# Short Paper: Jamming-Resistant Multi-path Routing for Reliable Intruder Detection in Underwater Networks

Michael Goetz[⋆◇], Saiful Azad[‡], Paolo Casari[‡§], Ivor Nissen[◇], Michele Zorzi[‡§]

[⋆]Fraunhofer Institute for Communication, Information Processing and Ergonomics, 53343 Wachtberg, Germany
[‡]Department of Information Engineering, University of Padova, via Gradenigo 6/B, 35131 Padova, Italy
[◇]Research Department for Underwater Acoustics and Marine Geophysics (FWG), 24148 Kiel, Germany
[§]Consorzio Ferrara Ricerche, via Saragat 1, 44122 Ferrara, Italy
michael.goetz@fkie.fraunhofer.de, {azad, casarip, zorzi}@dei.unipd.it, ivornissen@bwb.org

## ABSTRACT

In this paper, we discuss the performance of multi-path routing techniques in underwater acoustic networks applied to an intruder detection scenario. We assume that a network of submarine sensors is deployed close to a surveilled harbor, with the task to detect outbound surface boats. The communications take place in the 4 to 8 kHz band, in order to favor long-haul transmissions. This band is highly affected by the noise originating from the boat propellers. Therefore, we resort to jamming-resilient techniques such as multipath transmissions. The latter is accomplished by restricted flooding, and by an adaptive form of source routing as an alternative.

Our results show that the inherent redundancy of multi-path routing offers an effective shield against excessive packet losses in the presence of strong jamming. This increases the probability that data packets containing detection information are promptly delivered to the desired sinks, with respect to the performance of static, single-path routing. In particular, restricted flooding achieves the best delivery ratio at the price of a very high number of generated replicas, whereas adaptive source routing trades off a lower delivery ratio for a lower overhead.

## Categories and Subject Descriptors

C.2.0 [**Communication/Networking and Information Technology**]: General—*Data communications*; I.6.6 [**Simulation and Modeling**]: Simulation Output Analysis

## General Terms

Measurement, Performance

## Keywords

Underwater acoustic networks, movement detection, jamming resilience, multi-path routing, simulation

## 1. INTRODUCTION

The development and experimentation of collaborative strategies is turning modern navies into international cooperating forces, where vessels from different nations may collaborate to accomplish a common objective, often in international waters. In such a scenario, communications and situational awareness are of primary importance; this includes the surveillance not only of the sea surface, but also of the submarine environment. To establish and maintain a safe operating area, the use of autonomous sensors on the surface and the seafloor is envisioned [1]. These networks may detect relevant information such as movement via, e.g., magnetic or acoustic sensors; in addition, their acoustic communications equipment makes it possible to transmit such information to data-collecting endpoints in contact with the rest of the fleet.

Acoustic communications, in this case, also obey a practical constraint, i.e., to deploy the network rapidly without elaborated wiring. The nodes will be connected via acoustic links, and build a self-configuring underwater network. For this purpose, a project with name *Robust Acoustic Communication in Underwater Networks* (RACUN) led by Atlas Elektronik, Germany, was started in 2010 in the framework of the *European Defense Agency* (EDA), funded by and in collaboration with the Governments/MoDs of Italy, Germany, Norway, Sweden and The Netherlands. RACUN has the objective to develop and demonstrate the capability to establish a robust ad hoc underwater acoustic network for multiple purposes, using both mobile and stationary nodes. Among the purposes of the network, the project targets general support for surface vessel operations via data collection from underwater nodes. This is also the case we consider in this paper.

In more detail, we focus on an underwater intrusion detection network, deployed at the entrance of a harbor in order to monitor outbound surface boats (also called "intruders" for brevity in this paper). The presence of the network is unknown to the boats. In order to maintain this status, the nodes forward data to collaborating surface vessels by means of acoustic communications only. Also, no gateway buoys are placed very close to the harbor to act as surface sinks and gateways. This measure avoids that such equipment may be detected and stolen, or tampered with.

A further design objective regards the coverage of acoustic communications, which should allow the network to monitor a sufficiently large area with only a few nodes. In turn, this calls for a multihop configuration, where each hop spans 5 to 10 km, so that a line of nodes can monitor a wide portion of the coast, while at the same time being able to haul data out to a sea base at a safe distance, several hops away. A basic design guideline stemming from the sonar and empirical noise power spectral density equations in [2,3] suggests that acoustic communications over such distances should be operated in the 4 to 8 kHz band, in different shipping and wind conditions. The main concern with this band, however, is that it is highly affected by the noise generated by boat propellers, es-

*WUWNet'11,* Dec. 1 - 2, 2011, Seattle, Washington, USA
Copyright 2011 ACM 978-1-4503-1151-9 ...$10.00.

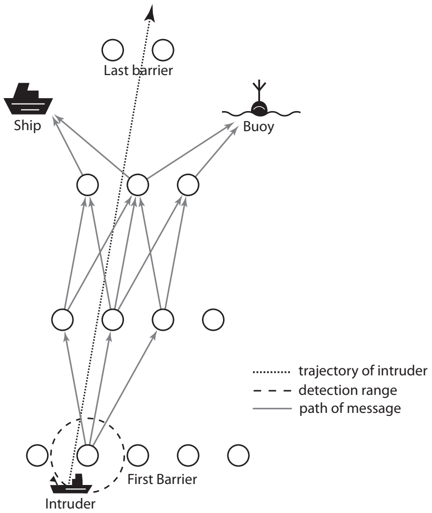

**Figure 1: Harbor surveillance network, with 14 bottom nodes organized in 4 parallel barriers. A ship and a buoy act as sea-borne sinks and gateways. Grey links show the forwarding paths obtained using the RF strategy (see Section 3.2.2).**

pecially by those of speedboats [4, 5], which are the main target of the movement detection network. This noise may disrupt communications. In order to cope with this problem, we propose to exploit the redundancy of multi-path routing to increase the probability that detection data is correctly delivered. In other words, multiple routes allow data to escape jamming,[1] in that at least one route is hopefully sufficiently free of the propeller noise generated by the boats. Note that for this detection application it is not necessary that $100\%$ of the detection data reaches the sink: a subset of the generated packets would suffice to reconstruct the movement of the boat to a rougher degree of accuracy: however the number of detections should not be too low, otherwise the received data may be interpreted as a false alarm, and therefore neglected.

## 2. SCENARIO AND SYSTEM PARAMETERS

With reference to Fig. 1, we assume that an underwater acoustic network is deployed in the proximity of a harbor to be surveilled. All nodes are bottom-mounted and organized in subsequent lines, or barriers. The first barrier is placed in front of the harbor, and is composed of 5 nodes, in order to obtain good coverage along the coast. The distance between nearest neighbors within a barrier is $3\,\mathrm{km}$. The sensing range is $2\,\mathrm{km}$. Every $8\,\mathrm{km}$ comes another barrier which can sense movement as well as relay data, and has one node less than the previous one, so that 2 nodes constitute the fourth and last barrier. Again, this reflects the need to provide finer movement readings near the coast. The network covers a total area of $16\,\mathrm{km} \times 32\,\mathrm{km}$. The intended maximum transmission range of a node in RACUN amounts to about $10\,\mathrm{km}$, hence adjacent barriers are typically in range of each other. We finally assume that a ship and a gateway buoy are deployed close to the last barriers to act as sea-borne sinks and gateways towards the sea base. More details about this scenario can be found in [6].

The traffic generation pattern in this scenario is inherently event-based. In a real application, the message generation frequency could also be tuned to provide finer knowledge of the node movements: one of our objectives is to evaluate how this affects the network performance. All messages will be relayed to the sink using one of the routing strategies described in the next section. The size of a detection message is set to 16 bytes, according to the Generic Underwater Application Language (GUWAL) [6].

Although the number of nodes is reduced after each barrier, the network features high connectivity, and multiple paths exist between the nodes. This makes the network robust against node failures, as well as against link breakage caused by jamming. In addition, it makes no difference which sink first receives a given data packet, as they are assumed to be connected to each other and to the sea base via other radio (terrestrial or satellite) links.

## 3. ROUTING PROTOCOLS

In this Section, we describe our routing strategies, which include both single-path and multi-path routing. The latter is obtained either via restricted flooding or with a form of adaptive source routing. The redundancy of multi-path routing is introduced to reduce the impact of jamming noise from the boat leaving the harbor.

Our protocols are proactive, i.e., they exchange routing information and find paths before actual network operations, which is feasible here due to the static network topology. Therefore, the delivery of data packets takes less time. An on-demand route discovery process would take too long in a networks with such long distances and propagation delays, and in addition it may also be interfered by the jamming noise. In the following, we introduce our route establishment procedure, and subsequently three routing strategies, used to forward the data packets to the sinks.

### 3.1 Route establishment

The route establishment in our protocols is conducted by the sinks. Each sink broadcasts a control packet every 5 minutes, which includes the sink address, a sequence number and a hop count field. Using a shortened 2-byte network address, the size of this packet is 6 bytes (2 bytes for each field).

Every bottom node which receives the message adds the sink to its routing table, and stores the hop distance and the last hop address, which is included in the MAC header. If a node receives the control packet for the first time, it increments the hop distance by one and rebroadcasts it. Duplicates received from other neighbors are not discarded, but stored to have alternative routes available if links break due, e.g., to temporary interference or node failures.

Routing entries are declared outdated $i$) after a period twice as long as the broadcast interval of the message from the sinks, or $ii$) if a packet with a higher sequence number and the same originating sink and the same last hop address as the current entry is received.

We note that a multi-point relay selection (MPR) does not work here, in contrast to, e.g., the Optimized Link State Routing (OLSR) [7], which employs MPR to reduce the flooding overhead of control packets. In fact, we require that a complete flooding is carried out to cover all nodes, and collect a sufficient number of alternative routes involving potentially any neighbors. This way, there is a greater probability that one of the known routes still works, even in the presence of a node generating jamming noise.

### 3.2 Data forwarding

After a bottom node has received at least one control packet from one of the sinks, it can start transmitting detection data. As mentioned before, we implemented three different forwarding strategies, which are described in the following subsections. The first one represents single-path routing, supporting anycast addressing, in that a packet can be received by either sink. The second one uses restricted flooding in the direction of the sinks. The third strategy selects disjoint paths from a topology graph inferred from control

[1] In this paper, the word jamming describes possibly unintentional interference coming from a source other than the network nodes.

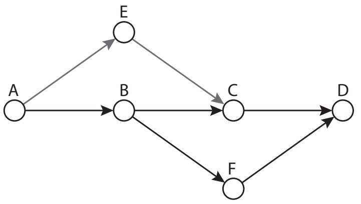

**Figure 2: Example of data forwarding using MSRP.**

messages, and forwards the data via source routing to the different sinks.

### 3.2.1 *Single-path routing (SP)*

In this case, whenever a node wants to transmit data, it searches in its routing table for the sink reachable with the smallest number of hops. Then, the node sends the data packet by specifying a next hop field, so that only the node addressed in such field will receive the packet and forward it further with the same technique. With this technique, the packet is routed back to the closest sink on the shortest reverse path. If a node notices that the next hop is not responding, it can select another neighbor from the routing table. Also, if routing entries become obsolete the node can directly select another routing entry from the list without being forced to wait until the next control packets are broadcast.

The advantage of this strategy is its low overhead, which sums up to only one address field; moreover, no unnecessary duplicates are sent. However, this also makes the protocol more vulnerable to jamming and broken links.

### 3.2.2 *Restricted Flooding (RF)*

The restricted flooding strategy (or selective flooding) [8] takes advantage of the fact that all nodes know the minimum hop distance to a sink. If a node has data to send, it adds only a time-to-live (TTL) field to the packet, before broadcasting it. The TTL field is set to the hop distance of the closest sink. All nodes which receive this packet look into their routing tables and forward the packet only if they know a route to that sink with shorter or equal TTL.

Fig. 1 shows how this forwarding strategy works in our scenario. The node in the first barrier broadcasts its packet; all nodes in the second barrier which receive the packet will forward it further, and so forth. Therefore, the packet will be received by both sinks in most cases. To limit unnecessary replica generation, if a node on a barrier re-broadcasts a data packet, all nodes on the previous barrier will drop it. This strategy is more robust than single-path routing, but such robustness comes at the price of the additional overhead due to the possibly many duplicates generated. The robustness can be improved (at the price of an increased overhead) by increasing the start value of the TTL field. For example, if the TTL value is increased by one, all nodes in the same barrier will also forward the data packet.

### 3.2.3 *Multi-sink routing protocol (MSRP)*

Whereas the information about the hop count and the last hop is sufficient for the first two algorithms, the third variant needs additional topology knowledge. In particular, we need to construct a topology graph, which in turn requires that each signaling packet stores the identities of the nodes that relay it downstream. This gives rise to additional overhead during route establishment, but allows all bottom nodes to find disjoint paths to the different sinks.

In our version of this protocol, we select two paths from the graph, one for each sink, possibly involving disjoint nodes. To guarantee that the packets are routed along these chosen paths, we pre-determine all hops via source routing.

We also extended the route establishment phase, via a technique similar to that described in [9] for the graph-based multi-path routing. The basic idea is to collect additional information about the topology by making every node wait a few seconds after receiving a control packet before forwarding it. During this waiting period, the node collects duplicates of the control packets transmitted via other routes. The path information in each packet is merged, and a more complete topology sub-graph is transmitted when forwarding the control packet further. Figure 2 shows how an additional waiting period can lead to additional routes. If every node forwarded the control packet directly, node D would only learn the routes A→B→C→D and A→B→F→D, which are not disjoint. The route A→E→C→D (which is disjoint from A→B→F→D) would not be found, because C would forward the packet from B and therefore drop the packet coming later from E. This problem can be mitigated by waiting before propagating signaling messages, thereby merging route information at each intermediate node. However, the argument above depends heavily on the network topology. In particular, an additional waiting period does not always lead to better routes in the RACUN topology. Moreover, the additional overhead produced by the merged graphs reduces the performance of our protocol. In fact, it turns out that routing to multiple sinks already leads to sufficiently disjoint routes, as opposed to the case of data routing towards the same destination through multiple paths. Therefore, for all simulations we set the waiting period to zero.

Before proceeding, we stress that we focus on routing in this paper, and employ a medium access control protocol as simple as ALOHA. This separates the routing performance results from the performance of lower-level protocols. In addition, ALOHA is a feasible choice in large multihop networks as discussed in [10]: this is true also in our scenario, where the small packet size and large propagation delay make it unlikely that many collisions take place, and jamming noise is the major source of packet losses.

## 4. SIMULATION RESULTS

The evaluation of the network performance has been carried out using the nsMiracle simulator [11]. The scenario reflects the topology of Fig. 1. All nodes are deployed at an average depth of about $1000\,\mathrm{m}$, and each has a detection range of about $2\,\mathrm{km}$. There are two static sinks, one on the left side and a second one on the right side of the network. The boat to be detected (or "intruder") leaves the shore and enters the detection range of the nodes in the first barrier. As long as the intruder is within the detection range of a node, that node will generate detection packets, which are to be routed to either sink using one of the routing algorithms described in Sect. 3. These packets are $16\,\mathrm{Bytes}$ long, and are generated at a fixed rate as long as the boat is within the detection range. We test the network performance over typical packet generation rates of interest in RACUN, from 1 to 6 packets per minute. We simulate imperfect detections by applying a $5\%$ chance that a detection fails: in this case, the corresponding packet is not generated. Control packets are $6\,\mathrm{Bytes}$ long, plus an additional $2\,\mathrm{Bytes}$ for every source routing entry in MSRP.

The nodes communicate in the RACUN band, from $4$ to $8\,\mathrm{kHz}$. The transmission bit rate is $256\,\mathrm{bps}$, which corresponds to a transmission time of $0.5\,\mathrm{s}$ for a detection packet. The transmit power of each node is $157.3\ \mathrm{dB\ re}\ \mu\mathrm{Pa}$, and has been set so that two subsequent barriers can communicate, but no node can reach two barriers away. The attenuation of the acoustic signals is computed via the link budget model in [2, 3]. The noise in this case is generated both by the environment and by the engines of the intruder, which acts as a de-facto jammer. In order to test the network performance under

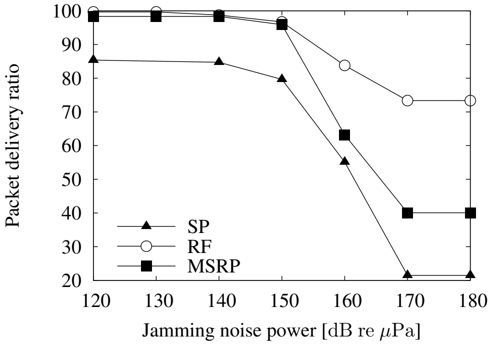

**Figure 3: Packet delivery ratio as a function of the jamming noise power for a packet generation rate of** $6$ **pkt/min.**

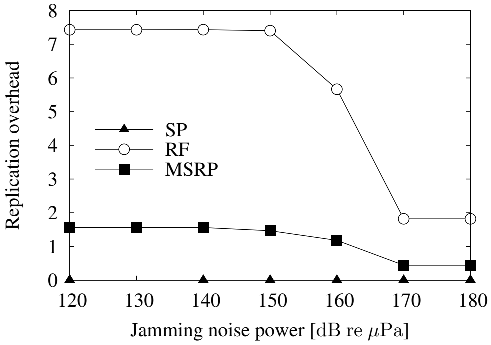

**Figure 4: Packet overhead as a function of the jamming noise power for a packet generation rate of** $6$ **pkt/min.**

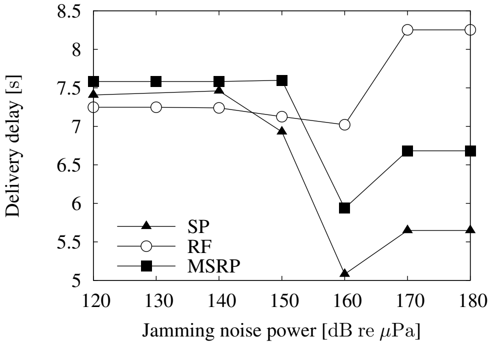

**Figure 5: Delivery delay as a function of the jamming noise power for a packet generation rate of** $6$ **pkt/min.**

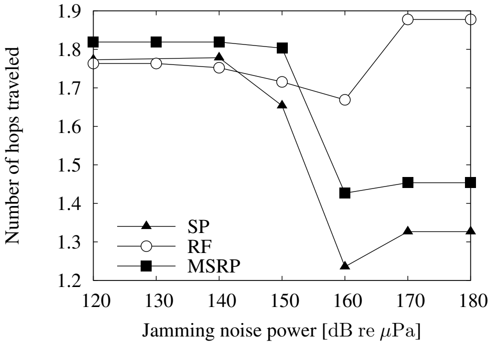

**Figure 6: Number of hops traveled per packet as a function of the jamming noise power for a packet generation rate of** $6$ **pkt/min.**

different jamming power, in our results we also vary such power from $120$ to $180$ dB re $\mu$Pa.

The simulation results are averaged over several runs, each featuring a different, random position of the nodes within a circular area of radius $500\,\mathrm{m}$ around their nominal location. The trajectory of the node exiting the harbor is always a straight line, whose starting point and direction are also randomized at each run. The speed of the intruder is fixed to $10\,\mathrm{knots}$. The background noise level, inferred from the empirical equations in [2], is $34$ dB re $\mu$Pa.

Figs. 3 to 6, depict the average packet delivery ratio (PDR), the packet overhead, the average delivery delay and the number of hops traveled per packet, respectively. All metrics have been calculated based only on the first copy that reaches either sink: the PDR is the average fraction of generated packets that reach either sink; the delivery delay is the average time elapsed from the generation of the original packet to when the first copy reaches either sink; the number of traveled hops is similarly defined as the average route length incurred by the first packet copy that correctly reaches either sink; finally, the packet overhead is the average ratio of the number of duplicate packets that reach the sinks to the number of generated packets.

In Fig. 3 we plot the average packet delivery ratio against the jamming noise power caused by the intruder. The generation rate of detection packets is fixed to $6\,\mathrm{pkt/min}$. As expected, the single-path (SP) protocol fails to deliver $100\%$ of the transmitted packets, even in the presence of a low-power jammer. This is due to errors caused by noise and collisions over the long-haul links in Fig. 1. (Recall that we focus on routing approaches in this paper, and thus do not consider specific medium access protocols or error control schemes.) Multi-path approaches may exploit the redundancy offered by multiple transmissions at the price of greater overhead, whereas the SP protocol cannot: an erroneous transmission over any link of the only route leading from the source to the sink would result in a lost packet. For low jamming power, both the restricted flooding (RF) algorithm and the multi-sink routing protocol (MSRP) achieve near-$100\%$ delivery ratios. On the contrary, for high jamming MSRP performs worse, as it saves on the number of replicas via a form of source routing, which requires updates before a new route can be established. This procedure is also subject to errors as route update packets, albeit very short and frequently sent, may be corrupted by the jamming noise. However, the multi-path behavior still gives MSRP an advantage over SP. RF works best thanks to local flooding in the direction of the sinks, which gives rise to more packet replicas.

The latter statement is proven by Fig. 4, which shows the much larger overhead induced by RF with respect to MSRP. (The overhead of SP is $0$.) At high jamming power, around 2 of the many replicas generated by RF survive, whence its higher PDR.

The delivery delay and number of hops traveled by a packet are very similar for all policies (see Figs. 5 and 6 respectively). We observe that for low jamming power, the delay is about $7.5\,\mathrm{s}$, as the average is taken over both short and longer routes. As the jamming noise increases, the detection packets traveling the longest routes get corrupted and are sometimes lost, whence the decreasing PDR in Fig. 3. Conversely, the packets traversing a lower number of hops reach the sink with high probability. As the average delay is computed only over correctly received packets, its value decreases. When the jamming power increases beyond $160$ dB re $\mu$Pa, the interference considerably affects even shorter routes, and the delay increases again. The greater number of replicas created by RF (responsible of the better PDR) comes also at the price of longer routes, which also leads to longer delays. We infer that RF's performance would get worse if the routes got longer: a possible countermeasure would be to increase the number of sinks if the number of nodes increases. As a final note on this first set of results, the average number of hops required to reach a sink is always on the order of 1 to 2: this is a consequence of the deployment of the network in barriers, and of the placement of the sinks on the left and right of the third barrier. In fact, the packets generated by the first barrier require about 3 hops to reach one of the sinks (see also Fig. 1), those generated by the second barrier require about 2 hops, whereas the last two barriers make it to the closest sink in one hop.

We conclude our evaluation of the SP, RF and MSRP routing protocols by briefly noting that their packet delivery ratio is almost constant as a function of the number of packets generated by the bottom nodes (figure omitted for brevity). This is a consequence of two facts: $i$) the detection packets are short, which helps keep them separated in time, and $iii$) the traffic generation pattern is strongly event-based, which limits the amount of generated traffic. The same observations apply also in the absence of the jammer. With respect to this case, the drop observed when the jammer is present is about 15% for RF, and about 30% for SP and MSRP. The other metrics considered in the first part of this section are also quite insensitive to the packet generation rates.

## 5. RELATED WORK

There exists a wide range of routing protocols for wireless ad hoc networks, typically defined as proactive or reactive, depending on whether or not routes are established before they are actually used to convey traffic. In this paper, we focus on proactive protocols only, which help reduce the delay before a detection packet is reported to a sink, and also avoid that route establishment packets are jammed on their way to the sinks. For terrestrial ad hoc networks, many multi-path protocols were also developed. For example, Multipath-DSR (M-DSR) [12], extends the Dynamic Source Routing (DSR) [13] protocol by replying to multiple Route Requests (RREQ) which carry a link-disjoint path. However, duplicate RREQs can still be dropped at intermediate nodes, hampering the discovery of disjoint paths (see also Sect. 3.2.3). Split Multipath Routing (SMR) [14] counters this problem by introducing a different route discovery mechanism, requiring more control packets. However, such a high control overhead would not be feasible in underwater networks. A different approach is taken in the Graph-based Multipath Routing (GMR) [9] protocol. GMR includes graph information in the control packets during route discovery, in order to build a mostly complete network graph at the destination. A local graph search algorithm is used to find disjoint paths. GMR will finally select only one path, while retaining the alternatives for use in case of link breakage on the current path. This reduces the delivery delay, as no route rediscovery is necessary. In this paper, we used multiple routes simultaneously, with the objective to enhance robustness against jamming and to improve the probability of correct data delivery. These guidelines have been followed in the design of MSRP (see Sect. 3.2.3). Another important difference between MSRP and other multipath protocols is that, in our scenario, each sensor can report its detection to any of the sinks, which makes the network multi-source, multi-sink, and anycast, unlike general-purpose communication networks.

## 6. CONCLUSIONS

In this paper, we compared one single-path (SP) and two multi-path routing protocols for underwater acoustic networks in terms of resilience against in-band jamming noise. The two multi-path protocols achieve jamming resistance via restricted flooding (RF) or via adaptive source routing (MSRP). Overall, we concluded that the best protocol in terms of PDR is RF, whereas SP is the worst. However, the absence of multi-path routing overhead in SP can make it a good candidate whenever the power of jamming noise is known to be significantly lower than the power of received signals. MSRP is a protocol with intermediate performance, and represents a good tradeoff between the requirements of high PDR and limited overhead, even though its PDR may suffer in the presence of very high jamming noise.

Future work on this topic includes an evaluation of the protocols for varying number of static and mobile sinks.

## Acknowledgment

The work described in this publication was done under a multinational four-year project with the name "Robust Acoustic Communications in Underwater Networks" (RACUN) under the EDA Project Arrangement No. B 0386 ESM1 GC. The partners are: Atlas Elektronik (Germany), WTD71-FWG (Germany), L-3 Communications ELAC Nautik (Germany), TNO (The Netherlands), Köngsberg Maritime (Norway), FFI (Norway), FOI (Sweden), SUS (Sweden), WASS (Italy) and CETENA (Italy).

## 7. REFERENCES

[1] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: research challenges," *Elsevier's Ad Hoc Networks*, vol. 3, no. 3, pp. 257–279, May 2005.

[2] R. Urick, *Principles of Underwater Sound*. New York: McGraw-Hill, 1983.

[3] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," *ACM Mobile Comput. and Commun. Review*, vol. 11, no. 4, pp. 34–43, Oct. 2007.

[4] B. Kipple and C. Gabriele, "Underwater noise from skiffs to ships," in *Proc. of Glacier Bay Science Symposium*, Juneau, AK, Oct. 2004.

[5] S. Amoser, L. E. Wysocki, and F. Ladichc, "Noise emission during the first powerboat race in an alpine lake and potential impact on fish communities," *J. Acoust. Soc. Am.*, vol. 116, no. 6, pp. 3789–3797, Dec. 2004.

[6] M. Goetz and I. Nissen, "Generic Underwater Application Language (GUWAL) – A Specification Approach," FWG, Kiel, Germany, Tech. Rep. WTD71–0161/2010, Jun. 2010.

[7] T. Clausen and P. Jacquet, Eds., *Optimized Link State Routing Protocol (OLSR)*. United States: RFC Editor, 2003.

[8] M.-Y. Iu, "Selective flooding in ad hoc networks," 2002. [Online]. Available: http://etd.uwaterloo.ca/etd/my2iu2002.pdf

[9] G. Koh, D. Oh, and H. Woo, "A graph-based approach to compute multiple paths in mobile ad hoc networks," in *Proc. of HSI*, Seoul, South Korea, Jun. 2003.

[10] M. Zorzi, P. Casari, N. Baldo, and A. F. Harris III, "Energy-efficient routing schemes for underwater acoustic networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 9, pp. 1754–1766, Dec. 2008.

[11] N. Baldo *et al.*, "MIRACLE: The Multi-Interface Cross-Layer Extension of ns2," *EURASIP J. on Wireless Commun. and Networking*, Jan. 2010. [Online]. Available: http://www.hindawi.com/journals/wcn/2010/761792/cta/

[12] A. Nasipuri, R. Castaneda, and S. R. Das, "Performance of Multipath Routing for On-demand Protocols in Mobile Ad Hoc Networks," *ACM/Kluwer Mobile Networks and Applications*, vol. 6, no. 4, pp. 339–349, 2001.

[13] D. B. Johnson and D. A. Maltz, *Mobile Computing*. Kluwer Academic Publishers, February 1996, ch. Dynamic source routing in ad hoc wireless networks, pp. 153–181.

[14] S. J. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in *Proc. of IEEE ICC*, Helsinki , Finland, Jun. 2001.