A Resilient Routing Algorithm for Long-term Applications in Underwater Sensor Networks

Dario Pompili, Tommaso Melodia, Ian F. Akyildiz

Broadband and Wireless Networking Laboratory
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, GA 30332
e-mail: {dario, tommaso, ian}@ece.gatech.edu

***Abstract*— Underwater sensor networks will find applications in oceanographic data collection, pollution monitoring, offshore exploration, disaster prevention, assisted navigation, and tactical surveillance. Underwater acoustic networking is the enabling technology for these applications. In this paper, the problem of data gathering for three-dimensional underwater sensor networks is investigated at the network layer by considering the interactions between the routing functions and the characteristics of the underwater acoustic channel. A two-phase resilient routing solution for long-term monitoring missions is developed, with the objective of guaranteeing survivability of the network to node and link failures. In the first phase, energy-efficient node-disjoint primary and backup paths are optimally configured, by relying on topology information gathered by a surface station. In the second phase, paths are locally repaired in case of node failures.**

I. Introduction

UNDERWATER sensor networks are envisioned to enable applications for oceanographic data collection, ocean sampling, pollution and environmental monitoring, offshore exploration, disaster prevention, assisted navigation, tactical surveillance, and mine reconnaissance. Wireless underwater acoustic networking is the enabling technology for these applications. UnderWater Acoustic Sensor Networks (UW-ASNs) [1] consist of sensors that are deployed to perform collaborative monitoring tasks over a given three-dimensional volume. Acoustic communications are the typical physical layer technology in underwater networks. In fact, radio waves propagate through conductive salty water only at extra low frequencies $(30 - 300\ Hz)$, which require large antennae and high transmission power. Optical waves do not suffer from such high attenuation but are affected by scattering. Thus, links in underwater networks are usually based on *acoustic wireless communications* [2].

Although there exist many recently developed network protocols for terrestrial wireless ad hoc and sensor networks, the unique characteristics of the underwater acoustic channel require very efficient and reliable new communication protocols. Major challenges in the design of UW-ASNs are: i) the available bandwidth is severely limited; ii) high bit error rates and temporary losses of connectivity (shadow zones) can be experienced; iii) sensors are prone to failures because of fouling and corrosion; iv) battery power is limited and usually batteries cannot be easily recharged; v) propagation delay is five orders of magnitude higher than in radio frequency terrestrial channels; vi) the channel is severely impaired, especially due to multipath and fading.

Most impairments of the underwater channel are adequately addressed at the physical layer, while characteristics such as limited bandwidth, temporary losses of connectivity, and sensor failures need to be addressed at higher layers. For these reasons, we present a resilient routing algorithm tailored for long-term critical monitoring missions. It follows a two-phase approach consisting of a centralized algorithm, based on a network manager that resides on a surface station, and on an online localized algorithm that guarantees survivability of the network to node and link failures. Given the characteristic of the underwater channel and the 3D volume that the application needs to monitor, we introduce a model to set the optimal packet size, which is a critical factor to achieve reliability and energy efficiency.

The remainder of this paper is organized as follows. In Section II, we discuss the suitability of the existing sensor routing solutions for the underwater environment. In Section III, we introduce a communication architecture for 3D UW-ASNs, while in Section IV we present an optimization problem to set the optimal packet size for long-term monitoring applications. In Section V, we propose our resilient routing algorithm. Finally, in

Section VI we show the performance results, while in Section VII we draw the conclusions.

II. Related Work

In the last few years there has been an intensive study in routing protocols for ad hoc [3] and wireless sensor networks [4]. However, due to the peculiar nature of the underwater environment and applications, there are several drawbacks with respect to the suitability of existing routing solutions for underwater networks. Existing routing protocols are divided into three categories, namely *proactive*, *reactive*, and *geographical* protocols.

Proactive protocols provoke a large signaling overhead to establish routes for the first time and each time the network topology is modified because of mobility or node failures. For this reason, they are not suitable for underwater networks. Reactive protocols are more suitable for dynamic environments but incur a higher latency and still require source-initiated flooding to establish paths. These protocols are unsuitable for UW-ASNs as they also cause high latency in the establishment of paths, which is even amplified underwater by the slow propagation of acoustic signals. Moreover, the topology of UW-ASNs is unlikely to vary consistently on a short-time scale. Geographical routing protocols are very promising for their scalability feature and limited required signaling. However, GPS (Global Positioning System) radio receivers do not work properly in the underwater environment. Still, underwater devices need to estimate their current position in order to be able to associate the sampled data with the 3D position of the device that generates the data, irrespective of the chosen routing approach.

Some recent papers propose network layer protocols specifically tailored for underwater acoustic networks. In [5], a routing protocol is proposed that autonomously establishes the underwater network topology, controls network resources, and establishes network flows, which relies on a centralized network manager running on a surface station. Although the idea is promising, the performance evaluation of the proposed mechanisms has not been thoroughly studied. In [6], a vector-based forwarding (VBF) routing is developed, which does not require state information on the sensors and involves only a small fraction of the nodes in routing. The proposed algorithm, however, does not consider applications with different requirements. In [7], the authors provide a simple design example of a shallow water network, where routes are established by a central manager based on neighborhood information gathered from all nodes by means of poll packets. The paper, however, does not discuss the criteria used to select data paths. In [8], a long-term monitoring platform for underwater sensor networks consisting of static and mobile nodes is proposed, and hardware and software architectures are described. The nodes communicate point-to-point using a high-speed optical communication system, and broadcast using an acoustic protocol. However, due to the limitations of optical transmissions, communication is enabled only when sensors and mobile mules are in close proximity.

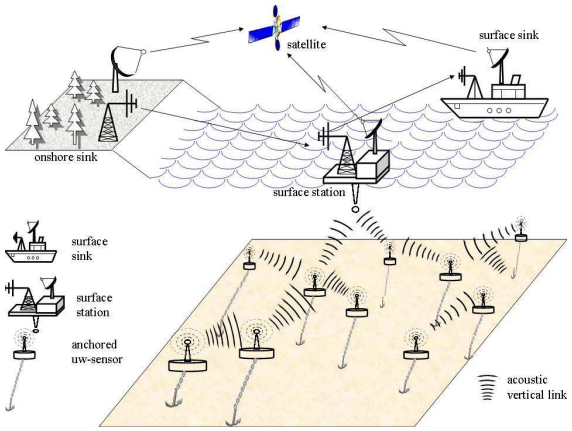


Fig. 1. Architecture for 3D Underwater Sensor Networks

III. Network Architecture and Models

In this section, we introduce a communication architecture for 3D UW-ASNs, and the network and propagation models that will be used in the formulation of our routing algorithm. These networks are used to detect and observe phenomena that cannot be adequately observed by means of ocean bottom sensor nodes, i.e., to perform cooperative sampling of the ocean environment [1]. In three-dimensional underwater networks, sensor nodes float at different depths to observe a given phenomenon. Our approach is to anchor winch-based sensor devices to the bottom of the ocean, as depicted in Fig. 1. Each sensor is equipped with a floating buoy that can be inflated by a pump. The buoy pulls the sensor towards the ocean surface. The depth of the sensor can be regulated by adjusting the length of the wire that connects the sensor to the anchor, by means of an electronically controlled engine that resides on the sensor. The main strengths of such an architecture are that sensors: i) are not vulnerable to weather and tampering or pilfering, ii) cannot be easily detected and deactivated by enemies in military settings, and iii) do not obstruct ship navigation.

The underwater network can be represented as a graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = \{v_1, .., v_N\}$ is a finite set of nodes in a finite-dimension 3D volume, with $N = |\mathcal{V}|$, and

$\mathcal{E}$ is the set of links among nodes, i.e., e_{ij} equals 1 if nodes v_i and v_j are within each other's transmission range. The node v_N (also N for simplicity) represents the sink, i.e., the surface station. $\mathcal{S}$ is the set of sources, i.e., those sensors that sense information from the underwater environment and send it to the surface station.

The transmission loss $TL(d, f)$ $[dB]$ that a narrow-band acoustic signal centered at frequency f $[KHz]$ experiences along a distance d $[m]$ is described by the Urick propagation model [9],

$$TL(d, f) = 20 \cdot Log(d) + \alpha(f) \cdot d + A. \quad (1)$$

In (1), which models how the acoustic intensity decreases as a pressure wave propagates outwards from a sound source, $\alpha(f)$ $[dB/m]$ represents the *medium absorption coefficient* and quantifies the dependency of the transmission loss on the frequency band. The quantity A $[dB]$ is the so-called *transmission anomaly*, and accounts for the degradation of the acoustic intensity caused by multiple path propagation, refraction, diffraction, and scattering. Its value is higher for shallow-water horizontal links (up to 10 dB), which are more affected by multipath [9]. More information can be found in [1].

IV. Underwater Optimal Packet Size

In this section, we study the effect of the characteristics of the underwater environment on the optimal packet size for delay-insensitive long-term monitoring applications. We consider a generic medium access control (MAC) protocol where a device transmits a data packet and the corresponding device acknowledges the correct reception with a short ACK packet. We assume that the payload of the data packet to be transmitted has size L^D bits, while the header has size L^H bits. Moreover, the packet may be protected with a forward error correction (FEC) mechanism, which introduces a redundancy of L^F bits. $\hat{N}^{TX}$ represents the average number of link transmissions such that a packet is successfully decoded at the receiver. It is defined as $\hat{N}^{TX} = [1 - \psi^{\mathcal{F}}\left(L, L^F, BER\right)]^{-1}$, where $\psi^{\mathcal{F}}()$ represents the *packet error rate* (PER) given the packet size L and the *bit error rate* (BER) on the link, when a FEC scheme $\mathcal{F}$ with redundancy L^F is adopted.

We define the packet efficiency $\eta(L, L^F)$ as

$$\eta(L, L^F) = \frac{L - L^H - L^F}{\hat{N}^{TX} \cdot L}, \quad (2)$$

which is the ratio of the packet payload and the packet size multiplied by the average number of transmissions such that a packet is successfully decoded at the receiver. The optimal packet size (L^*) and packet FEC redundancy (L^{F*}) are chosen in such a way as to maximize the packet efficiency in (2), as it is cast in the optimal packet size problem $\mathbf{P_{Size}}$ for long-term monitoring applications. We introduce the notations that are used in the problem formulation:

- $P^{TX}_{i,max}[W]$ is the maximum transmitting power for node i, and $\overline{P}^{TX}_{max}[W]$ is the average among all nodes of the maximum transmitting power;
- $\Pr\{l\}$ is the distance distribution between neighboring nodes, which depends on how nodes are statistically deployed in the volume (for a random 3D deployment, $\Pr\{l\}$ is derived in [10]);
- r and f_0 are the bit rate and central frequency;
- $BER = \Phi^{\mathcal{M}}\left(\frac{\overline{P}^{TX}_{max}}{r \cdot \overline{N_0} \cdot \overline{TL}}\right)$ describes the average bit error rate on a link; it is a function of the ratio between the average energy of the received bit $\overline{P}^{TX}_{max}/(r \cdot \overline{TL})$ and the expected noise $\overline{N_0}$ at the receiver, and it depends on the modulation scheme $\mathcal{M}$;
- $PER = \psi^{\mathcal{F}}\left(L, L^F, BER\right)$ describes the packet error rate on a link, given the packet size L, the FEC redundancy L^F, and the bit error rate BER, and it depends on the adopted FEC technique $\mathcal{F}$.

$\mathbf{P_{Size}$: Packet Size Problem for Delay-insensitive Long-term Monitoring Applications in UW-ASNs

$$\begin{aligned} Given: &\quad \overline{P}^{TX}_{max}, r, f_0, \overline{N_0}, \Pr\{l\}, \psi^{\mathcal{F}}(), \Phi^{\mathcal{M}}() \\ Find: &\quad L^*, L^{F*} \\ Maximize: &\quad \eta(L, L^F) = \tfrac{L - L^H - L^F}{\hat{N}^{TX} \cdot L} \\ Subject\ to: & \end{aligned}$$

$$BER = \Phi^{\mathcal{M}}\left(\frac{\overline{P}^{TX}_{max}}{r \cdot \overline{N_0} \cdot \overline{TL}}\right); \quad (3)$$

$$\overline{TL} = \int_0^{\infty} TL(l, f_0) \cdot \Pr\{l\} dl; \quad (4)$$

$$\hat{N}^{TX} = [1 - \psi^{\mathcal{F}}\left(L, L^F, BER\right)]^{-1}. \quad (5)$$

The optimal packet size L^* is found by maximizing the packet efficiency (2) for different FEC schemes $\mathcal{F}$ and code redundancies L^F, under proper constraints. The packet size is optimized given the distance distribution between neighboring nodes $(\Pr\{l\})$, which determines the average transmission loss $\overline{TL}$, and ultimately the BER, computed as a function $\Phi^{\mathcal{M}}()$ of the modulation scheme $\mathcal{M}$ and the average signal-to-noise ratio at the receiver, as formally defined in (3). Thus, $\mathbf{P_{Size}}$ jointly finds the optimal packet size and packet FEC redundancy, given the device characteristics $\left(\overline{P}^{TX}_{max}, r, f_0, \psi^{\mathcal{F}}, \Phi^{\mathcal{M}}\right)$, the deployment volume and node density, which impact the distribution between neighboring nodes $(\Pr\{l\})$, and the average ambient noise $(\overline{N_0})$, as

$$(L^*, L^{F*}) = argmax_{(L, L^F)}\, \eta(L, L^F). \quad (6)$$

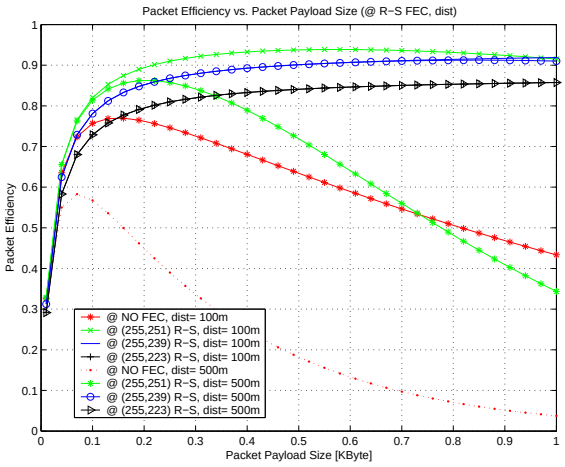


Fig. 2. Underwater packet efficiency vs. packet payload size for different average node distances in delay-insensitive applications

Figure 2 shows the underwater packet efficiency vs. packet payload size L^D for different node distances, given the distance distribution between neighboring nodes $(\Pr\{l\})$. For a volume with an average node distance of $100\ m$, the highest packet efficiency $(\eta^* = 0.94)$ is achieved with a packet payload size of $L^{D*} = 0.55 KByte$ and a $(255, 251)$ Reed-Solomon (R-S) FEC, while for a volume with an average node distance of $500\ m$, the highest packet efficiency $(\eta^* = 0.91)$ is achieved with a packet payload size of $L^{D*} = 0.9\ KByte$ and a $(255, 239)$ R-S FEC. Note that $\mathbf{P_{Size}}$ finds the optimal packet size and packet FEC redundancy for delay-insensitive applications *off-line*, whereas the strength of the FEC technique may be adjusted *on-line* according to the dynamic channel conditions. The choice of a fixed packet size is motivated by the need for system simplicity and ease of sensor buffer management. In fact, a design proposing per-hop optimal packet size would encounter several implementation problems, such as the need for segmentation and reassembly functionalities that incur tremendous overhead, which requires advanced buffer management techniques.

V. Resilient Routing Algorithm for UW-ASNs

The reliability requirements of long-term critical underwater missions, and the small scale of underwater sensor networks, suggest to devise routing solutions based on some form of centralized planning of the network topology and data paths, in order to optimally exploit the scarce network resources. Hence, the proposed solution relies on a *virtual circuit* routing technique, where multihop connections are established *a priori* between each source and sink, and each packet associated with a particular connection follows the same path. This requires centralized coordination and leads to a less flexible architecture, but allows exploiting powerful optimization tools on a centralized manager (e.g., the surface station) to achieve optimal performance at the network layer with minimum signaling overhead.

The proposed routing solution follows a *two-phase* approach. In the *first phase*, the network manager determines optimal *node-disjoint primary* and *backup* multihop data paths such that the energy consumption of the nodes is minimized. This is needed because, unlike in terrestrial sensor networks where sensors can be redundantly deployed, the underwater environment requires minimizing the number of sensors. Hence, protection is necessary to avoid network connectivity being disrupted by node or link failures. In the *second phase*, an on-line distributed solution guarantees survivability of the network, by locally repairing paths in case of disconnections or failures, or by switching the data traffic on the backup paths in case of severe failures. The emphasis on survivability is motivated by the fact that underwater long-term monitoring missions can be extremely expensive. Hence, it is crucial that the deployed network be highly reliable, so as to avoid failure of missions due to failure of single or multiple devices. The protection scheme proposed can be classified as a dedicated backup scheme with 1:1 path protection, with node-disjoint paths. Link protection schemes are not suitable for the underwater environment as they are too bandwidth consuming [11].

A. First Phase: Centralized Routing Problem

We formulate the problem of determining optimal primary and backup data paths for UW-ASNs as an *Integer Linear Program* (ILP) [12], where:

- e_{ij} is a binary variable representing a link that equals 1 iff nodes i and j are within each other's transmission range, while c_{ij} is the cost of the link between nodes i and j, i.e., the energy needed to transmit one bit;
- $f_{ij}^{1,s}$ and $f_{ij}^{2,s}$ are binary variables that equal 1 iff link (i, j) is in the *primary* or in the *backup* data path from the source s to the surface station, respectively;
- u_i is the capacity of node i (number of concurrent flows, ingoing and outgoing, that it can handle), while l_{ij} is the capacity of link (i, j) (number of concurrent flows that can be transmitted on the link).

$\mathbf{P_{Rout}}$: Optimal Node-disjoint Routing Problem

$$
\begin{aligned}
Given: &\quad \mathcal{G},\ \mathcal{S},\ e_{ij},\ c_{ij},\ w_1,\ w_2,\ u_i,\ l_{ij} \\
Find: &\quad f_{ij}^{1,s*},\ f_{ij}^{2,s*} \\
Minimize: &\quad C^T = \textstyle\sum_{s\in\mathcal{S}} \sum_{(i,j)\in\mathcal{E}} c_{ij} \cdot (w_1 f_{ij}^{1,s} + w_2 f_{ij}^{2,s}) \\
Subject\ to: &
\end{aligned}
$$

$$
\sum_{j\in\mathcal{V}} (f_{sj}^{x,s} - f_{js}^{x,s}) = 1, \forall s \in \mathcal{S},\ x = 1, 2; \qquad (7)
$$

$$\sum_{j\in\mathcal{V}}(f_{Nj}^{x,s}-f_{jN}^{x,s})=-1,\forall s\in\mathcal{S},\ x=1,2; \quad (8)$$

$$\sum_{j\in\mathcal{V}}(f_{ij}^{x,s}-f_{ji}^{x,s})=0,\forall s\in\mathcal{S},\forall i\in\mathcal{V},i\neq s\ and\ i\neq N,x=1,2; \quad (9)$$

$$f_{ij}^{x,s}\leq e_{ij},\forall s\in\mathcal{S},\forall i\in\mathcal{V},\forall j\in\mathcal{V},\ x=1,2; \quad (10)$$

$$\sum_{s\in S}(f_{ij}^{1,s}+f_{ij}^{2,s})\leq l_{ij},\forall i\in\mathcal{V},\forall j\in\mathcal{V}; \quad (11)$$

$$\sum_{s\in S}\left[\sum_{j\in V}(f_{ji}^{1,s}+f_{ji}^{2,s})+\sum_{j\in\mathcal{V}}(f_{ij}^{1,s}+f_{ij}^{2,s})\right]\leq u_i,\forall i\in\mathcal{V}; \quad (12)$$

$$f_{ji}^{1,s}+\sum_{n\in\mathcal{V}}f_{ni}^{2,s}\leq 1,\forall s\in\mathcal{S},\forall i\in\mathcal{V}\ s.t.\ i\neq N,\forall j\in\mathcal{V}. \quad (13)$$

The objective function of problem $\mathbf{P_{Rout}}$ aims at minimizing the overall energy consumption as a sum of the energy consumptions of all links that compose the primary and backup data paths. Two different weights w_1 and w_2 are assigned to the primary and backup data paths, respectively, with $w_1 + w_2 = 1$. By increasing w_2 we are increasing the weight of the backup paths in the optimal solution, i.e., we are trying to obtain energy efficient backup paths. This may worsen the energy consumption of the primary data paths, and should be done only in scenarios where we expect nodes to fail often, as will be discussed in Section VI. In general, we will have $w_2 << w_1$. Constraints (7), (8), and (9) express conservation of flows [12], i.e., each source generates a flow that has to reach the sink. Constraint (10) forces data paths to be created on links between adjacent nodes. Constraint (11) ensures that the sum of all flows (primary and backup) transported on a link do not exceed the link capacity, while constraint (12) imposes that the sum of all flows (incoming and outgoing, primary and backup) handled by a sensor node do not exceed the node capacity. Constraint (13) requires the primary and backup paths to be node disjoint. It can be shown that problem $\mathbf{P_{Rout}}$ is at least as complex as the Geometric Connected Dominating Set problem, which is proven to be NP-complete [13]. However, it is still possible to solve the routing problem for networks up to 100 nodes (UW-ASN case).

B. Second Phase: Localized Network Restoration

In the second phase of the proposed resilient routing algorithm, an on-line distributed solution guarantees survivability of the network, by locally repairing paths in case of disconnections or failures. Let us consider the set of connections $\mathcal{G}_i$ for which node i is either a *source* or a *relay* node. We refer to each element in $\mathcal{G}_i$ as g_i^s, i.e., a connection generated by source s and passing through node i. Hence, node i is a *source* for the connection g_i^i, while it is a *relay* for each other connection in $\mathcal{G}_i$, if any. The connections in this second group, i.e., $\mathcal{G}_i \setminus g_i^i$, are referred to as *relayed* connections for i, while g_i^i is referred to as *native* connection for i. The restoration of a network connection at node i is performed in different ways for native and relayed connections, as discussed in the following.

1) Restoration of a Native Connection: We refer to Fig. 3(a) and consider a node i as the source of a native connection g_i^i. Let us assume that j is the next hop of i on its primary path towards the sink. The restoration process is based on a link quality metric q_{ij} that is collaboratively estimated by the two corresponding nodes at each side of link (i, j), i.e., node i counts how many ACK timeouts expire given a certain number of transmitted packets towards j. Based on this link quality, which accounts for both packets corruptions due to channel impairments and receive failures due to collisions, i performs the following operations.

- If $q_{ij} < q^{low}$, the link is considered to be in good standing and no action is taken.

- If $q_{ij} > q^{high}$, or if no acknowledgement is received from j, the link is considered to be impaired altogether. Then, i starts sending the data that it generates to its next hop m on the backup data path. According to $\mathbf{P_{Rout}}$, m is guaranteed to have node capacity reserved for the backup path of i towards the source, and capacity is guaranteed to have been reserved on the backup link (i, m), and on every link on the backup path of i towards the surface station.

- If $q^{low} \leq q_{ij} \leq q^{high}$, the link is considered to be in an intermediate state. Hence, i assumes that the quality of link (i, j) on the primary path is degrading. Therefore, i starts transmitting duplicated packets on the backup path, and, thus, starts computing estimates q_{im} of the quality of link (i, m). If $q^{low} \leq q_{im} \leq q^{high}$, i keeps transmitting all packets on both the primary and backup paths in order to increase the end-to-end reliability. Conversely, if the quality of the backup link is good, i.e., $q_{im} < q^{low}$, node i tears down the connection on the primary path to save energy. Finally, if $q_{im} > q^{high}$, node i tears down the connection on the backup path.

As a final remark, if the quality metrics of the links on the primary and backup data paths are both below q^{low}, i.e., $q_{ij} < q^{low}$ and $q_{im} < q^{low}$, node i stops transmitting for a time $T_{blackout}$. After that, it probes the primary and backup links to check if their quality has improved. If not, i sends the data to a random neighbor in the positive advance set.

2) Restoration of Relayed Connections: Let us consider a relayed connection $g_i^s \in \mathcal{G}_i$, generated by a source

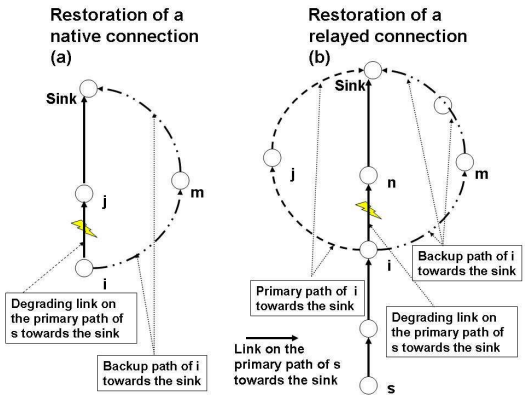


Fig. 3. Restoration of a native (a) and relayed connection (b)

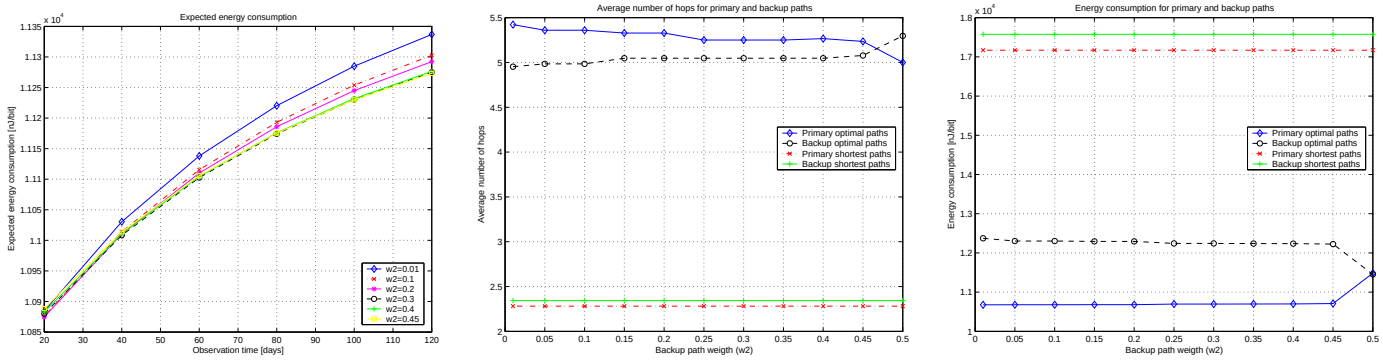
s and relayed by node i. By referring to Fig. 3(b), let us assume that node n is the next hop of node i on the primary data path for the relayed connection g_i^s. As in the previous case, nodes j and m are the next-hop nodes of i on the primary and backup data paths towards the sink, respectively, while node i monitors the quality of link (i, n). However, if the quality of (i, n) degrades, node i itself cannot switch the connection on the backup path of s. In fact, i is not a relay node for the backup path of s towards the sink, since primary and backup paths are node disjoint. Hence, node i could either inform source s of the relayed connection to switch to its reserved backup path, or try to locally find an alternate path. Since informing source s would involve signaling from i back to the source, incurring in high energy consumption and delay, we propose a localized solution that tries to take advantage of possibly available local paths and uses the capacity reserved at source s only in the worst case, when no capacity is locally available. Hence, i tries to accommodate the relayed connection g_i^s on its own primary or backup data paths, since they are likely to be on energy efficient paths towards the sink. However, neither the node capacity of next hops j and m, nor the capacity of links (i, j) and (i, m) are guaranteed to be sufficient to accommodate the relayed connection. This happens because $\mathbf{P_{Rout}}$, implemented at the surface station, finds backup paths on an end-to-end basis (path protection). In other words, the primary path is protected by a node-disjoint backup path, but not every single link of the primary path is protected by its own backup path (link protection). Hence, each connection is guaranteed to have backup capacity reserved only on a path that starts from its source node. Therefore, i tries to route the failing connection on its primary or backup data paths, but it may fail due to lack of capacity. Thus, according to the available node and link capacities on links (i, j) and (i, m), their link qualities q_{ij} and q_{im}, and the link quality q_{in} of the original link (i, n), i decides whether to use one or both of its primary and backup data paths, according to the rules in Section V-B.1. Note that n could coincide with either i or j, which would restrict the choice to only two data paths. If at any step in the end-to-end path towards the sink no node or link capacity is available, an error message is sent back. Each intermediate node tries to find an alternate path on its own primary and/or backup paths, as explained above. In the worst case, the source of the relayed connection is reached by the error message, which triggers a switch to the backup path. Connections that are using the capacity reserved for other connections are treated as best effort and can be preempted by those connections the capacity is reserved for.

TABLE I
SOURCE BLOCK PROBABILITY (SBP) VS. OBSERVATION TIME

Obs. Time [Days]	20	40	60	80	100
SBP (λ=**1 year**$^{-1}$)	0.05	0.18	0.33	0.47	0.55
SBP (λ=**1/2 year**$^{-1}$)	0.02	0.05	0.12	0.18	0.26
SBP (λ=**1/3 year**$^{-1}$)	0.01	0.03	0.07	0.1	0.15

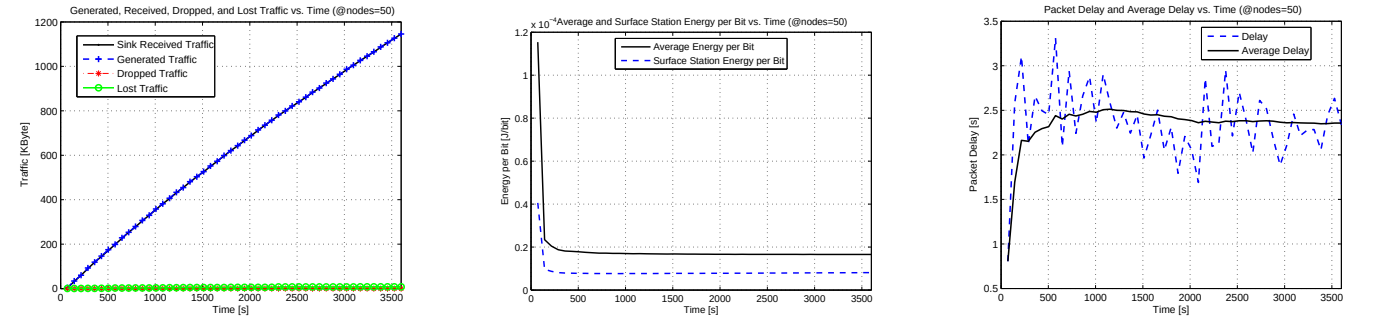
VI. PERFORMANCE EVALUATION

The optimization problem $\mathbf{P_{Rout}}$ presented in Section V-A was implemented in AMPL [14], and solved with CPLEX [15]. In Figs. 4(a-c), we compared its performance with a simpler solution, where two node-disjoint shortest weighted paths are calculated with an energy metric. We considered 50 sensors randomly deployed in a 3D volume of 500x500x50 m^3, which may represent a small harbor, and we set the bandwidth to 50 $Kbps$ and the maximum transmission power to 5 W. In particular, Fig. 4(a) shows the expected energy consumption of the network by weighting the cost of the primary and backup paths with the probability of using each of them. We adopted a Poissonian model with failure rate $\lambda = 1/2\, year^{-1}$ to capture the reliability of each sensor node (in average one node failure every two years). The expected energy consumption increases with the observation time, and decreases with increasing w_2. This happens because by increasing w_2 the objective function of $\mathbf{P_{Rout}}$ weights more the backup paths. Hence, when failures occur, the connections are switched to backup paths characterized by lower energy consumption, which ultimately results in decreased energy consumption. This phenomenon becomes more evident with increasing observation time. Table I shows the source block probability (SBP) with increasing observation time, when



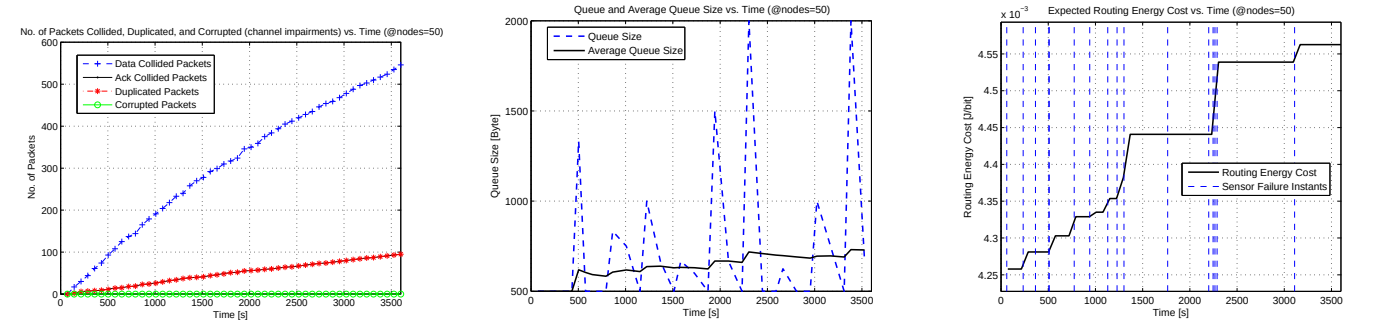
(a) (b) (c)

Fig. 4. (a): Expected energy consumption for primary and backup paths; (b): Average number of hops for primary and backup paths (optimal and shortest path); (c): Energy consumption for primary and backup path (optimal and minimum-hop path)



(a) (b) (c)

Fig. 5. (a): Generated, received, dropped, and lost traffic vs. time (50 nodes); (b): Average and surface station used energy per received bit vs. time (50 nodes); (c): Packet delay and average delay vs. time (50 nodes)



(a) (b) (c)

Fig. 6. (a): No. of packets collided, duplicated, and corrupted (due to channel impairments) vs. time (50 nodes); (b): Queue and average queue size vs. time (50 nodes); (c): Expected routing energy increase due to sensor failure vs. time (50 nodes)

different failure rates are considered. The source block probability is defined as the probability that a source is able to transmit neither on the primary nor on the backup data path, since both have at least one failed node. While the source block probability increases with increasing observation time and failure rate λ, it only slightly depends on the weight w_2, which allows selecting w_2 based on energy considerations, irrespective of the required reliability. Figure 4(b) shows a comparison of the average number of hops of source-to-sink connections on primary and backup paths. Primary paths are shown to be longer (higher number of hops), and more energy efficient. Figure 4(c) compares our solution to primary and backup node-disjoint shortest weighted paths calculated with a hop-distance metric. While the number of hops of the paths calculated by our solution is doubled, the energy

consumption is lower than with a shortest-hop metric. The cross-over points in Figs. 4(b-c) occur when $w_2 = w_1 = 0.5$, i.e., when the primary and backup paths are equally weighted to compensate for high failure rates.

As far as the restoration phase in Section V-B is concerned, we implemented the whole protocol stack of a sensor node to simulate the underwater transmission loss, the transmission and propagation delays, the channel fading, and the physical layer characteristics of underwater receivers. The packet size was set to $500\ Byte$, and the initial node energy to $1000\ J$. All deployed sensors are desynchronized sources, with packet inter-arrival time equal to $60\ s$, which allows us to simulate a *low-intensity monitoring traffic* from the entire volume. Since the development of a new MAC for the underwater environment is left for future work, we adapted the behavior of IEEE 802.11, although we do not advocate this access scheme for this environment. Firstly, we removed the RTS/CTS handshaking, as it yields high delays in a low-bandwidth high-propagation delay environment. Secondly, we tuned all the parameters of IEEE 802.11 according to the physical layer characteristics. For example, while the *slot time* is set to $20\mu s$ for 802.11 DSSS (Direct Sequence Spread Spectrum), we found that a value of $0.18s$ is needed to allow devices a few hundred meters apart to share the underwater medium. We also set the values of the contention windows CW_{min} and CW_{max} [16] to 8 and 64, respectively, whereas in 802.11 DSSS they are set to 32 and 1024.

Figures 5 and 6 show the overall performance of the proposed algorithm, when sensor-sink primary and backup paths are set according to the first phase of our algorithm (Section V-A), and sensor failures are locally handled by the restoration algorithm (Section V-B). In particular, Fig. 5(a) reports the generated, received, dropped (due to queue overflows), and lost traffic (due to sensor failures), while Fig. 5(b) shows the time evolution of the energy per received bit used by the surface station and by an average node. Figure 5(c) depicts delay and average delay of packets reaching the surface station. The effect of the fast fading Rayleigh channel (coherence time set to $1\ s$), which models the heavy multipath UW channel, is captured in Fig. 6(a), which compares the number of corrupted packets due to channel impairments to the number of packet collisions and duplications (caused by lost ACKs). Finally, Fig. 6(b) depicts the average queue time evolution, while Fig. 6(c) quantifies the energy increase caused by the routing reconfigurations that are triggered by the algorithm restoration phase in order to face sensor failures occurring at unpredictable instants (vertical lines).

VII. Conclusions

The problem of data gathering in a three-dimensional underwater sensor network was investigated, by considering the interactions between the routing functions and the underwater acoustic physical channel. A resilient routing solution tailored for long-term critical monitoring missions was proposed. Its effectiveness in providing energy-efficient data paths and its robustness to sensor failures were evaluated by means of simulation.

Acknowledgments

This work was supported by the Office of Naval Research under contract N00014-02-1-0564.

References

[1] I. F. Akyildiz, D. Pompili, and T. Melodia, "Underwater Acoustic Sensor Networks: Research Challenges," *Ad Hoc Networks (Elsevier)*, vol. 3, no. 3, pp. 257–279, May 2005.

[2] M. Stojanovic, "Acoustic (Underwater) Communications," in *Encyclopedia of Telecommunications*, J. G. Proakis, Ed. John Wiley and Sons, 2003.

[3] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A Review of Routing Protocols for Mobile Ad Hoc Networks," *Journal of Ad Hoc Networks (Elsevier)*, vol. 2, pp. 1–22, Jan. 2004.

[4] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks," *Journal of Ad Hoc Networks (Elsevier)*, vol. 3, no. 3, pp. 325–349, May 2005.

[5] G. Xie and J. Gibson, "A Network Layer Protocol for UANs to Address Propagation Delay Induced Performance Limitations," in *Proc. of IEEE OCEANS'01*, vol. 4, Honolulu, HI, Nov. 2001, pp. 2087–2094.

[6] P. Xie, J.-H. Cui, and L. Lao, "VBF: Vector-Based Forwarding Protocol for Underwater Sensor Networks," UCONN CSE UbiNet-TR05-03," Technical Report, 2005.

[7] E. Sozer, M. Stojanovic, and J. Proakis, "Underwater Acoustic Networks," *IEEE Journal of Oceanic Engineering*, vol. 25, no. 1, pp. 72–83, Jan. 2000.

[8] I. Vasilescu, K. Kotay, D. Rus, M. Dunbabin, and P. Corke, "Data Collection, Storage, and Retrieval with an Underwater Sensor Network," in *Proc. of ACM SenSys'05*, San Diego, CA, USA, Nov. 2005.

[9] R. J. Urick, *Principles of Underwater Sound*. McGraw-Hill, 1983.

[10] L. Miller, "Distribution of Link Distances in a Wireless Network," *Journal of Research of the National Institute of Standards and Technology*, vol. 106, no. 2, pp. 401–412, Mar.-Apr. 2001.

[11] S. Ramamurthyt and B. Mukherjee, "Survivable WDM Mesh Networks, Part I - Protection," in *Proc. of IEEE INFOCOM'99*, vol. 2, New York, NY, USA, Mar. 1999, pp. 744–751.

[12] R. Ahuja, T. Magnanti, and J. Orlin, *Network Flows: Theory, Algorithms, and Applications*. Prentice Hall, Feb. 1993.

[13] M. Garey and D. Johnson, *Computer and Intractability*. W. H. Freeman and Co., 1979.

[14] R. Fourer, D. Gay, and B. Kernighan, *AMPL: A Modeling Language for Mathematical Programming*. Duxbury Press / Brooks/Cole Publishing Company, 2002.

[15] CPLEX solver, http://www.cplex.com. [Online]. Available: http://www.cplex.com

[16] G. Bianchi, "Performance Analysis of the IEEE 802.11 DCF," *IEEE Journal on Selected Areas of Communications (JSAC)*, vol. 18, no. 3, pp. 535–547, Mar. 2000.