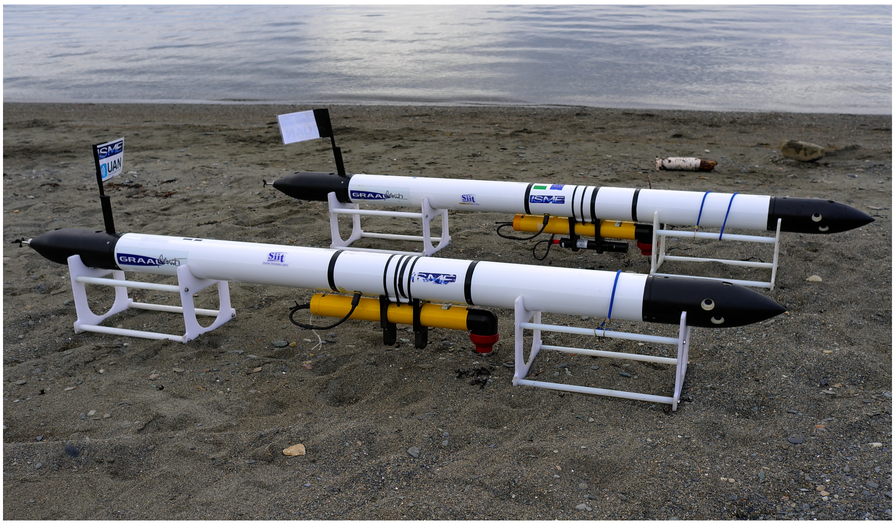


Figure 17: Folaga used during the sea trial with KM modems and (in one case) with a Valeport CT.

In addition to the two Folaga vehicles it was also set up a simulated on R/V Gunnerus to allow the operator to monitor in real-time the network and MOOS performance.

MOOS was completely tested during the UAN11 sea trial. At first in its non-secure form and then activating all the network security features on May 26, h 15.14.

The whole MOOS middleware, both in its non-secure and secure form, behaved as expected showing robustness during all the different phases of the communication. Interruption of any of the underneath network layers did not cause any problem and both the clients and the database were always able to adapt to the communication conditions correctly.

In addition, the modification done in order to simplify the handshake phase and to adapt the application layer to the constraints of the other layers of the network gave very good results allowing for a quick establishment of the client-server connection with a reduced communication overhead.

MOOS was used during the whole experiment using UDP as transport protocol without any problem in the data received and transmitted. Mission control commands from the C2 were received, acknowledged and successfully accomplished.

According to the adaptive cooperative algorithm described in D51, Folagas were able to identify, from an application level point of view, abrupt interruption in the communication. In particular, Folagas were able to identify its moving in an area were the acoustic communication was lost (no MOOS messages were received for more than 15 minutes) and autonomously started to move towards the vertical array where the communication could have been re-established.

Diameter	155mm
Length (with UAN-Payload)	2750mm
Length (without UAN-Payload)	2004mm
Energy Storage	NiMh batteries 12V 45Ah
Max speed	2 knots
Endurance	6 hours at max speed
Max operation depth	50m
Weight in air (without UAN-payload	31 kg

Table II: Folaga technical specifications

Figures 18 and 19 show Folaga 1 and Folaga 2 locations during the test on May 27, 2011.

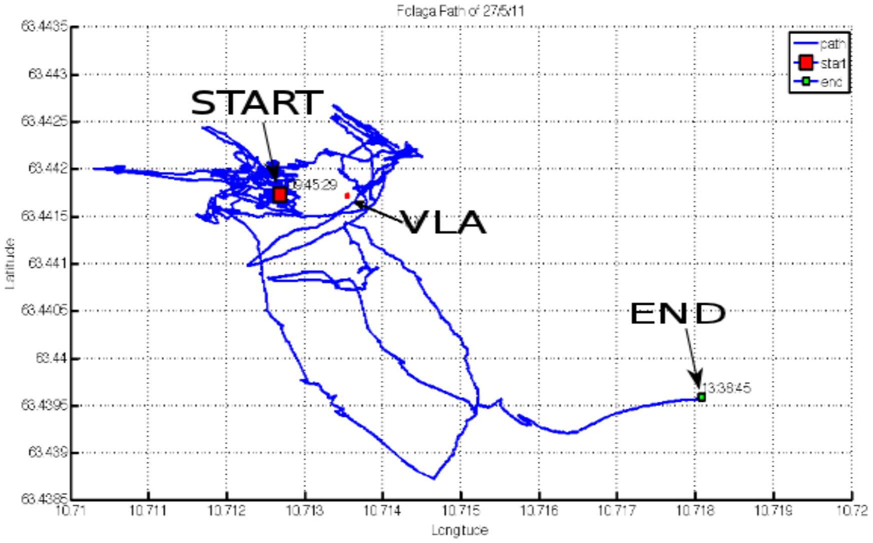


Figure 18: Folaga 1 path during the networking test (May 27, 2011). VA is located at (N63.441718, E10.713545)

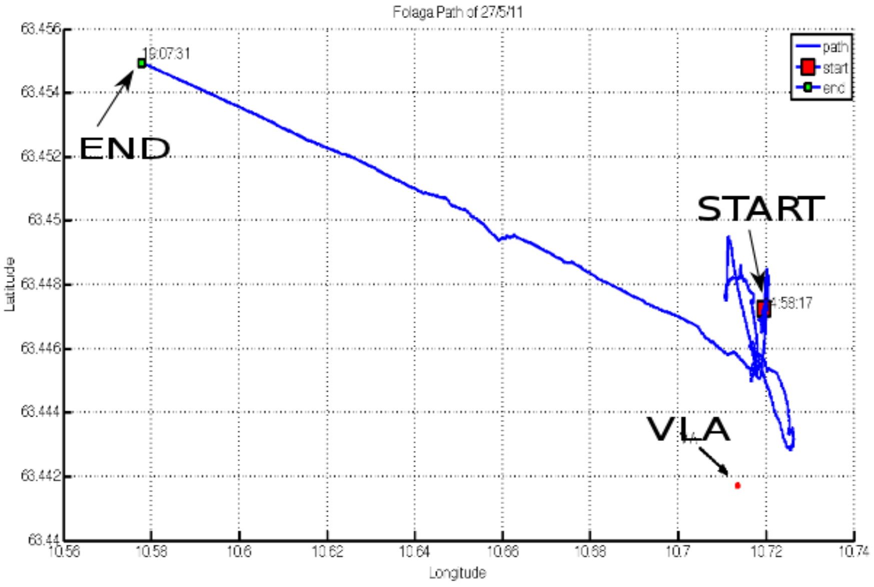


Figure 19: Folaga 2 path during the networking test (May 27, 2011). VA is located at (N63.441718, E10.713545)

Figures 20 and 21 show the MOOS communication statistics obtained on May 27, 2011 for Folaga 1 and Figure 22 statistics on the communication between the MOOSDB and the FNO2 during 14h of operations.

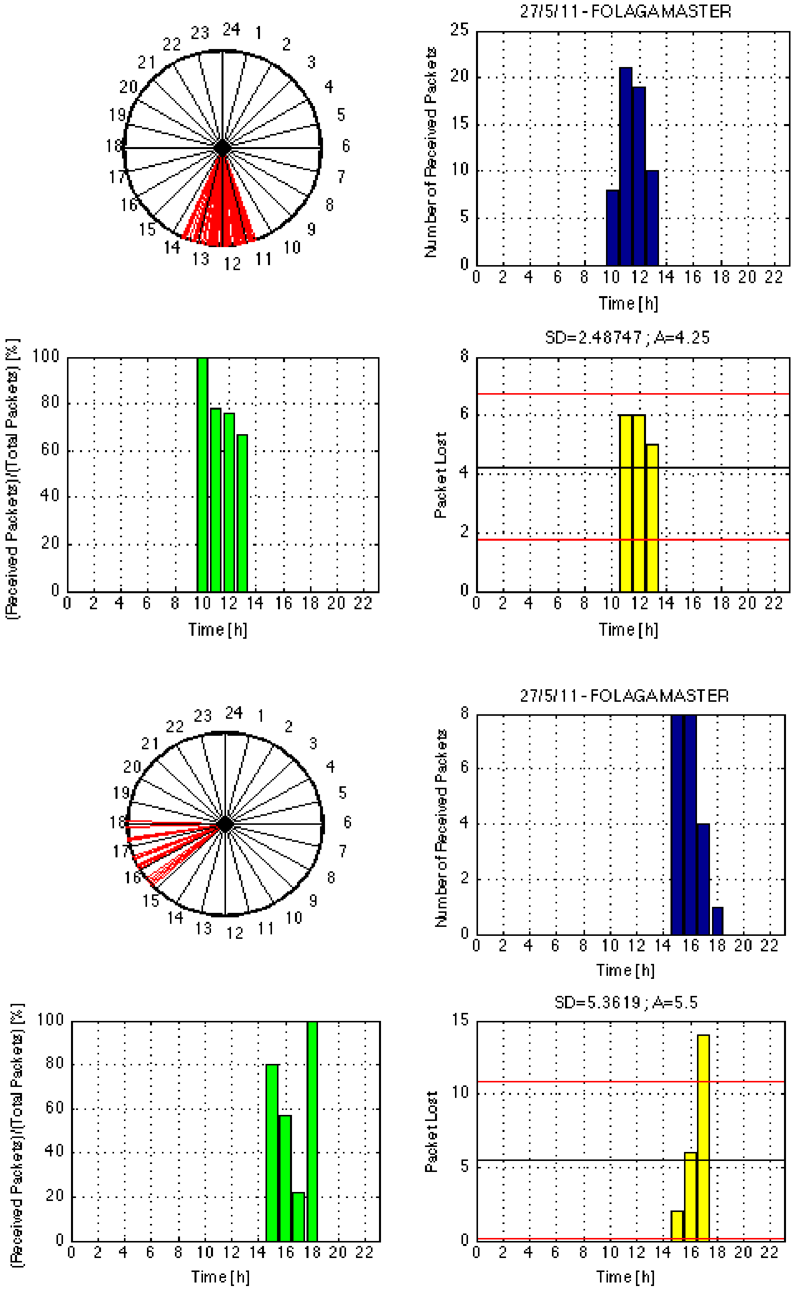


Figure 20: Statistics collected on Folaga 1; Blue histograms: received packets; green: % recived vs. total; yellow: packet loss; red bars on clock indicate the periods of operation of the network. Top: In the morning of May 27, 2011; Bottom: in the afternoon of May 27, 2011. See figure 9 for the corresponding statistics on the MOOS-DB

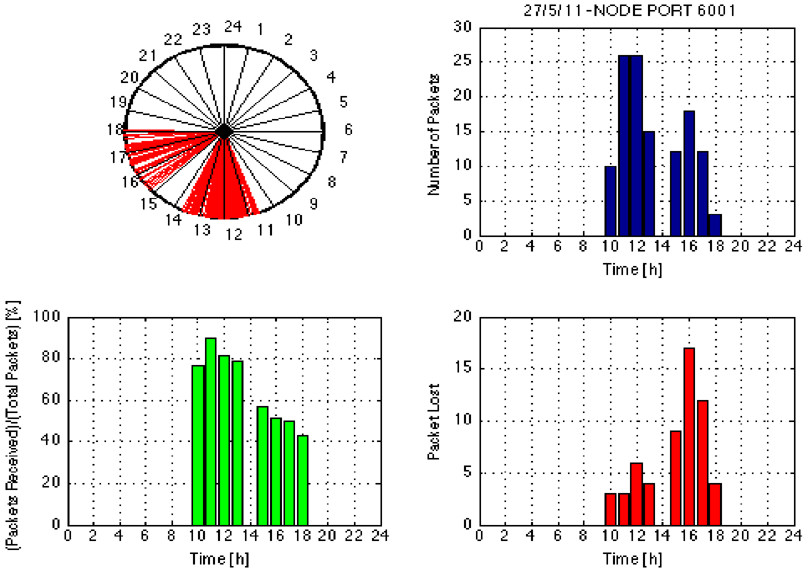


Figure 21: Statistics collected on MOOS-DB and relative to the communication with Folaga 1 on May 27, 2011

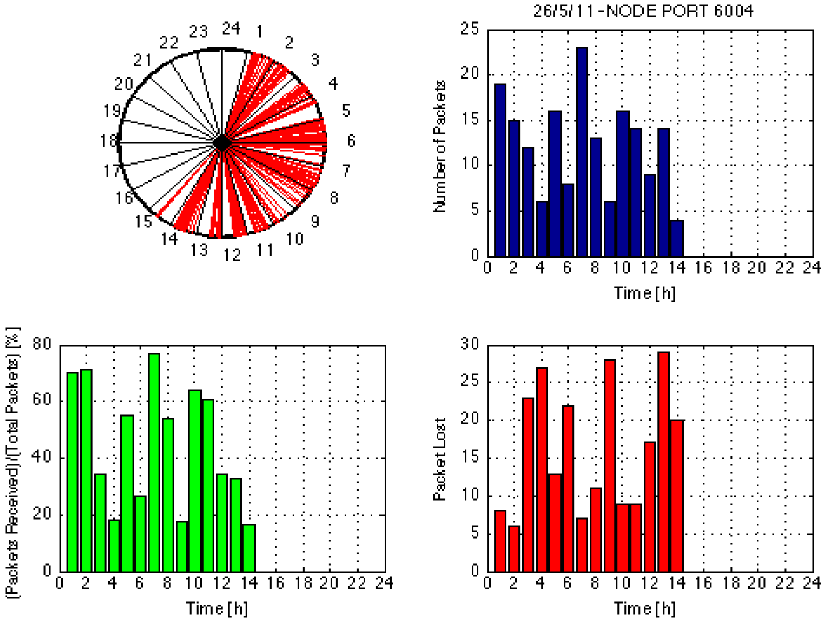


Figure 22: Statistics on the communication between the MOOS-DB and Fixed Node 2 on May 26, 2011. The communication was active until 15:00 when the MOOS-DB was switched to Secure mode. From that moment on all messages from FNO2 were dropped by the DB since FNO2 was kept non-secure and hence it was not able to re-establish the connection. It is clearly visible from the graph the variation in the number of packets

received during the hours of operation and due to the variation in the acoustic communication quality.

Corrections

As mentioned in the corresponding section of WP5, the upgrading of the Secure MOOS was moved from WP5 to WP6 activities; as a result, ISME manpower effort in WP6 has been greater then planned. The delay with respect to the original plan in the final release of the Secure MOOS had no impact on the other activities, and it was completed and tested in time for the final UAN experiment.

WP7 – Dissemination and exploitation

Summary of progress

As a rule of thumb, the turn around time between obtaining research results and their dissemination is normally six months to one year for conference papers and two to three years for journal publications. This third project year was no exception to this rule, with a large number of conference participations showing the results obtained on simulations and on engineering test data performed on project year two and already one journal paper based on system development performed on project year one. Result exploitation can only be effectively started after final project results have been obtained and some integration with existing partner applications was minimally performed, so as to be able to present a market coherent product idea.

During this third project year there were 10 conference papers presented in various scientific and technical fora, including a special session in “Underwater Communication Networks” at the Ocean'11 IEEE/MTS conference in Santander (Spain) in June. There was also one journal paper published in Sea Technology and at least one submitted to Journal of Oceanic Engineering. More directed to exploitation partner Selex SI has participated and presented a UAN poster on the Security Research Conference 2011 (SRC'11) in Warsaw.

Main achievements

The MTS/IEEE Oceans Conference is world class forum for presenting and showing what is being done in the field of ocean engineering and science. Oceans takes place twice a year alternating between the US and Europe or Asia, every year. This year the Europe event was held in Santander (Spain) from June, 6-9 and, as usual attracted a large number of participants both from academia and industry, judging for the large exhibit in the large dedicated room. UAN has partnered with FP7 funded project CLAM to organize two special sessions on “European Projects on Underwater Networks” where UAN has made six participations.

The Security Research Conference is an annual event that this year took place in Warsaw from 19 to 21 of September. This is the largest European event focused on security research and gathers policy makers, researchers, industry representatives and end users from across Europe to foster the debate on future research priorities and the technological, legal and organisational solutions answering current public security threats. By addressing security as a whole, the conference bridges the gap between needs and policies and technological and research issues. The security of at sea and coastal infrastructures is a relevant topic of discussion, where underwater communication networks play an important role. UAN was present at the conference through a poster presented by SELEX SI showing the recent results obtained during the UAN'11 sea trial as part of an integrated infrastructure protection and surveillance concept proposed in UAN.

Corrections

No corrections are required for this work package.

References

[1] UAN WP2 Deliverable 2.2 - *Performance prediction methodology*, Tech. Rep. EC FP7, UAN, GA 225669, WP2 D2.2, FOI, Stockholm, 2010.

[2] *UAN WP2 Deliverable 2.3 – Performance evaluation prediction.* Tech. Rep. EC FP7, UAN, GA 225669, WP2 D2.4, FOI, Stockholm, 2011.

[3] *UAN WP2 Deliverable 2.4 - Validation of predicted performance against field data.* Tech. Rep. EC FP7, UAN, GA 225669, WP2 D2.4, FOI, Stockholm, 2011.

[4] L. Abrahamsson, I. Karasalo, and S. Ivansson, *Geoacoustic inversion of data from underwater communications at short range*, in 4th Int. Conf. & Exhib Underwater Acoustic Measurements: Technologies & Results, Kos, Greece, 2011, pp. 1095-1100.

[5] I. Karasalo, *Modelling of turbo-coded acoustic communication in realistic underwater environments*. in 4th Int. Conf. & Exhib Underwater Acoustic Measurements: Technologies & Results, Kos, Greece, 2011, pp. 1089-1094

[6] I. Karasalo, *Time-domain modelling of turbo-coded underwater communication*. Oceans'11, Santander, Spain, 6-9 June 2011.

[7] R. Bachman, *Acoustic and physical property relationships in marine sediments*, J. Acoust. Soc. Amer., 78 (1985), pp. 616-621.

[8] G. Gragg, D. Wurmser, and R. Gauss, *Small-slope scattering from rough elastic ocean floors: General theory and computational algorithm*, J. Acoust. Soc. Amer., 110 (2001), pp. 2878-2901.

[9] E. Hamilton, *Compressional-wave attenuation in marine sediments*, Geophysics, 37 (1972), pp. 620-646.

[10] D. Jackson and M. Richardson, *High-Frequency Seafloor Acoustics*, Springer, 2007.

[11] A. Voronovich, *Wave Scattering from Rough Surfaces*, Springer, 1999.

[12] A. Caiti, *Test-plan September 2010, Experimental activities*, Tech. Rep. EC FP7, UAN, GA 225669, ISME, University of Pisa, 2010.

[13] F. Zabel, C. Martins and A. Silva, *Design of a UAN node capable of high-data rate transmission*, in Sea Technology, pp. 32-36, March 2011.

[14] U. Vilaipornsawai, A. Silva and S.M. Jesus *Underwater communications for moving source using geometry adapted time reversal and DFE: UAN'10 data*, in Proc. IEEE OCEANS'11, June 2011.

[15] A. Silva, S.M. Jesus and J.P. Gomes, *Probe timing optimization for time-reversal underwater communications*, in Proc. OCEANS'11, Santander (Spain), June 2011.

[16] A. Caiti, P. Felisberto, T. Husoy, S.M. Jesus, I. Karasalo, R. Massimelli, T.A. Reinen and A. Silva, *UAN - Underwater Acoustic Network*, in Proc. IEEE OCEANS'11, Santander (spain), June 2011

[17] U. Vilaipornsawai, A. Silva and S.M. Jesus, *Combined adaptive time reversal and DFE technique for time-varying underwater communications* submitted for publication in Journal of Oceanic Engineering, September 2011.

[18] Gianluca Dini and Angelica Lo Duca, *A Cryptographic Suite for Underwater Cooperative Applications*, Proc. of the IEEE International Symposium on Computers and Communications (ISCC 2011), pp.1-6, Kerkyra (Greece), June 28- July 1, 2011.

[19] B. Schneier, *Applied Cryptography: protocols, algorithms, and source code in C (2nd ed.).* John Wiley & Sons, Inc., 1995.

[20] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, October 1996.

[21] C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," in Proceedings of the Second International Conference on Embedded Networked Sensor Systems (SenSys'04), Baltimore, MD, USA, November 3–5 2004, pp. 162–175.

[22] Gianluca Dini and Ida M. Savino, "TITLE," Proceedings of the 3rd IEEE International Conference on Mobile Ad-Hoc and Sensor systems (MASS'06), pp.457-466, Vancouver (BC, Canada), October 9-12, 2006.

[23] L. Lamport, "Password authentication with insecure communication," Communications of the ACM, no. 11, pp.770-772, vol. 24, November 1981.

[24] Y. W. Law, J. Doumen, and P. H. Hartel, "Survey and benchmark of block ciphers for wireless sensor networks", ACM Transactions on Sensor Networks, vol. 2, nr. 1, pages 65-93, February 2006.

[25] B. Preneel, A. Biryukov, E., Oswald, B.V. Rompay, L. Granboulan, E. Dottax, S. Murphy, A. Dent, J. White, M. Dichtl, S. Pyka, M. Schafheutle, P. Serf, E. Biham, E. Barkan, O. Dunkelman, J.-J. Quisquater, M. Ciet, F. Sica, L. Knudsen, M. Parker and H. Raddum 2003. NESSIE Security Report. Deliverable D20, NESSIE Consortium. February, 2003. Available at: https://www.cosic.esat.kuleuven.be/nessie/deliverables/D20-v2.pdf

[26] Cryptography Research and Evaluation Committee (CRYPTREC), Specification of e-Government Recommended Ciphers, February 20, 2003. (http://www.cryptrec.go.jp/english/images/cryptrec_01en.pdf)

[27] Wang, X., Yao, A., and Yao, F. 2005. New collisions search SHA-1. In Rump session of the 25th Annual International Cryptology Conference (CRYPTO 2005). Springer-Verlag, Santa Barbara, CA, USA, 2005.

[28] Roman, R., Alcaraz, C., and Lopez, J., A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes. Mobile Network & Applications 12, 4 (August), 2007.

[29] Dobbertin, H., Bosselaers, H., and Preenel, B., Ripemd-160, a strengthened version of RIPEMD. In Proceedings of the 3rd International Workshop on Fast Software Encryption (FSE'96). Lecture Notes in Computer Science, Vol. 1039. Springer-Verlag, Cambridge, UK, 1996.

[30] National Institute of Standard and Technology, Cryptographic Hash Algorithm Competition, November 2, 2007 (http://csrc.nist.gov/groups/ST/hash/sha-3/index.html).

4. Deliverables and milestones tables

List of deliverables (excluding the periodic and final reports) produced during the period covered by this report with the used resources indicated in the last column.

TABLE 1. DELIVERABLES[3]

Del. no.	Deliverable name	WP	Lead beneficiary	Nature	Dissemination level	Delivery due date (proj/month)	Delivered Yes/No	Actual / Forecast delivery date	Used resources (PM)
5.4	Field test evaluation	5	ISME	R	PP	31/OUT/10	Y	31/MAR/11	2.48
6.2	Wide area network integration	6	SINTEF	R	PP	31/JAN/11	Y	10/FEB/11	14.30
3.3	Modem functionality verification	3	KM	R	PP	31/JAN/11	Y	30/SEP/11	6.58
2.3	Performance evaluation prediction	2	FOI	R	PP	31/JAN/10	Y	07/FEB/11	5.27
7.4	Final plan for the dissemination of foreground	7	SSI	R	PP	30/MAR/11	N	-	4.43
4.5	Environmental channel equalization algorithm	4	CINTAL	R	PP	30/MAR/10	Y	3/MAY/11	5.50
4.6	Field test report	4	ISME	R	PP	30/MAR/10	Y	26/MAY/11	2.48
7.3.5	Newsletter #5	7	CINTAL	R	PU	30/MAR/11	Y	08/APR/11	1.10
6.3	Project sea trial report	6	SINTEF	R	PP	31/JUL/11	Y	05/SEP/11	26.74
2.4	Validation of predicted performance against field	2	FOI	R	PP	31/JUL/11	Y	16/AUG/11	5.44
7.3.6	Newsletter # 6	7	CINTAL	R	PU	30/SEP/11	Y	10/OCT/11	1.10

[3] For Security Projects the template for the deliverables list in Annex A1 has to be used.

Milestones

In agreement with the plan foreseen in Annex I there were the following milestones reached during this period.

TABLE 2. MILESTONES

Milestone no.	Milestone name	WP no	Lead beneficiary	Delivery date from Annex I	Achieved Yes/No	Actual / Forecast achievement date	Comments
2.2	Prediction of communication network performance on benchmarking	2	FOI	31/JAN/11	Y	31/JAN/11	
3.2	Working modem pair and testing at sea	3	KM	31/JAN/11	Y	29/FEB/11	Slight delay (see text)
4.2 **5.2**	Field test of system integration on Folaga	4-5	ISME	30/MAR/10	Y	30/ABR/11	
6.1	Main project sea trial	6	SINTEF	31/JUL/11	Y	31/JUL/11	

5. Project management

The planning of the third project year took place in the UAN consortium meeting during the annual report review in December 2010, in Brussels. Understandably, the planning was mostly focused on the organisation of the project sea trial, scheduled to take place and the end of May of 2011 in Trondheim, Norway. Very strict deadlines were decided to : i) identify and solve all issues raised during the UAN'10 engineering test, including hardware damages and software compatibility, ii) finalize modem tests, iii) realization of a integration workshop to take place in Faro in March 2011 and iv) preparing the project sea trial test plan. From the management point of view that workshop in Faro was crucial to identify all bottlenecks and most relevant issues. Later on, it was also decided to make a second integration workshop in the week prior to the sea trial, in Trondheim, already at the sea trial location.

Project management tasks are mainly performed under WP1 and shared by all partners under the lead of the project coordinator (PC). WP1 had four distinct tasks running in parallel throughout the duration of the project. Progress along these tasks during year three is reported in detail below.

Task 1.1: General project management

During this third and last project year there were very few management events with a significant impact in the project implementation and progress. There were foreseen delays in various tasks of WP3 as well as associated deliverable delivery dates. These changes were previously mentioned and extended from the second to the third project year, with no impact whatsoever in the timely achievement of the project milestones. The pace of this year was heavily marked by the main project sea trial, its preparation and then on the reporting and dissemination of its outcome. Various tests, meetings and workshops were scheduled in view of the fixed date of the sea trial at the end of May. The actual writing of various deliverables was delayed with no impact on the effective delivery of its content.

All main tasks were timely achieved by the Consortium with no or little deviations from current version of Annex I. The list of meetings held during this period is shown in the table below.

TMB meetings

Meeting type	Date	Venue	Type	Partners present	Scope
Review	Dec 2, 2010	Brussels (BE)	presentat.	All	annual review
Technical	Jan 19, 2011	Stockholm (SE)	presentat.	FOI, KM	WP3
Technical	Mar 31, 2011	---	tele-conf.	All	Test plan

Workshop	Dec 17, 2009	Faro (PT)	presentat.	All but FOI	Eng. Test
Briefing	May 22, 2011	Trondheim (NO)	presentat.	All	Sea trial
Debriefing	Jun 6, 2010	Santander (SP)	presentat.	All but SSI	Dissemination

The project is on time and has achieved all the objectives foreseen for the third project year.

Task 1.2: Administrative management

UAN Consortium administration is controlled by the Project Steering Committee (PSC). The Consortium Agreement (CA) foresees that the PSC meets once a year. The three first meetings were held in October 2008, November 2009 and November 2010, while a fourth meeting is scheduled for the second week of November 2011 (see table below).

PSC meetings

Meeting type	Date	Venue	Type	Partners present	Scope
Review	Nov 30, 2010	---	video-conference	KM,SINTEF, FOI, SSI	annual review
Review	Nov 10, 2011	(planned)	video-conference	All	Annual review

An amendment to the contract was requested by ISME, in order to explicitly include in the Special Clause 10 regarding third parties as for the University of Pisa, acting as third party of ISME-UNIGE. It was explained by ISME that it was erroneously understood that the Special Clause was automatically in force, when in presence of a Joint Research Unit among different Universities, as ISME is, and when the participation of key personnel from different Universities is mentioned in the DoW, as in the case of UAN. Documentation on ISME status, as well as internal documentation distributing UAN tasks among the units of Universities of Genova and Pisa, pre-existing the date of the request, has been provided. The other beneficiaries have been informed of the situation and made no objections to the request. The request was to take effect from the date of the project start, i.e., October 1st 2008 and is at the moment awaiting for approval from EC.

Budget distribution rules were decided by the PSC and in particular that the pre-financing should be distributed according to the partner's request for each project year and according to the expenses during the previous project year. It was constituted a reserve fund, to be distributed upon request of and justified by any partner with execution rates deviating more than 5% from the foreseen budget. This allowed for a flexible internal funding structure with a near optimal management of EU funds and redistribution according to each partner spending. Relevant information was transmitted to the Project Advisory Board (PAB) and comments collected. PAB is now composed of the following individuals: Andreas Birk, Anders Svenson, Connie-Elise Solberg and Tiziano Angelini. A fourth

PSC meeting is foreseen to take place early November 2011. The preliminary agenda for the meeting includes, among others, the project third year and final reports as well as the project financial execution as a whole and the analysis of the PAB reports.

The accumulated number of person*month (PM) at the end of the project have used approximately the estimated human resources. All work packages are equilibrated within 10% of the estimated resources, apart from WP6 and WP7. As already foreseen in the second year management report WP7 used approximately 6 PM less than estimated and WP6 used 9 PM more than estimated. Work package 6 concentrated most of the effort during this last project year.

Task(*)	**WP1**	**WP2**	**WP3**	**WP4**	**WP5**	**WP6**	**WP7**	
T1	6.70	6.50	3.62	6.44	15.00	15.92	14.49	
T2	8.36	11.25	16.78	28.42	6.17	39.55	6.25	
T3	6.12	11.07	20.40	17.38	6.10	40.43	-	
T4	1.30	14.70	-	13.07	3.00	-	-	
T5	-	-	-	6.25	10.54	-	-	
T6	-	-	-	-	14.87	-	-	
Total	**22.48**	**53.52**	**40.80**	**71.56**	**55.68**	**95.90**	**20.74**	**350.68**

KM total reported costs for all three periods exceeds the budget laid down in the grant agreement by 6.1 %. The reason for this was the unexpected complexity of the modem serial line interface in combination with the Linux host modem driver. Somewhat higher travel costs related to management, implementation of the turbo equalizer and dissemination activities also contributed to extra costs. Also SINTEF's total direct and indirect costs for the period 1. October 2008 to 30. September 2011 are above budget. The main reason for this is the reduced currency exchange rate euro/NOK. In addition the direct costs associated with the final tests were higher than planned mainly due to needs for renting lab and meeting facilities.

Task 1.3: Technical management

One of the main scopes of this task is to provide communication among partners to respond to technical issues appearing in the course of task/WP execution. During this third project year there was a significant activity mostly related to the fulfilment of the requirements for the completion of the project main sea trial at the end of May in Trondheim (Norway). This has enforced the realization of an previously unforeseen gathering of one week in Faro (Portugal) with all the networking equipment for lab and at sea controlled testing (in the close by Lagoon) of all the components dully integrating in order to make sure of the correct interfacing and communication between communication layers and systems. Issues were identified and solved either during the meeting or between the meeting and the sea trial. Other individual or intertask gatherings and tests took place, like those performed by KM and FOI, or the one in Genova organized by ISME and SSI. These various contacts and exchange of information – data – configurations were essential for the success of the final sea trial.

Task 1.4: Contacts with other projects

The already mentioned contact with EU funded project CLAM has led to the organization of a joint session on the MTS/IEEE Oceans Conference in Santander (Spain) in June 6-9, 2011. This session was very welcomed by the Oceans organizing committee and has attracted significant visibility to the subject of underwater acoustic communications and networking as well as to both projects and to EU 7th Framework Program as a whole.

6. Explanation of the use of the resources

TABLE 6.1 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR COST ITEMS FOR BENEFICIARY 1 - CINTAL FOR THE PERIOD OCT 1 2010 – SEP 30 2011

WP	Item description	Amount [€]	Explanations
1,2,3, 4,6,7	Personnel costs	55.393	Scientist 15,22 PM; tecnhician 1,57 PM; administrative 3,94 PM; total: 20.73 PM.
4	Major cost items	21.194	Equipment depreciation 12464€; consumables 8730€;
1,4,7	Travel costs	9.195	Annual meeting (2p); meeting KM Oslo (1p); Oceans'2011 (2p); sea trial Norway (3p);
7	Remaining costs	5.316	Renting conference room for annual meeting 404€ UAN website fee 11€; equipment transportation sea trials 3341€; transportation modems 1560 €.
TOTAL DIRECT COSTS		**91.098**	

TABLE 6.2 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR COST ITEMS FOR BENEFICIARY 2 – SSI FOR THE PERIOD OCT 1 2010 – SEP 30 2011

WP	Item description	Amount [€]	Explanations
1,6,7	Personnel costs	96.436	Research staff 17,95 PM; management 0,41 PM; total 18.36 PM.
6	Major cost items	1.280	equipment
6,7	Travel costs	15.645	Annual meeting, (1p); Eng. Test Faro Mar 2011 (2p); Trondheim UAN11 (3p); SRC11 Warsaw (1p);
TOTAL DIRECT COSTS		113.361	

TABLE 6.3 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR COST ITEMS FOR BENEFICIARY 3 - SINTEF FOR THE PERIOD OCT 1 2010 – SEP 30 2011

WP	Item description	Amount [€]	Explanations
1,2,3, 5,6	Personnel costs	106.830	Research staff: WP1 0.41PM; WP2 2.12PM; WP5 0.71PM; WP6 5.61PM, WP7 0.3PM; total 9.15PM.
1,2,3, 5,6	Travel costs	7.053	Y2 Annual review meeting (2p); Engineering tests Faro (2p);
6	Remaining costs	28.621	Final tests – rental of research vessel and RHIB, rental of lab and meeting facilities, safety equipment and components, local transport
TOTAL DIRECT COSTS		142.504	

TABLE 6.4 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY 4 - ISME FOR THE PERIOD OCT 1 2010 – SEP 30 2011

WP	Item description	Amount [€]	Explanations
1, 2, 4, 5,6,7	Personnel costs	88.999	Scientist 8,5PM; administrative 0.5 PM; Ph.D. students 7 PM; total 16PM.
1	Subcontracting	5.000	Audit cost statement (not yet incurred)
4,5	Major Cost Items	9.190	Costs of engineering test in Pianosa Island during UAN'10 (costs charged in October 2010)
1, 5	Travel costs	12.420	Review meeting (1p); Water Side Security, Italy (1p); Eng. test Faro, (3p); sea trial Trondheim (2p); Oceans'11, Santander (2p); IEEE ISCC, Kerkyra (Greece);
1, 5	Remaining direct costs	5.040	Equipment transportation and insurance for the Faro test (Mar11) and Trondheim sea trial (May11);
TOTAL DIRECT COSTS[4]		**120.649**	

TABLE 6.5 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS FOR BENEFICIARY 5 - FOI FOR THE PERIOD OCT 1 2010 – SEP 30 2011

WP	Item description	Amount [€]	Explanations
1,2,3,6,7	Personnel costs	114.584	Salaries for research staff WP1 0.67PM; WP2 7.04 PM; WP6 2.82PM; WP7 1.75PM; total 12.28PM.
1	Subcontracting	1.091	Audit certificate
1,3,6,7	Travel costs	9.957	Annual meeting Brussels (1p); field trial UAN10 Pianosa (2p), field Trondheim UAN11 (3p), Oceans 11 Santander (2p);UAM, Kos, Greece (2p);
137	Remaining direct costs	3.924	Conference fees for Oceans'11 and UAM; licence cost for data program Tex2Word;
TOTAL DIRECT COSTS		**129.556**	

TABLE 6.6 PERSONNEL, SUBCONTRACTING AND OTHER MAJOR DIRECT COST ITEMS BENEFICIARY 6 - KM FOR THE PERIOD OCT 1 2010 – SEP 30 2011

WP	Item description	Amount [€]	Explanations
1,3,6,7	Personnel costs	182.294	Salaries for staff WP1 0.6PM, WP3 4.99PM, WP6 4.82 PM, WP7 1.22PM: Total 11.63 PM.
1,3,4,5	Travel costs	9.867	Field trial UAN10 Pianosa (2p), WUWNet 2010 Woods Hole (1p); Annual meeting Brussels (1p); Meeting Stockholm Jan 2011 (1p); Eng. test Faro Mar. 2011 (1p), Trondheim UAN11 (2p), Oceans 11 Santander (1p)
TOTAL DIRECT COSTS		**192.161**	

[4] Total direct costs have to be coherent with the directs costs claimed in Form C

6. Financial statements – Form C and Summary financial report

Please submit a separate financial statement from each beneficiary (if Special Clause 10 applies to your Grant Agreement, please include a separate financial statement from each third party as well) together with a summary financial report which consolidates the claimed Community contribution of all the beneficiaries in an aggregate form, based on the information provided in Form C (Annex VI) by each beneficiary.

When applicable, certificates on financial statements shall be submitted by the concerned beneficiaries according to Article II.4.4 of the Grant Agreement.

IMPORTANT:

Form C varies with the funding scheme used. Please make sure that you use the correct form corresponding to your project. Templates for Form C are provided in Annex VI of the Grant Agreement. An example for collaborative projects is enclosed hereafter. A Web-based online tool for completing and submitting the forms C is under preparation. If you have to submit forms C before the tool becomes available, please ask your Commission project officer for an Excel version of the form.

If some beneficiaries in security research have two different rates of funding (part of the funding may reach 75% in reference with Article 33.1 of the EC rules for participation - REGULATION (EC) No 1906/2006) then two separate financial statements should be filled by the concerned beneficiaries and two lines should be entered for these beneficiaries in the summary financial report.

7. Certificates

List of Certificates which are due for this period, in accordance with Article II.4.4 of the Grant Agreement.

Beneficiary	Organisation short name	Certificate on the financial statements provided? yes / no	Any useful comment, in particular if a certificate is not provided
1	CINTAL	yes	
2	SSI	no	Expenditure threshold not reached
3	SINTEF	no	Provided on year two
4	ISME	yes	
5	FOI	no	Provided on year two
6	KM	no	Expenditure threshold not reached