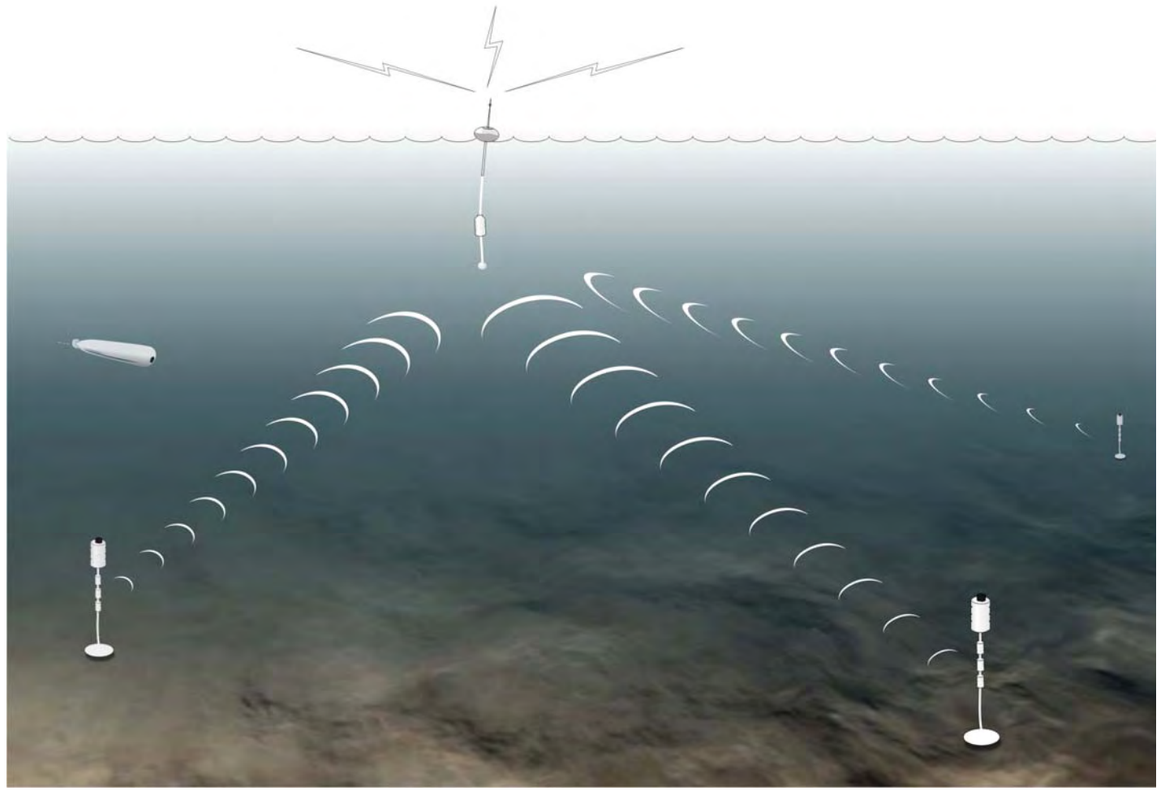
Wireless Underwater Sensor Networks

JIMMI GRÖNKVIST, JAN NILSSON, ERLAND SANGFELT



FOI, Swedish Defence Research Agency, is a mainly assignment-funded agency under the Ministry of Defence. The core activities are research, method and technology development, as well as studies conducted in the interests of Swedish defence and the safety and security of society. The organisation employs approximately 1000 personnel of whom about 800 are scientists. This makes FOI Sweden's largest research institute. FOI gives its customers access to leading-edge expertise in a large number of fields such as security policy studies, defence and security related analyses, the assessment of various types of threat, systems for control and management of crises, protection against and management of hazardous substances, IT security and the potential offered by new sensors.

FOI
Defence Research Agency
Defence & Security, Systems and Technology
SE-164 90 Stockholm

Phone: +46 8 555 030 00
Fax: +46 8 555 031 00

www.foi.se

FOI-R-- 2408 --SE Technical report
ISSN 1650-1942 December 2007

Defence & Security, Systems and Technology

Jimmi Grönkvist, Jan Nilsson, Erland Sangfelt

Wireless Underwater Sensor Networks

FOI-R--2408 --SE Technical Report Defence & Security, Systems and Technology
ISSN 1650-1942 December 2007

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Defence & Security, Systems and Technology SE-164 90 Stockholm	FOI-R--2408--SE	Tecnical report
	Programme Areas 4. Sensors and Low Observables	
	Month year December 2007	**Project no.** E20604
	Subcategories 43 Underwater Technology - Surveillance, Target acquisition and Reconnaissance	
	Subcategories 2	

Author/s (editor/s)	Project manager
Jimmi Grönkvist, FOI Jan Nilsson, FOI Erland Sangfelt, FOI	Tommy Öberg
	Approved by Matts Gustavsson
	Sponsoring agency Swedish Armed Forces
	Scientifically and technically responsible Jimmi Grönkvist and Jan Nilsson

Report title (In translation)

Wireless Underwater Sensor Networks

Abstract

In the report a wireless sensor network for passive as well as active acoustic surveillance under water is described. A feasible use is surveillance of an area at sea like the entrance to a harbour or a base. With other sensors the network also has a civilian use, e.g. for environmental surveillance. The network has a decentralised architecture and a large part of the signal processing is done locally within each node or in a group of network nodes, after which the result is presented to the operations centre or similarly. Being autonomous and wireless the system is rapidly deployed, and covert if needed. The major part of the report deals with the design of the communications protocols for the network.

Designing network protocols for the underwater acoustic channel is a great challenge. To achieve reasonable capacities, protocols need to be tailored to the specific scenario. In particular the MAC protocol is important to design properly. In the report we discuss two different protocol solutions, one based on Aloha and one on TDMA. The solution based on Aloha is simple to implement but gives an expected low throughput in the network. A TDMA solution, on the other hand, can be made fairly efficient when tailored to our specific scenario.

Keywords

Network protocols, MAC, underwater, communication, sensor network, communication network

Further bibliographic information	Language English

ISSN 1650-1942	Pages 23 p.
	Price acc. to pricelist

Utgivare FOI - Totalförsvarets forskningsinstitut Försvars- och säkerhetssystem 164 90 Stockholm	**Rapportnummer, ISRN** FOI-R--2408--SE	**Klassificering** Teknisk rapport
	Forskningsområde 4. Sensorer och signaturanpassning	
	Månad, år December 2007	**Projektnummer** E20604
	Delområde 43 UV-teknik - sensorer	
	Delområde 2	
Författare/redaktör Jimmi Grönkvist, FOI Jan Nilsson, FOI Erland Sangfelt, FOI	**Projektledare** Tommy Öberg	
	Godkänd av Matts Gustavsson	
	Uppdragsgivare/kundbeteckning Försvarsmakten	
	Tekniskt och/eller vetenskapligt ansvarig Jimmi Grönkvist och Jan Nilsson	

Rapportens titel

Wireless Underwater Sensor Networks

Sammanfattning

I rapporten beskrivs ett trådlöst sensornätverk för passiv såväl som aktiv akustisk övervakning under vatten. En möjlig användning är övervakning av ett begränsat havsområde, t.ex. ett sund eller inloppet till en hamn eller bas. Med andra sensorer har nätverket också en civil användning för t.ex. miljöövervakning. Nätverket har en decentraliserad arkitektur och en stor del av signalbehandlingen sker lokalt inom varje nod eller i en grupp av nätverksnoder, varefter resultatet redovisas till en ledningscentral eller dylikt. Autonomiteten och trådlösheten gör att systemet kan läggas ut snabbt, och om så önskas dolt. Huvuddelen av rapporten handlar om hur kommunikationsprotokollen för ett minde nät med begränsad funktionalitet kan byggas upp.

Att konstruera en nätverkslösning för undervattensnätverk är en utmaning. Att anpassa designen för det speciella scenariet är väsentligt om en acceptabel nätkapacitet ska kunna uppnås . Speciellt är MAC protokollet viktigt att beakta i designen. I rapporten diskuteras två olika protokollösningar, en baserad på Aloha och en på TDMA. En lösning baserad på Aloha är enkel att implementera men en sådan lösning förväntas ge låg nätkapacitet. En TDMA lösning å andra sidan kan bli relativt effektiv om den skräddarsys utifrån scenariot.

Nyckelord

Nätverksprotokoll, MAC,undervatten, kommunikation, sensornätverk, kommunikationsnätverk

Övriga bibliografiska uppgifter	**Språk** Engelska
ISSN 1650-1942	**Antal sidor:** 23 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Contents

1. Introduction

Underwater wireless sensor networks employing acoustic communication links is an area of intense research as evidenced by e.g. a large number of presentations at Oceans'07 in Aberdeen, Scotland [1]. One of the goals of our project is to describe an operational scenario for using such networks in area surveillance, and to describe a possible solution for the communication network protocols. Later, a smaller version of this network consisting of only three or four nodes will be demonstrated at sea.

In this report we shortly describe how a network of nodes, each one consisting of sensors and an acoustic modem, can be used for shallow water area surveillance, and foremost, how the network protocols can be designed. The advocated protocol solution will later be further developed, and eventually evaluated in a sea trial demonstration.

A network node will be assumed to have sensors that can be used for detection and localization. It will also have a modem with transmitter/receiver for communication and a computer which contains both the modem and sensor software. The nodes can be placed on the sea bottom, or they can be fitted onto an autonomous underwater vehicle (AUV). However, in this preliminary study only stationary nodes will be studied. In the network, one of the nodes should be placed in the wet end of a surface buoy, which also has a radio modem in the air for communication with a base or command centre.

In principle, the modem transmitter could be used for active sonar detection using the other nodes as multistatic receivers. The receiving hydrophones could be used for reception of communication signals from outside the network. Thus, the nodes can function as communication nodes, relays of information, individual surveillance or co-operative surveillance together with other nodes in the network. If the sensor set is extended with oceanographic sensors or environmental probes, the use of the network in civilian applications, like e.g., environmental monitoring of the sea, becomes an interesting possibility. Whether the use is military or civilian, the network is wireless and therefore, can be rapidly and effortlessly deployed compared to a cabled network. Thus, area surveillance in any shallow water can quickly be achieved.

Designing network protocols for the underwater acoustic channel is a great challenge due to low data rates, long propagation delay, energy limitations, difficult channel multipath conditions and difficulty of time synchronization. This is specifically the case regarding the access to the channel medium. Large propagation delays and limited capacity will make developed protocols for radio communication difficult to use. To achieve reasonable capacities, protocols need to be tailored to the specific scenario. Generalized solutions are probably not possible within the foreseeable future.

The report is organized in the following way. In Chapter 2 we describe the scenario and some technical parameters of the modems used that will determine the conditions of the networking solutions. In Chapter 3 we describe the medium access problem and some solutions to that. Chapter 4 deals with routing and higher layers. Finally, in Chapter 5 we give some conclusions from our work.

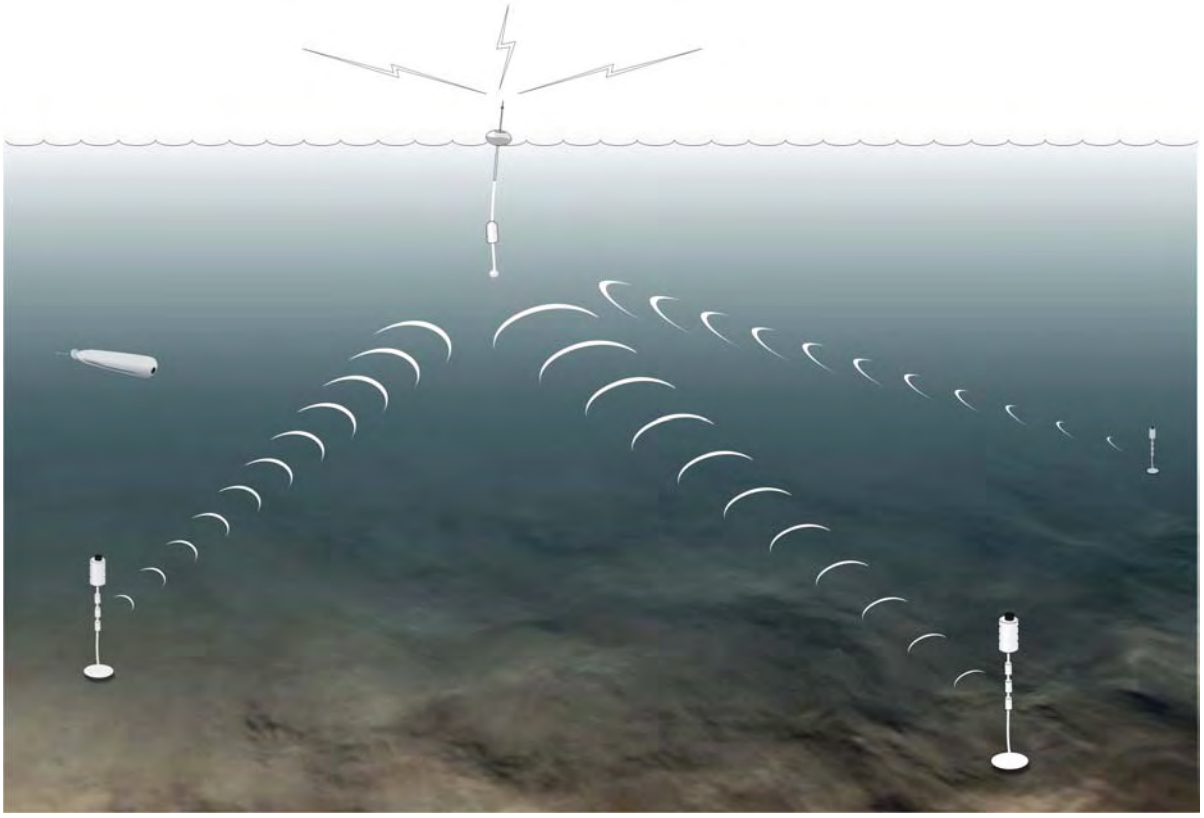


Figure 1. Illustration of a part of the network providing detection of an unmanned underwater vehicle. Three of the nodes report their detections to the surface buoy. The way that the nodes have been depicted does not necessarily reflect the actual design of the nodes.

2. Using the network

The Swedish Armed Forces are developing towards rapid action and flexible forces, engaging more in international crisis prevention and peace keeping/enforcement rather than protection against a homeland invasion. Defence of selected areas like harbours or bases against sabotage or terrorism, i.e. asymmetric threats from a less well identified enemy have to be considered. The field of action is likely to be abroad as well as in domestic waters. The need for underwater sensor networks arises naturally in a maritime rapid action mission in littoral waters, in particular abroad. There may be an insufficient environmental knowledge, at least in an early stage of the mission. An assessment of the environment, and an initial battlespace preparation, is envisioned to sometimes be performed covertly using submarines or AUV's. The sensor network could be deployed from such assets, and then autonomously initiate itself, making advanced surveillance possible without the need to have personel in the proximity of the potentially dangerous network area.

Even if the operation is covert, it could be advantageous to deploy the surveillance sensors in the form of a wireless network from a ship or from an aircraft, providing rapidness and simplicity in the set up.

2.1 Scenario

A littoral water area, about which relatively little is known in advance, and which is lacking any useful infrastructure for cabled sensors should be surveilled. Nodes consisting of underwater sensors with acoustic modems will be deployed, using AUV's or some other asset of the task force. It is assumed that the position of the nodes can be determined. A deploying AUV could use its own navigation system to assess the positions approximately, the nodes can then improve positioning on their own [2].

The network should autonomously detect passages of targets like submarines or ships in the area, and transfer information about the targets to the command center. An illustration of this is given in Figure 1. The command center will process the information from the network and use it to update e.g. the recognized maritime picture (RMP). We will assume that an RF- or SAT-link placed in a surface buoy is available. The wet end of the buoy carries underwater sensors and an acoustic modem. Thus, the surface buoy acts as a gateway (or access point) to the under water nodes and it has identical surveillance capacity and the same acoustic modem in a base line design. The command center can transmit information or orders back to the network through the gateway buoy. If for example, more data about some detection is wanted, the center could ask for it through the buoy.

The RF- or SAT-links could also be placed in an AUV that can be part of the network. However, this possibility will not be included in this scenario. The inclusion of mobile nodes in the network will be deferred to a forthcoming study.

Another alternative for communicating with the command center would be to relay messages via a number of relaying underwater modems. This would however cause large delays in the data transmission, at least if the relay distance is large. If the requirement is to stay covert by using stealth communication under water the relaying may provide a solution. In this study we do not study this option.

The command center can be onboard a ship which operates far away from the area where the surveillance nodes are deployed. An RF-link in the gateway buoy may permit communication distances of 10-30 km, larger distances may demand a SAT-link. It is also possible that an amphibious force, having the command center located on some piece of land in the littoral area, employs the network.

2.2 Sensors and nodes in the scenario

The underwater sensors in a node will be assumed to possess some directivity, allowing for detection and providing a three-dimensional direction to the passing target. The sensors could consist of three pairs of hydrophones or non-acoustic sensors. The nodes will be placed on the sea bottom, or will be moored above the bottom. Mooring may necessitate keeping track of the sensor orientation. Each node will, in addition to the sensors, have a computer for signal processing and communication, batteries for long time operation, and an acoustic transducer for communication. The communication frequency band is judged to be best chosen so as to minimize interference from own ship and own submarine active sonar frequencies. Conversely, interference from the network to the sensors is minimized. Taking account of the high frequency absorption in high salinity environments that may be encountered during international missions, it seems reasonable to use carrier frequencies well below our usual sonar frequencies. A carrier frequency somewhere in the 8 – 20 kHz

band may be appropriate, allowing for bandwidths of several kHz using fairly low cost transducers.

In our operational scenario the network will consist of at least eight deployed nodes. The detection range for a silent submarine will be rather limited, a reasonable judgement may be a couple of hundred meters, while ships far away may be easily detected. The use of direction finding sensors may be necessary to sort out a passage in the network area from a large number of remote targets. In order to get a relatively descent surveillance coverage against silent targets, the nodes need to be fairly close to each other. Thus, the deployed network will typically look as described in Figure 2.

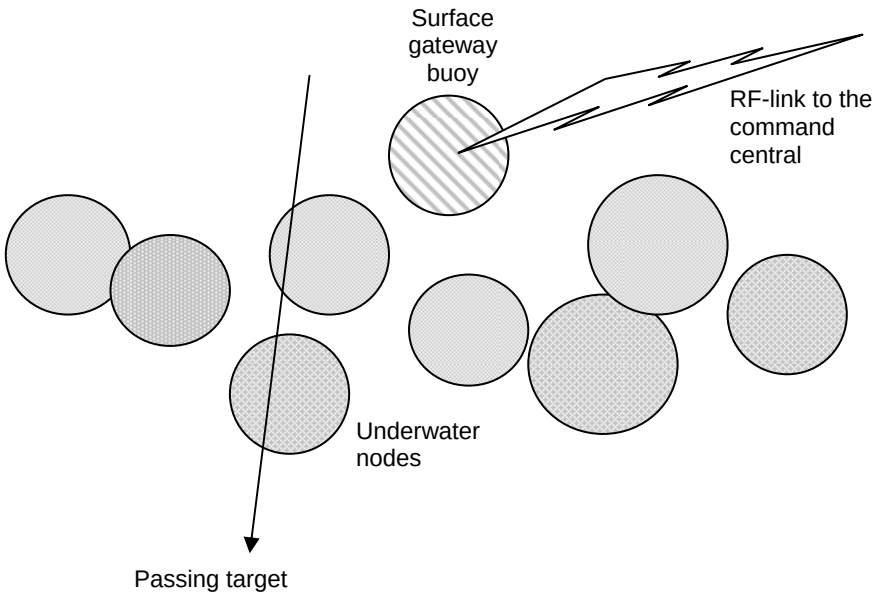


Figure 2. An example of a deployed network for surveillance and communication is depicted. The grey areas define the detection range for a silent target. The nodes may have different detection ranges depending on their depth and on the bottom topography. The distance between two neighbouring nodes is about 500 m - a compromise between the detection range requirements and area coverage requirements. The nodes could in this case cover e.g. a strait of about two km, thus forming an efficient tripwire against passages. The acoustic communication range is assumed to be at least two km. This implies that all the nodes will reach the surface buoy, and the network architecture will be a star topology.

The sea surface buoy is itself a node for surveillance and underwater communication like the others. It receives messages from the bottom nodes and relays them through the RF/SAT-link to the command center. It may receive messages from the command center and broadcast them to the nodes.

Collection of data, signal processing, and extraction of target information is conducted automatically in each node. When a target has been detected, raw data from up to 10 seconds of the target signal, represented by 12 bits/sample, can be stored and later sent up to the surface or gate way buoy. If we assume a baseband sampling frequency of 1000 Hz for the signal, we need to transfer 120 kbit of data for this example. Since power consumption needs to be kept low, such data is not transmitted to the command center on a regularly basis, but can be communicated upon request via the gate way.

The modem transmitters could be used as active sonar for detection of nearby targets. However, the interference with the passive surveillance will be severe. Therefore, the active sonar mode would only be used after a passive indication of a target nearby, and only a few pings will be used. In this case, it will be the command center that orders one of the nodes to perform an active search. The other nodes will be multistatic receivers in this case.

2.3 Modem parameters

The modems will be assumed to have a carrier frequency of 17 kHz, and a useable bandwidth of 4000 Hz. This allows for some spectrum spreading in the covert mode, or allows for data rates of 4000 coded symbols per second in cases where higher data rates are needed. The communication algorithms will employ an error correcting turbo code and modulation schemes selectable as BPSK, QPSK, 16QAM, or possibly some other scheme. The algorithms have been tested previously in sea trials by FOI [3,4,5]. The turbo code will be rate 1/3, i.e. each third bit provides information while the other two are parity bits.

The modems should have a robust or covert mode entailing a data rate of 75 infobits per second (ibps), and a high data rate mode sending 4000 symbols per second.

The transmitter power needs to be variable, it will necessarily be different on different nodes in order to maintain balanced signal strength between the signals received from different nodes. A maximum transmitter output power of 180 dB is judged sufficient to reach communication ranges up to 4 – 5 km in a noisy environment, or in an environment with unfavourable signal propagation.

The nodes have passive, directional sensors that provide detection and localization parameters in some frequency band. These sensors also form communication receivers in the nodes. We choose to separate the communication frequencies from the surveillance frequencies, even if the protocols can be designed to handle a more general case. The target parameters are obtained from the nodes passive sensors and the associated signal processing. There is also an acoustic transducer which, in addition to the communication signals, can be used for sending out a few pings upon request from the command center. We can conclude that the node computer will have to perform automated detection and localization as well as ordinary communication processing.

Typically, a target parameter message will contain about 600 infobits that provide node number, time for detection, frequency band, localization data like bearing, etc.

Finally, we assume that the position of the nodes are accurately determined and that each node is equipped with a clock which provides an accurate timing for detection, time gates etc. The surface buoy is assumed to have GPS.

2.4 Data frame specifications for the modems

Each data frame consists of a training sequence, a header, and a message according to the tables 1-2 below. We have assumed that the header will be protected by a rate 1/3 turbo code having a blocksize, or interleaver size, equal to 960 coded bits. Of these, 317 constitutes information bits. In this header block we double the symbol length, tantamount to reduce the data rate by 50%, in order to obtain a lower risk for biterrors. The message part of the frame will be protected by the same turbo code but having an interleaver size of

1920 coded bits, of which 637 are information bits. An alternative way to protect the frame is to first provide the header with some error correcting code, and then use the same turbo code for header and data together with a doubling of the interleaver size. This will be investigated later in the project.

The frame which will be used in the covert mode is given in table 1 below:

Acquisition and training PRBS (Pseudo Random Binary Sequence) of length 2047.	Header with information about message length, type of information, etc., 317 infobits.	Message with target data, 637 infobits
~ 0.51 s	~ 7.2 s	~ 7.2 s

Table 1. Frame for the covert mode with data rate 75 infobit per second. The lower row gives the calculated time length in seconds for the frame parts, assuming an available band width of 4 kHz. The covert signals are direct sequence spread spectrum with 15 chip per symbol.

Thus, the total frame size is about 15 s for the covert mode. The frame for the high data rate mode is about 0.6 s long:

Acquisition and training using a PRBS of length 511	Header data, 317 infobits	Message, 637 infobits
~ 0.13 s	~ 0.24 s	~ 0.24 s

Table 2. Frame for the high data rate mode of 4000 symbols per second. For a QPSK modulation this corresponds to 2667 infobit per second, considering that each third bit carries information. We have assumed a raised cosine shaping of the symbols with which a passband bandwidth of 4000 Hz is sufficient.

In rare cases a modem should, upon request from the command center and via the gate way buoy, transmit raw data. Each such message is about 100 kbit long. Using the rate 1/3 turbo code we need to transmit about 300 000 coded bits. Assuming a data rate of 10 kbit per second, we need a transmission time of about 30 seconds in the uplink. During this time, the network will not be able to send or receive anything else. It may still be able to detect passages in another frequency band.

Propagation times from node to gateway vary between 0.3 - 2 s, depending on the distance. The guard time after reception of a packet at a receiving node is 0.2 s. After this guard time the node can receive the next package, provided the source levels of the transmitting nodes have been balanced (two different transmitting nodes should have about the same level at the receiving node). The guard time after a transmission, i.e. when the reverberation from the transmitted signal has levelled off enough for reception to be possible is set to 1 s.

The traffic model is sparse, we expect to detect one target per 10 min. The network has an energy detector running. The communication in the network is assumed to be triggered by a chirp signal – the detecting modem transmits it to the gate way which broad casts a similar signal to wake up the remaining modems. The entire network can be in sleep mode when it is not even surveying anything, but it can be waked up from the command center through a suitable signal mediated via the gateway.

3. Medium Access Control

A very important issue that needs to be resolved in order to make networks working is the medium access control (MAC). This is the mechanism that determines the rules on how the nodes access the common transmission channel. This is specifically important in the underwater acoustic channel since this medium is far more complex and difficult to handle than the average used radio channel.

In general, MAC can be divided into two different types, conflict-free protocols that assure that collisions do not occur, and contention-based protocols, where nodes contend for the channel when needed and possible conflicts are resolved whenever they occur.

Example of conflict-free MAC protocols are time division multiple access (TDMA), where each user is given their own time slot, or frequency division multiple access (FDMA) where each user is given a unique part of the frequency spectrum. Another example is code division multiple access (CDMA) where coding techniques is used to divide the available channel into separate (more or less independent) channels. For CDMA, either frequency hopping or direct sequence can be considered although in the latter the near-far problem needs to be specifically resolved since the channels then cannot be made fully orthogonal.

In short, the near-far problem is when a node tries to receive from a user far away, but there is a transmitter close by which power will interfere with the weaker one. In cellular networks this is resolved by power control, but this is difficult in more general network structures, since the closer node may be transmitting to someone far away as well.

Therefore, for an ad hoc (or mesh) structure, only time division fully makes the MAC protocol conflict-free, since it is usually difficult to transmit and receive at the same time even if the channels are completely separate.

More advanced protocols of this type can for example be scheduled protocols as spatial reuse TDMA (STDMA), where time slots can be reused if the distance is sufficient far away. Such rescheduling can achieve very high capacity but requires very much information about the network, which may be expensive in mobile networks.

The contention-based protocols does not try to guarantee conflict-free transmissions (although some protocols try to avoid them), conflicts are instead detected and handled by retransmissions. The simplest of these protocols is Aloha. A node that has a packet to send with this protocol simply sends it, if it collided at the receiver the node waits a random time before retransmission. This protocol is not very efficient but it needs an absolute minimum of information about the network. It does need a feedback channel though, to be informed about failed transmissions.

A more popular protocol is Carrier Sensing Multiple Access (CSMA), it differs from Aloha in that sense that before a transmission is attempted, a node listens (receives) on the channel to see whether it is used. Only if no transmissions are detected the node will transmit a packet. The general problem with this approach is that sensing can be done on the transmitter side, while collisions occur at the receiver. In a network where everybody can communicate directly this is less of a problem than if direct communication is not possible since this creates the so called hidden terminal problem. The receiver is already busy but this cannot be detected due to the other transmitter is out of range.

Furthermore, CSMA is sensitive to long propagation times even in a single hop network. If the propagation time of the packet is a significantly large time compared to the time it takes to send the packet, CSMA starts to perform as bad as Aloha (or actually worse).

To resolve some of these problems in multi-hop networks, collision avoidance protocols have been introduced. This was first suggested in [6] as Multiple Access Collision Avoidance (MACA) and works such that a node first sends a short request-to-send packet (RTS), the receiver then replies with a clear-to-send (CTS) if reception is possible, nodes that hear these messages refrain from sending for a while. Ideally only RTS packets now collide, which should be short packets and the longer data packets are safe from collision. In reality this does not always work so well, and for long propagation times we now have two round trip times added on the packet, during which other nodes need to refrain from sending.

The WLAN standard IEEE 802.11 is in ad hoc mode based on CSMA combined with CA to handle the hidden terminal problem, and is now the by far most used protocol for ad hoc radio networks due to that it is standardized and cheap to deploy.

3.1 Problems caused by the acoustic channel

Significant work on MAC for radio networks exists, only more recent have the problem been expanded to find good solutions for creating networks using the underwater acoustic channel. There are several important differences between the radio channel and the acoustic channel.

The absolutely most important difference is the propagation delay over the channel. In radio communications the propagation delay is usually only a small part of the delay of a packet and guard times can easily be used without significant loss of capacity.

In the acoustic channel, propagation delays are significant and normally the main part of the delay of a packet. Since the delay from transmitting a packet to reception can be seconds, and the fact that a packet will arrive at the different receiver at very different time instances make most of the MAC protocols developed for radio function much less efficiently in underwater networks based on the acoustic channel.

Another important difference is capacity of the links; the acoustic links usually have much lower obtainable data rates than what can be expected in a radio network, which will also have consequences for MAC performance, since this will limit the overhead we can allow.

An additional problem is the turn around time when going from transmission to reception, this can cause some problems also in a radio, but in the acoustic case it is a larger problem. Local reflections close to the transmitter will make it very difficult to receive a much weaker signal until these disappear, which can be a significant time sometimes.

3.2 Previous suggested solutions

In general most suggested solutions for acoustic networks have (not surprisingly) been based on more or less modified techniques from radio networks. See for example [7] for a good overview of some practical issues in underwater communications.

Although some earlier projects have used FDMA, this has mostly been due to modem limitations [8]. Much work have suggested protocols similar to MACA and [9, 10, 11, 12]

are some examples of these protocols. They all assume shorter distances and thereby less propagation delay than what is common in our scenario though.

In [13, 14], the use of CDMA is suggested as MAC protocol, but this assumes that the nodes are well spread out at a similar distance to solve the near-far problem, which may be possible in a centralized scenario. In itself CDMA is a bit limited method for resolving the MAC problem though since additional mechanisms in term of frequency, time division or random access needs to be added in order to avoid transmitting and receiving at the same time. CDMA may be interesting as an addition to a first solution, although, the use of CDMA also requires more complex modems.

3.3 Suggested Solutions for further studies

Due to the problems of many of the previous described solutions, we will choose to describe two different techniques that could potentially be solutions in our scenario.

Aloha

The first method is simply to use the original Aloha protocol. This protocol does not really assume anything about the channel and the large propagation time has mostly impact on acknowledgement of packets and the delay we will get.

In short, the basic protocol can be described as follows: Each time an idle node gets a packet to transmit it directly sends this packet, then it waits until it knows whether the packet arrived correctly. If this is the case, the node can then return to idle or send a new packet if one has arrived. If the packet collided, the node waits for a random time interval and then retransmits the packet. This is then repeated until the packet is received correctly or the maximum number of allowed retransmissions is reached and the packet is discarded.

However, some things are missing. In the original definition of Aloha, the transmitter's knowledge on occurred collisions are sent on a separate feedback channel, which we do not have available here. In addition, the transmission scheme is of type "stop and wait", i.e. we do not send the next packet before we know that the previous one has arrived correctly. This may lead to inefficiencies for long propagation delays, especially for streams of packets.

Some updates of Aloha that might make it work better are needed in a multi-hop network. First, acknowledgements are needed for all packets, these must be sent on the same channel as the packets themselves. However, depending on traffic type we may or may not need to respond immediately. If the packet is the first in a chain of packets it might be better to wait and acknowledge several packets, while a single packet should be acknowledged as quickly as possible.

As long as there is only one stream, this can easily be handled with a combination of the techniques used in the Transmission Control Protocol (TCP) and additional information, included in the packet, that informs the receiver on how acknowledgements are expected to be handled. In TCP a sliding window is used to allow several packets to be unacknowledged at the same time. Each time a new packet is transmitted the window length is increased and every time a packet is acknowledged it is decreased. It has a maximum size though, after that number of packets has been sent without receiving an acknowledgement, no new packets are allowed to be sent.

To increase efficiency in the process, each packet is given a sequence number and acknowledgements are given by sending the highest number of the so far correctly received packets for which all lower numbered packets also have been correct. We can clarify this with a small example. Assume that all packets up to number 9 have been correctly received. If a packet with number 11 arrives, we know that number 10 have been lost (or delayed), to report this we will once again acknowledge packet number 9 (assuming an acknowledgement was sent when 9 arrived). From this second acknowledgement of packet 9 the sender now knows that packet 10 was lost but that later packets still arrive, and will retransmit packet 10. Once packet 10 arrives in the receiver, it can now acknowledge packet 11, since it now have all packets up to number 11 correctly received.

A problem in the acoustic channel, though, is that the sending or receiving of acknowledgements may collide with the actual transmissions of messages. This has the potential of significantly decreasing the efficiency of Aloha. One way to avoid this is to add a flag in the transmitted packets to inform the receiver of periods of silence in the transmitter when it will be receiving packets, after single packet transmissions this will always be done. For a chain of packets, breaks can be added now and then depending on the application. How well this will work when several nodes are competing for the channel is another question though that needs to be studied further. Some knowledge about the delay between the nodes could still be useful though, so that the transmitter have some idea on when an acknowledgment can be expected and when it can consider a packet to be lost.

Aloha is probably the only usable protocol in a totally random network where most or all nodes are mobile and we have little available information on the network status. Even in a more static network, where only few nodes are moving, it may be the only solution for initializing the network.

Link Scheduling

The second method to use is the STDMA scheme. If we only use the normal TDMA scheme where each node has their own time slot, we end up with the problem that each node can choose which one of its neighbors it will send information to each time the time slot is used. Since distance to the different neighbors is different, this means that propagation time also is different, in general the only way to make sure we have no collisions in the receiver is to have a time slot that includes the (largest) propagation time, thus giving us very long time slots and low efficiency as a result.

However, for STDMA we also have an assignment strategy called link assignment (or link activation) that schedules not only sender but also receiver. If the propagation delay on this link is known (or possible to estimate) a schedule can be created that do not use normal time slots, i.e. all nodes try to see the duration of a time slot simultaneously and time can be considered discrete. Instead the time axis will be continuous, and a scheduled transmission on one link will not occur at the same time as the scheduled reception on the same link.

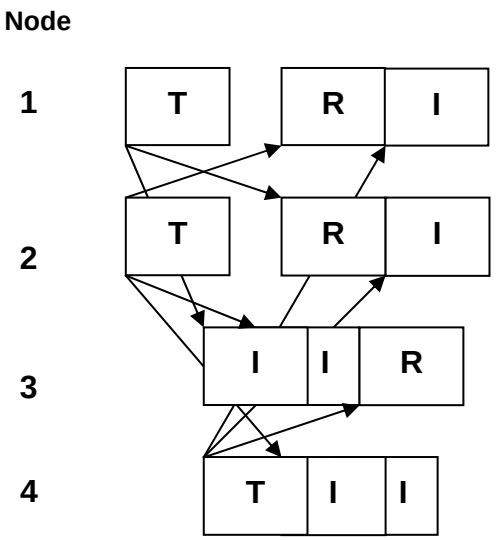


Figure 3: Example of how a short part of a generalized schedule can look like as seen from each node. Transmissions (T) can collide with Interference (I), but Receptions (R) must not collide with anything.

Time, in a more general sense than normal time slots, can now be reused if the nodes are sufficiently far apart. With each scheduled transmission and reception, we also need to schedule interference slots in the rest of the neighboring nodes, these interference "slots" cannot be allowed to collide with scheduled reception in these nodes, but there is no problem if they collide with scheduled transmissions, and of course they may also collide with other interference "slots" without problems. In Figure 3 we show how such a schedule could look like in the different nodes.

There are some additional considerations that need to be added in order to make this work well. One is the turn around time when we go from transmission to reception, so that we do not interfere with ourselves. This can be handled by adding an interference event just after a transmission to avoid scheduling a reception at that instant (or we prolong the scheduled transmission and do not use the full time slot, but that means that transmission time slots would be longer than reception time slots).

A second issue is similar but on a smaller scale. Due to multi-path the impulse response might be considerably spread in time and a guard time between scheduled receptions is necessary. Errors in the estimates of the propagation delay are also adding to the need of a guard time. It is important for efficiency that the guard times are kept small, while sufficiently large, to avoid interference between transmissions.

A third issue is mobility, similarly to radio networks it will cause new links and link breaks. This will enforce rescheduling. We will also see changes of reception times and interference times in the other nodes due to the variability in propagation time. If only a few nodes are mobile and the mobility is low we can potentially handle the last issue with larger guard times for all events regarding the mobile node. However, estimating the transmission times to and from the mobile node will be difficult since transmission events and interference events can be scheduled at the same time in neighboring nodes.

In general, designing a mobile acoustic ad hoc network is a great challenge and it will be difficult to make it efficient. However, there are some properties in our scenario that further simplifies the solution. First, traffic flow is presently only flowing from the nodes

to a central access point (AP) and back again. This means that nodes do not need to communicate among each other, except perhaps for relaying data to and from the AP. This means that the used links in the network will form a tree with the AP as the root.

Further, in our main scenario the access point is within the range of all nodes which will allow us to use a star topology with the access point as the central node. This significantly simplifies the problem, since this central node can control the scheduling and the only used links will be the links to and from the AP. This means also that spatial reuse will not be possible.

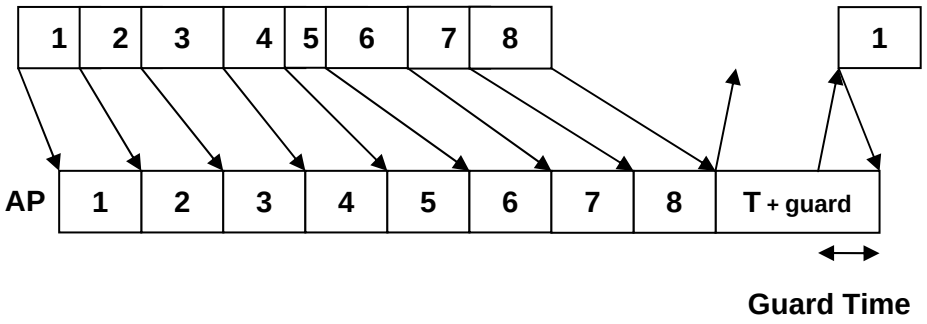


Figure 4: The Proposed Schedule as seen in the access point (bottom) and when each node transmits (top). Notice, since nodes may have different propagation delay to the AP, their scheduled transmissions will overlap, but will be correctly separated when being received in the AP.

In Figure 4 we show a possible schedule that can be used, as it is seen from the access point. This can be regarded as the default schedule when the network is waiting on events. However, all time slots can be quickly rescheduled by the AP. Each time slot in the schedule will be 0.8 s long; this allows one high rate packet (0.6 s) and a guard time of 0.2 s between receptions from the different nodes as stated in Chapter 2. The AP need to switch from transmission to reception directly in the end of its slot which forces it to use the larger guard time of 1 s. Assuming that the AP uses the same type of packets as the rest of the nodes, this will result in an AP slot of 1.6 seconds length.

In total this gives a schedule length of 8 s after which it is reused and each of the 8 nodes gets a slot in each frame in which it can send a 954 bit packet. If the sensing times are attuned to the scheduling (the opposite is not really possible) the delay from generated packets to reception, at the access point, can be kept low. Since the access point controls the schedule, it can also give several slots to the same node if necessary; although this means that some nodes may not be given a slot in each frame which may increase the detection time for some objects. If not more than half of the slots are required for other use we will not get more than 16 seconds delay, though, to detect any new objects.

Some specific issues still need to be considered when we use a schedule as shown in Figure 4. The first time slots in the schedule should be assigned to the nodes with the shortest propagation delay to the base station. The reason to this is that the first node needs to start sending before the end of the previous frame and at the same time we will have a propagation delay from the access point to one of the nodes (which could be node number 1 in the figure). This round trip time needs to be shorter than 1 second; otherwise we need

to increase the guard time of the AP even further. Turn around time of the other nodes will normally not be an issue unless all nodes are so close so that turn around time is larger than the propagation time of the node furthest away.

The fact that closer nodes send before nodes further away can cause an additional problem. Unless we have some form of power control it is likely that signals from further away is weaker than those from nodes nearby, which might force us to use longer guard times between the nodes.

A large proportion of the time is still used as guard time, though, 32 percent of the time is used as guard time. However, this is no remedy for this problem with only one channel as the guard times is large. Only by using longer time slots can we reduce the percentage of the channel that is used as guard times. However, doing so would also increase delay which is unwanted. An alternative would be using multiple channels, resulting in fewer users per channel, which can be used for shorter schedule lengths or longer time slots.

3.4 Concluding remarks on MAC

The medium access control problem is significantly much more severe in an underwater scenario than for a corresponding radio network. The specific propagation properties are much more difficult and available data rates are in general much lower.

In this chapter we have discussed two solutions to the MAC problem. The first, Aloha, does not require any information about the network and can probably handle even high mobility. However, it will not be especially efficient, and can have problem if many nodes generate data at the same time. The second solution, link scheduling, will allow more efficient access to the channel with predictable delay guarantees. However, this method will require predictable propagation delays and mobility may be difficult to handle. In addition, unless we have access to a centralized scheduler, generating the schedule and distribute it may add additional complexity, at least for a multi-hop network.

The use of some few multiple channels, either through CDMA or FDMA, could be another potential way of increasing the number of users (or throughput of existing users), or possibly decrease the delay. This is obtained in a simpler way than can be done by pure link scheduling today, however, such considerations will be left for future work.

4. Routing

The task of the routing algorithm is to find a path from a sending node to a receiving node through intermediate nodes when necessary. Routing protocols are divided into two categories, namely, proactive and reactive routing protocols. Notice, however, sometimes geographical routing protocols are mentioned as a category of its own. Proactive protocols try to keep an updated table in each node of the network link topology and the routes to the other nodes in the network. Reactive protocols, on the other hand, seek after the routes first when they are needed.

4.1 Routing options

In proactive routing link state information is normally sent to update the topology tables as soon as anything changes in the network topology. This may cause considerable signaling overhead. For this reason, and since the capacity is very limited, proactive routing is considered not suitable in underwater networks [14]. However, it all depends on how much routing updates that are needed. In a static network, or in a network with very few topology changes, proactive routing may still be a good option.

The problem with reactive routing is that it incurs a high latency if the path to the destination is unknown. First, a route search procedure has to be carried out. Due to the slow propagation of acoustic signals, the delay of this procedure is further increased as compared to radio networks.

Geographical routing protocols are often mentioned as suitable for underwater network [15]. The problem is to obtain the positions of the nodes since GPS is not working under water. Assume the positions can be obtained and are distributed in the network, a topology of the network can be built. The difference to proactive routing is that we do not know the conditions of a link, or even if it exists between two nodes based on the positions only. However, geographical routing is based on forwarding packets in the direction towards the receiving node and hoping that the packet arrives. If a packet comes to a dead end, it has to be resent over a new path if such a path exists. Furthermore, when transmissions occur in the network, link states can be collected, and increase the probability of finding a good path.

Even if geographical routing is promising it is difficult in general to point on a suitable routing strategy for underwater networks. Instead efficient routing should be tailored especially for the particular scenario, that is, the number of nodes, the mobility, the applications etc. The drawback with this approach is that new protocols, or modifications of existing ones, most likely have to be designed, implemented, tested, and verified which is time-consuming. Notice that routing is not needed, or is trivial, in a single hop network. Also, in multi-hop networks, a simple, but probably not so efficient solution could be flooding.

4.2 End to end transport protocols

The task of the transport layer is to provide an end-to-end connection, i.e., between two applications which may be located at different nodes in the network. To accomplish that, also flow control and congestion control need to be considered. To use the User Datagram Protocol (UDP) is of course possible, but we assume that a reliable transport protocol is needed. Most existing Transmission Control Protocol (TCP) implementations are unsuited for underwater networks. In fact, the existing rate-based transport protocols seem unsuited

for underwater networks, since they relay on feedback control messages sent back from the destination to adapt the transmission rate. The long and variable round trip time in underwater networks can cause instability in the rate control.

A reliable transport protocol needs to address the particular challenges of underwater networks, that is, large propagation delay, low bandwidths, energy constraints, high error probabilities and varying network topologies. The Segmented Data Reliable Transport (SDRT) protocol is a first attempt to propose such a protocol [16]. The basic idea is to use erasure codes (the so called Tornado codes) to recover dropped packets to reduce retransmissions. Also, several packets are grouped into coded blocks (packet trains) and the receiver feedbacks (acknowledgment) information about whole blocks instead of individual packets to minimize the feedback overhead. For non delay critical applications, the sender can wait on the feedback before the next block is sent. However, for delay critical applications the sender may need to continuously send blocks without waiting for the feedback.

Finding suitable transport protocols for underwater networks is an evolving work. Again the scenario and particular application is very important for the choice.

4.3 A tentative routing solution in an extended scenario

For the static scenario described in Chapter 2 routing is not an issue, everything about the routes in the network can be configured in advance. However, routing is needed if we consider an extended multi-hop version of the scenario which also includes a few mobile AUVs. Here, a tentative routing solution is outlined for this case. Only delay-insensitive traffic is considered. Other solutions are probably needed for delay-sensitive traffic. Since most nodes are static and only a few are mobile (the AUVs) we treat the nodes differently and divide the network into two sub-networks, one static sub-network and one mobile sub-network.

Firstly, an initialization phase is carried out when topology information of the static sub-network is created. This information includes positions of the nodes and link state information about the links between the nodes. The positions can be obtained by GPS before the nodes are placed on the sea bottom, or moored above the sea bottom. Link state information is acquired, e.g., by sending probe signals between the nodes. The topology information is thereafter stored in databases in all the nodes, both the static and the mobile ones. Due to varying channel conditions the link state information has to be updated now and then, however, probably not very frequently in our static case. Normally, the channel conditions do not change dramatically during a short time in our scenario. Furthermore, poor links for which the channel state information is old should be considered as unreliable links and avoided when possible.

During operation, proactive routing (e.g., using Optimized Link State Routing (OLSR)) is used within the static sub-network, i.e., the routes follow directly based on the data base information. Furthermore, a mobile node can predict where to connect to the static sub-network based on the positions of the static nodes. The problem is how to reach a mobile node from the static sub-network and how to find the routes between mobile nodes. There are two possible solution principles to deal with this problem, one proactive and one reactive. In the proactive procedure the mobile nodes send hello messages regularly to update the other nodes about their locations. However, due to a large overhead with such a

proactive procedure we propose to use a reactive one, which can be enhanced in our scenario using available side information in the following way:

When a mobile node connects to a node in the static network it can also inform that node about its movements and where it predicts to connect to the static sub-network in the future. This information can possibly also be distributed in the whole static sub-network. The idea is that this information, when available, guides the reactive route search procedure. Assume a static (or mobile node) wants to send data to a mobile node, then a route request is sent from a suitable node in the static network (or the mobile node) towards an area where the mobile node most likely can be found. If a first route request fails, a new attempt can be made later, or another area can by tried.

5. Summary

The design of underwater wireless acoustic sensor networks is challenging due to low data rates, long propagation delay, energy limitations, difficult channel multipath conditions and difficulty of time synchronization. These constraints, in particular the first two, make it important to utilize the network resources as efficiently as possible. It is therefore advisable to carefully tailor the protocol solution for the particular scenario in order to obtain as much network capacity as possible. A more general protocol solution working in a wide number of scenarios has a tendency to provide a poor capacity when one particular scenario is considered. Some important design considerations are, number of nodes, distances between nodes, number of mobile nodes, operation time of the network, available energy in the nodes and of course the applications the network shall support.

The particular scenario we have considered is a deployed network for surveillance and communication consisting of about eight nodes. A surface buoy functions as the access point and provides RF communication with the command centre. In the report we discuss two different protocol solutions. The first is based on Aloha and the advantage is that such a solution is simple to implement. It will also work if mobile nodes are added. The drawback is an expected low throughput and problem to have any delay bound guarantees.

However, the fact that the nodes are deployed in advance and at fixed locations makes it possible to tailor a more efficient protocol solution based on TDMA. This second proposed protocol solution is centralized and the schedule is controlled by the access point. We have specifically developed a schedule tailored for our application and showed that it can allow each node to send one 954 bit packet every 8 seconds to the access point.

This solution could further be expanded by including multiple channels, e.g. through CDMA, in order to increase capacity and reduce delay. However, this will increase complexity and are left as an option for future studies and experiments.

Notice, as long as we only have about eight nodes at fixed locations, and no multihop, routing is not an issue. If the scenario is extended to include multihop and mobile nodes a routing solution is needed. One tentative solution for such a case is discussed in which the network is divided into two sub-networks, a static and a mobile one. The idea is to store the positions of all the static nodes and link state information in all the nodes. The mobile nodes, and through them the mobile network, can then predict where and how they should connect to the static network and update the static network about those connections.

6. References

[1] Proc. IEEE OCEANS ’07, Aberdeen, Scottlnad 18-21 June 2007.

[2] Thomas J. Cutler, ”Dutton’s Nautical Navigation”, Publisher: US Naval Institute Press; 15 edition (December 2003).

[3] Erland Sangfelt, Tommy Öberg, ”Undervattenskommunikation 2006. Operativ och teknisk anpassning”. FOI-R--2143—SE. December 2006.

[4] Erland Sangfelt, Magnus Lundberg Nordenvaad, Niten Olofsson, Bernt Nilsson, Paul van Walree, Tommy Öberg, ”Underwater communication in the Baltic using Iterative Equalization”, in Proc. UAM 07, Krete, Greece, 25-29 June, 2007.

[5] Tommy Öberg, Bernt Nilsson, Niten Olofsson, Magnus Lundberg Nordenvaad, and Erland Sangfelt; ”Underwater communication link with iterative equalization”. Proceedings of Oceans’06, Boston, USA.

[6] P. Karn, ” MACA - A new channel access method for packet radio,” ARRL/CRRL Amateur Radio 9th Computer Networking Conference, 1990, , pp. 134-140.

[7] J. Partan, J. Kurose, and B. Levine, “A survey of practical issues in underwater networks,” *In Proceedings of WUWNet’06*, Sept, 2006.

[8] J. Rice et al. “Evolution of Seaweb underwater acoustic networking”, In Proceedings of IEEE Oceans 2000, Volume 3, ppp 2007-2017, Sep, 2000.

[9] P. Xie and J.-H. Cui, “Exploring Random Access and handshaking techniques in large-scale underwater wireless acoustic sensor networks,” in Proceedings of Oceans’06, Boston, USA

[10] A. Syed, W. Ye, and J. Heidemann, *T-Lohi: a new class of MAC protocols for underwater acoustic sensor networks*, USC/ISI Technical Report ISI-TR-638, Apr, 2007.

[11] B. Peleato and M. Stojanovic, “A MAC protocol for underwater acoustic sensor networks,” *In Proceedings of WUWNet’06*, Sept, 2006.

[12] M. Molins and M. Stojanovic, “Slotted FAMA: a MAC protocol for underwater acoustic networks,” in Proceedings of IEEE Oceans’06 Asia Pacific Conference, Singapore, 2006.

[13] E. Sozer, M. Stojanovic, and J. Proakis, “Underwater acoustic networks,” IEEE Journal of oceanic engineering, vol-25, No 1, Jan, 2000

[14] I. Akyildiz, D. Pompili, and T. Melodia, “Underwater acoustic sensor networks: research challenges”, Ad Hoc Networks 3, pp.257-279, July 2005.

[15] T. Melodia, D. Pompili, and I. F. Akyildiz, “Optimal local topology knowledge for energy efficient geographical routing in sensor networks,” in *Proceedings of IEEE INFOCOM 2004*, Hong Kong S.A.R., PRC, March 2004.

[16] Xie, Peng; Cui, Jun-Hong, An FEC-based Reliable Data Transport Protocol for Underwater Sensor Networks, Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on Volume , Issue , 13-16 Aug. 2007 Page(s):747 - 753