Monitoring Underwater Pipelines Using Sensor Networks

Nader Mohamed, Imad Jawhar, Jameela Al-Jaroodi, and Liren Zhang
The Faculty of Information Technology, UAEU
Alain, P.O. Box 17551, UAE, {nader.m, ijawhar, j.aljaroodi, lzhang}@uaeu.ac.ae

Abstract – Sensor networks can be used to monitor and control pipeline infrastructures. This paper discusses and compares different sensor network architectures that can be used for monitoring underwater pipelines infrastructures. These architectures are underwater wired sensor networks, underwater acoustic wireless sensor networks, RF (Radio Frequency) wireless sensor networks, integrated wired/acoustic wireless sensor network, and integrated wired/RF wireless sensor networks. The reliability characteristics, advantages, and disadvantages among these architectures are discussed and compared. Three reliability factors are used for the discussion and comparison: the network connectivity, the continuity of power supply for the network, and the physical network security.


I. INTRODUCTION

There are several long underwater pipeline systems used for different applications around the world. One of the longest pipelines in use is the Langeled Pipeline that extends for 1200km from the Ormen Lange field in Norway to the Easington Gas Terminal in England under the North Sea used to transfer natural gas to England. This pipeline started operating in October 2007 and can carry 25.5 billion cubic meters per year and supplies around 20% of the natural gas demand in England. Another long pipeline is located between Qatar and UAE under the Arabian Gulf and owned by Dolphin Energy Limited of Abu Dhabi. It is used to transfer processed gas from Qatar’s offshore North field to the UAE. It extends for 367km through the Gulf and transfers a high percentage of UAE’s gas needs. In addition, pipelines are intensively used in the Gulf of Mexico to transfer oil. There are around 30,000 miles of underwater pipelines in the Gulf of Mexico.

The economic feasibility of using underwater pipelines for transferring gas, oil and water led many countries to plan for projects to build a number of new underwater pipeline infrastructures. Most existing and planned underwater pipeline projects are considered important infrastructures for economic stability and growth. Having a reliable monitoring and control system for these infrastructures can significantly help in inspecting and saving them. One of main approaches is sensor networks. This paper discusses and compares different sensor network architectures suitable for underwater pipeline infrastructure monitoring. The architectures are underwater wired sensor networks, underwater acoustic wireless sensor networks, RF wireless sensor networks, integrated wired/acoustic wireless sensor networks, and integrated wired/RF wireless sensor networks. Three reliability factors are used to compare the architectures in terms of network connectivity, continuity of power supply for the network, and the physical network security. In addition, the advantages and disadvantages of the architectures are discussed.

The rest of the paper is organized as follows: Section II provides some information on network reliability for monitoring pipelines. Section III discusses different sensor network architectures for monitoring pipelines. Section IV provides a discussion and compression of these architectures. Sections V and VI develop and evaluate a hierarchical sensor network design for monitoring underwater pipelines. Section VII discusses the related work while Section VIII concludes the paper.

II. NETWORK RELIABILITY

A network is usually needed on the pipelines to provide communication media for data acquisition, video monitoring, control, and command systems. There are usually numerous sensor points along any pipeline that provide data about the material flowing through the pipeline and the conditions of the pipelines. Data needs to be collected from these sensors and sent back to a control and monitoring center. Network components are usually spread along pipelines to transfer the measurements collected from distributed sensors scattered along pipelines.

One of the main differences between the networks used for pipelines and other networks is that the network needed for pipeline applications is structured in a line where all sensor and actor nodes are distributed on that line. This characteristic enforces some reliability challenges in monitoring pipeline infrastructures. The monitoring systems for pipelines will not be able to function properly unless the network connecting these sensors, actors, and control points functions without any problems. Having a reliable network is one of the main conditions of having a reliable monitoring system for pipelines.

Different network architectures are used or can be used for reliable communication in pipeline systems. These architectures are based on wired networks, wireless networks, or a combination of wired and wireless networks. These architectures are evaluated in this paper based on three reliability factors:

1. The connectivity of the network: since the pipeline network extends linearly, it is important for the network to be continuously connected to transfer information from the sensors distributed across the pipeline to the control station.

2. The continuity of power supply: pipeline networks will not be able to operate unless there is sufficient power supply.
available continuously. Power is needed not only to operate the network but also to operate the sensor nodes.

3. The physical network security: pipelines are usually considered important infrastructures. Devices or networks monitoring these infrastructures must be physically secured. Otherwise, the monitoring systems will fail easily and the pipelines will not be appropriately protected.

III. SENSOR NETWORK ARCHITECTURES

There are various sensor network architectures that can be used to monitor underwater pipelines. In this section, we discuss these architectures and show their advantages, disadvantages, and challenges.

A. Underwater Wired Sensor Networks

These days most pipeline sensors are connected using wired networks. Wired networks are either copper or fiber optic cables [1][2]. The wired networks are usually connected to regular sensor devices that measure specific attributes such as flow rate, pressure, temperature, sound, vibration, motion, and other important attributes, see Figure 1. The wires are not used for communication only but also to transfer electrical power to different parts of the pipeline system to enable the sensors, actors, and communication devices to function. Power for the pipeline resources and networks can be provided by different sources:

1. Pipeline Flow Energy: electric power can be generated using turbines embedded through the pipeline. These turbines rotate under the pressure of the fluid moving through the pipelines and generate electric power. This can be used for the different sensor and communication devices installed along the pipeline [3].

2. Other External Energy: power can be provided from external sources such as external gas-based power generators or third-party power generators. This power is transferred in wires to different communication and sensor devices along the pipeline.

   ![Wired Sensors](image)

   Figure 1. Underwater wired sensor network.

Wired networks are considered the traditional way for communication in pipeline systems. They are easy to install and provide power supply for through the network wires. However, there are a number of reliability problems related to using wired networks with regular sensors for monitoring pipelines:

- If there is any damage in any part of the wires of the network, the pipeline communication system will be completely or partially damaged. In addition, if there is a power outage, sensor nodes will not operate.

- It is easy for unauthorized people to disable the network simply by cutting some of the network wires.

   These problems make wired networks for pipeline communication systems undependable. Although, wired networks provide an easy solution for underwater pipeline monitoring and controlling, they face a number of major reliability and security problems. The main reason of these problems is the structure and type of networks used for pipelines. If any part of the wired network is disabled for any intentional or natural reason, the monitoring system can be partially or completely affected.

   One possible solution to enhance the reliability of a wired network is to use multiple networks that expand through the whole area. One of these networks will be used as primary while others are kept as backup. However, unlike other systems, using multiple wired networks and a fault tolerance mechanism among them will not enhance the reliability of the network. This is due to the fact that all wires will be expanded together along the pipelines and any damage occurring in one of them may also occur in the others. More specifically an accidental (or intentional) break in the line has a very high probability of happening to all wires.

B. Underwater Acoustic Wireless Sensor Networks

Acoustic sensor nodes can be installed with underwater pipeline infrastructures. Each node has a limited transmission capability in which each node can communicate with few neighboring nodes. Multi-hop communication is used to transfer the sensed information among the underwater pipeline.

Wireless networks can solve some of the reliability problems of current wired networks technologies in pipeline systems [4]. For example, wireless sensor networks can still function even when some nodes are disabled. Faults in sensor nodes can be easily tolerated by using other available nodes to cover the faulty ones. Using dense sensor networks with a high number of nodes and/or using wide acoustic transmission range, the network can maintain connectivity and the sensed information can be transported through the network to its destination even with the existence of some node failures. For example, each node in Figure 2 can communicate with two nodes to the left and two nodes to the right. If for example node 3 and 5 are damaged, node 4 can still send its sensed data through nodes 2 or 6.

   ![Reliability in dense sensor networks](image)

Each sensor node for monitoring pipelines is usually equipped with an acoustic transceiver, a processor, a battery, memory, and small storage in addition to one or more sensor devices. Power consumption is critical to the life span of pipeline...
communication systems. Pipeline systems are usually installed to be used for years. Therefore the associated communication systems should also be long lived. Unlike wired networks where the power is not a constraint in building the system, network designers have to consider power as one of the main constraints in the wireless system. Power in a node can be consumed when data is sent through the transceiver, when the transceiver is turned on waiting to receive data from other nodes, when sensor devices are turned on, and when the processor is active. Careful scheduling of these resources is needed to optimize power consumption.

Although increasing the range can provide better reliability, more energy will be consumed from the nodes. A dynamic configuration for the wireless transmission range can provide better power management. Example of this configuration is in Figure 3. In this network, nodes 3 and 5 are dead. Therefore, the wireless range for node 4 is increased to reach nodes 2 and 6 while other nodes use a smaller transmission range to reduce the power consumption.

![Figure 3. Automatic wireless/acoustic range configuration.](image)

In addition, nodes are used to route information from other nodes to the control station. As a result, nodes close to the station will consume more power than other nodes since they will route more packets. All nodes will have the same level of sensing activity; however, closer nodes to the station will consume more power due to more packet routings. One of the main issues for wireless/acoustic networks when used to monitor pipelines is the optimal design of a network protocol that balances the power consumption of batteries on the nodes with and without node failures. This balancing is crucial to extend the life of the network.

One approach to enhance the reliability of underwater acoustic sensor networks for pipelines is to divide the network into multiple parts. In each part, there is a surface buoy that is linked with one of the underwater sensor nodes through a wire as shown in Figure 4. Each surface buoy is equipped with a radio communication system to transfer collected information to the control station. The collected information can be transferred either directly through satellite communication links or using radio multi-hop communication among the available surface buoys. All acoustic sensor nodes need to transfer their sensed information to the nearest neighboring node linked to one of the surface buoys.

Generally, underwater acoustic networks suffer some major problems [5]. First, the available bandwidth is very limited among the nodes. The bandwidth of underwater acoustic channels depends on both the distance and frequency [6]. Communication among nodes located within the range of a few tens of kilometers may have a bandwidth of only a few kHz. The bandwidth can be increased to a hundred kHz, if the nodes involved are located closer (i.e. within several tens of meters). Second, propagation delay of acoustic signals underwater is very high and variable [7]. It is around five orders of magnitude higher than that in radio frequency channels. Third, due to the characteristics of the underwater channel, high bit error rates and connectivity losses can be encountered. Fourth, battery power is consumed and it is difficult to renew or replace. In addition to the power needed to operate the nodes and their transceivers, in underwater communication advanced signal processing techniques are needed to reduce the impact of underwater communication characteristics; however, these signal processing techniques will consume more power and will reduce the life of the nodes’ batteries.

![Figure 4. Underwater acoustic sensor network.](image)

C. RF Wireless Sensor Networks

Another architecture that can be used for monitoring underwater pipelines is wireless sensor networks that use radio frequency. The main differences between this architecture and other wireless sensor networks used for above ground applications is that each sensor node is connected to a surface buoy through a cable. On the surface buoys, radio transceivers are available. As a result, the nodes can communicate through radio frequency channels which provide better communication bandwidth, propagation delay, bit error rate and connectivity, as well as less power consumption for processing communication signals compared to the underwater acoustic wireless sensor network. In addition, surface buoys can be equipped with solar cells to provide energy for the sensors and communication devices.

Although this architecture has many advantages over the acoustic wireless sensor network, it has two major physical security problems. First, the floating buoys and their cables may be damaged by passing ships. In addition, the locations of the floating buoys are a good indication for the location of the pipeline. Therefore, the pipeline can be easily discovered and sabotaged.

D. Integrated Wired/Acoustic Wireless Sensor Networks

As we can see from the previous sections the main reliability challenges in pipeline sensor networks communication systems are network connectivity, continuity of power supply, and physical security of the network. To solve all these issues, we are proposing in this section new network architecture for underwater pipeline communication systems. The architecture in
this system consists of multiple point-to-point segments as shown in Figure 5. These segments link the system nodes.

Each node is connected to a acoustic transceiver and a wired network interface. Sensor nodes also consist of processor, memory and storage units. The nodes are connected through wireless acoustic and wired links. Wires are used for networking and for transferring power to the nodes. Unlike completely wireless nodes in the wireless or underwater acoustic wireless sensor network architectures, nodes in this architecture have rechargeable batteries which are charged by the received power through the connected wires. The power can be provided for this network architecture using the techniques used for wired network architecture as discussed in subsection III.A.

Neighborhood nodes can communicate either using wired or acoustic communication. The transceivers in the normal case are turned off and the wired network is used for communication. Therefore the connectivity of the network is through the wired links in the normal case. Each node periodically checks the status of the right side of the network wire by sending echo messages to the neighboring nodes on the right. Each node also periodically checks the status of the left side network wire by receiving/replying to the echo messages received from the neighboring node on the left. A break of a wired link between two nodes can be discovered by the left node when it does not receive replies for the echo messages it just sent. The break can be discovered by the right node if there are no echo messages received from the left node. When both nodes discover the break, they will activate their transceivers and communicate through the acoustic link. This wireless acoustic link between the two nodes can provide connectivity for the pipeline network and sensed information can be still transported through the network as shown in Figure 5. The nodes that discovered the break will report it along with the location information to the control station for immediate maintenance. If an intermediate node is disconnected from the left and from the right, the node can operate temporarily using the rechargeable battery until the wire breaks are fixed.

Link breaks due to faulty nodes can be recovered by using a wider transmission range in which each node can communicate using the wireless links with multiple nodes on the left and multiple nodes on the right as discussed in subsection III.B. Discovered faulty nodes can be also directly reported to the control station. The network connectivity will remain even with multiple breaks on multiple segments occurring while any node faults or wire breaks will be discovered and reported for maintenance. In addition, with the availability of rechargeable batteries, the power constraint issue is terminated.

One of the main disadvantages of this architecture is that with a single wire cut, the overall bandwidth of the network will drop to the bandwidth of the replacement acoustic communication channel. However, unlike with the wired sensor network solution, the communication bandwidth will not drop to zero. The limited available bandwidth can be used to report the position of the faults as well as other critical information until the damage is fixed.

E. Integrated Wired/Wireless Sensor Networks

To enhance the communication of the architecture described in subsection III.D, radio frequency channels can be used instead of acoustic communication channels as shown in Figure 6. In this architecture, a buoy equipped with a radio transceiver is released when there is a cut or fault in the wire connecting a pair of nodes as shown in Figure 6. The buoys are attached to the nodes and they only float on the surface if there is a need for them. The transceivers on the floating buoys are activated to provide communication and connectivity among them thus replacing the broken link underwater.

![Figure 6. Integrated wired/RF wireless sensor network.](image)

This architecture is very similar to the one discussed in the previous subsection; however, it can provide better communication as radio frequency channels are used instead of the acoustic channels that have lower network properties. This architecture provides better physical security protection than the RF wireless sensor network architecture described in subsection III.C as the buoys will not appear unless there is a problem with the wired connections. In addition, only sparse pairs of buoys will be deployed at a time thus they will not reveal the full location or spread of the pipelines.

IV. DISCUSSION

The sensor network architectures for monitoring underwater pipeline mentioned in this paper provide different advantages for different objectives and requirements. Wired sensor networks usually provide higher communication bandwidth than wireless sensor networks and underwater acoustic sensor networks. Hence wired networks can be used for pipeline monitoring applications that demand high bandwidth such as camera-based monitoring.

On the other hand, wireless/acoustic networks provide better reliability for pipeline monitoring applications such as sudden damages detection. These applications are event based applications that do not need high communication bandwidth. Events occur only if there are exceptions discovered by the
sensors which they need to communicate. The integrated wired/RF wireless network and integrated wired/acoustic wireless network architectures can provide reasonable bandwidth as well as good reliability for event-based applications even if some parts of the network are damaged.

The network architectures mentioned in this paper also have different degrees of reliability. The wired network may completely fail with a single point failure. On the other end, using wide transmission ranges in wireless and underwater acoustic networks can solve the problem of a full network failure due to failure of one or more nodes. The reliability degree of the wireless network can be increased as we increase the transmission range. However, this increase of the wireless transmission range causes a significant increase in power consumption. Therefore, the battery will be consumed rapidly and the life of the network will be reduced significantly. In the integrated wired/wireless networks, the limitation of power sources is not an issue. Therefore, the node can be designed to use a wide transmission range for communication to provide better reliability. The node batteries will be used only if there is a fault in the wires providing power to the nodes. Unlike wireless sensor networks, if there is no cut for some period, the batteries will be fully charged during that period. As a result nodes will have better chance to have power supply in integrated wired/wireless sensor networks than wireless sensor networks. A summary of the reliability issues for all discussed architectures is in Table 1.

<table>
<thead>
<tr>
<th>#</th>
<th>Architecture</th>
<th>BW</th>
<th>BWF</th>
<th>EC</th>
<th>PSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Underwater wired network</td>
<td>High</td>
<td>0</td>
<td>No</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>Underwater acoustic network</td>
<td>Low</td>
<td>Low</td>
<td>Yes</td>
<td>Low</td>
</tr>
<tr>
<td>3</td>
<td>Wireless sensor network</td>
<td>Med</td>
<td>Med</td>
<td>Yes</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Integrated wired/acoustic network</td>
<td>High</td>
<td>Low</td>
<td>No</td>
<td>Low</td>
</tr>
<tr>
<td>5</td>
<td>Integrated wired/RF network</td>
<td>High</td>
<td>Med</td>
<td>No</td>
<td>Low</td>
</tr>
</tbody>
</table>

BW: Bandwidth, BWF: Bandwidth with fault condition, EC: Energy constraints, PSC: Physical security concern

V. HIERARCHICAL SENSOR NETWORK DESIGN

Although this paper provides several new architectures for underwater pipeline monitoring, it is noted that these architectures follow the linear sensor network model which we previously introduced in [8]. This general model can be adapted for the various categories of networks that were introduced. In this section, a brief description of this model is presented, and in a later section, simulation experiments performed to evaluate the performance of a specific implementation of this model will be offered. One of the important aspects of this hierarchical structure is its ability to take advantage of the linear structure to improve the reliability and robustness of the network in reaction to node failures. Even though the failures can have various causes, including intentional physical attacks, equipment failures, battery depletion (in case of battery-powered nodes), the network and corresponding message routing protocols are able to react quickly, autonomously, and efficiently to overcome the failures. In the above model, the following three types of nodes are defined. Each of these types of nodes has different functions to perform in the data collection, routing and final dissemination to the Network Control Center (NCC).

- **Basic Sensor Nodes (BSNs):** These are the most common nodes in the network. Their objective is to perform the sensing function and communicate this information to the data relay nodes.
- **Data Relay Nodes (DRNs):** These nodes serve as information collection nodes for the data gathered by the sensor nodes in their one-hop neighborhood. They also play a role in routing the data to the control center. The distance between these nodes is determined by the communication range of the MAC protocol used.
- **Data Discharge Nodes (DDNs):** These nodes perform the function of delivering the collected data to the NCC. The technology used to transfer data from these nodes to the NCC center can vary. For example, satellite cellular technology can be used. This implies that each of the DDN nodes would have such communication capability.

The DDNs provide the network with increased reliability since the collected sensor data would not have to travel all the way along the length of the pipeline from the sensing source to the NCC center. This distance is usually very long and can be hundreds of kilometers which would make it vulnerable to a large number of possible failures, unacceptable delay, higher probability of errors, and potential security attacks. The DDNs allow the network to pass on its sensor data simultaneously in a parallel fashion. Additionally, the distance between the DDNs is important and affects the reliability of the network. A small distance between the DDNs would increase the equipment cost of the network, as well as deployment and maintenance costs. On the other hand, a distance that is too large would decrease the reliability, security, and performance of the network. Figure 7 shows a graphic representation of the different types of nodes and their geographic layout.

A hierarchical relationship exists between the various types of nodes in the sensor network. Multiple BSNs transmit their data to the nearest DRN. In turn, several DRNs transmit their data using a multi-hop strategy through the intermediate DRNs to the nearest DDN node. Finally, all DDNs transmit their data to the Network Control Center. BSNs, DRNs, and DDNs can be completely wireless nodes that are equipped with batteries and used for underwater acoustic wireless sensor network or RF wireless sensor network architectures. BSNs, DRNs, and DDNs can be wired/wireless nodes and used for integrated wired/acoustic wireless sensor network and integrated wired/RF wireless sensor network architectures. In this case, the nodes will be equipped with rechargeable batteries that can be recharged from the wire. In addition, the wireless communication will be used only if there are some broken wires. In normal condition, the wire will be used for communication. In all cases, nodes can
be connected to buoys on the sea surface for RF wireless communication.

The hierarchical model described in this section can be used to represent any one of the various architectures presented earlier. For example, the underwater nodes belonging to the underwater acoustic sensor network presented in Figure 4 can be considered DRNs, and the surface buoy nodes can be considered DDNs. In addition, each of the DRNs can collect the information to be relayed along the pipeline from multiple BSNs that are local to it. On the other hand, the RF wireless sensor network can be considered as consisting of DRNs that relay the information among each other until a designated node transmits the collected information to the control center. Similar modeling can be done for the other presented architectures.

It is important to state that the classic routing protocols for wireless networks such as DSR and AODV are not used in this model due to the fact that they are designed for multi-dimensional topologies and do not take advantage of the linear structure that is assumed. For example DSR and AODV both use flooding from the source in order to discover paths to the destination, while this is not necessary in our case once the network is initialized and the tree structure is created. Also, DSR and AODV would have to deal with node failures by re-initiating path discovery from the source, and do not have provisioning to increase a node’s range in order to overcome failures in an efficient manner. They also do not inherently have the concept of having two alternate destinations in opposite directions, a characteristic which can also be exploited in order to increase network performance, reliability, and robustness in reaction to node failures. In addition, plain shortest path algorithms are not best suited for this environment either for similar reasons such as the lack of features to increase node range, or choose alternative destinations or sink nodes in response to changes in intermediate node states.

In order to still be able to transmit its DRN data successfully despite the lack of connectivity to its immediate neighbor, the DRN can increase its transmission power and double its range in order to reach the DRN that follows the current one. If multiple consecutive links are lost, then the DRN can increase its transmission range appropriately in order to bypass the broken links. This process can happen until the transmission power is maximal. If even with maximal transmission power the broken links cannot be bypassed, then the message is dropped. This maximal DRN transmission power is represented by a variable named MAX_JUMP_FACTOR which holds the maximum number of broken links or “disabled nodes” that a DRN transmission can bypass. Two strategies for using multi-hop routing of data messages through the DRNs to reach the nearest DDN can be used. The two algorithms deal differently with the failure of a next-hop DRN.

**Redirect Always Algorithm (RA):** In this variation of the routing protocol, the DRN source node sends its DRN data message to its parent DDN. While the message is being forwarded through the intermediate DRNs, if it reaches a broken link then the following steps are taken. The DRN determines if this data message has already been redirected. This is determined by checking the redirected flag that resides in the message. If the redirected flag is already set then the message is dropped and a negative acknowledgement is sent back to the source. Otherwise, the source can be informed of the redirection process by sending a short redirection message with the redirected message ID back to the source. The source will then re-send the data message in the opposite direction and update its database with the fact that this direction to reach the DDN is not functional. Furthermore, in order to make the protocol more efficient the entire data message is not sent back to the source since the source already has a copy of the data message. Only a short redirection message with the redirected message ID is sufficient to be sent back to the source.

Additionally, the redirection message also informs the other nodes on that side that there is a “dead end” in this direction and data needs to be transmitted in the other direction even if the number of hops to reach the other nearest DRN is larger. In that case, each DRN that receives this message will check the redirected flag, and if it is set, then it will continue to forward the message in the same direction. However, in order to prevent looping, if another broken link is encountered in the opposite direction the redirected message cannot be redirected again. In that case, the message is simply dropped.

**Smart Redirect or Jump Algorithm (SRJ):** This algorithm overcomes DRN failures by using a combination of the jumping and redirection strategies described in the previous sections. We define as sibling DRNs to a particular DRN \( x \), the DRNs that have the same parent DDN as \( x \). We also define as secondary sibling DRNs to \( x \) the DRNs that have as parent DDN the secondary parent DDN (i.e. the DDN that is on the opposite side of the parent DDN with respect to \( x \)) of \( x \). In this algorithm, each node contains information about the operational status of its sibling and secondary sibling DRNs. Consequently, before dispatching the message, it calculates the total necessary energy it needs to reach its parent DDN \( E_{s,p} \) and the total energy it needs to reach its secondary parent \( E_{s,sp} \). It then dispatches the message in the direction which takes the lower total energy to reach either the parent DDN or the secondary parent DDN. Specifically, if \( E_{s,p} \leq E_{s,sp} \) then the message is sent towards the parent DDN. Otherwise, the message is sent towards the secondary parent DDN. This algorithm relies on the information in the node to reduce the total energy consumed by the network for the transmission of the message. This information about failure status of DRNs is cached by the DRNs from participations in previous packet transmissions. More research is being conducted for the most efficient means of gathering such information by the DRNs.

**VI. PERFORMANCE EVALUATIONS**

Simulation experiments were performed to verify the correctness of operations, and evaluate the performance of the proposed framework and network protocol. In this paper, we consider the network presented in Figure 4 as a case study. The simulator is event-driven and it was written using Java. It places all the nodes in a linear formation, and simulates the communication and routing processes as described in the paper. The main focus of the experiments was to validate and evaluate the design and inter-workings of the proposed model. As indicated in Table 2, the number of DDN nodes used in the simulation is 10, the number of DRN nodes per DDN node was varied between 50 and 100. The number of BSN nodes per DRN node is 6. DRN nodes communicate using a data rate of 4800
bps. Depending on the transmission range of the nodes, this number of nodes covers an area of tens of kilometers while the network can cover longer stretches of pipelines. However, since the hierarchical network consists of segments which are separated by the DDN nodes, the simulation of several segments of the network is relatively sufficient to reflect the performance of the entire system. This is because the data is only multi-hopped through the DRN nodes to the nearest DDN node. The data is then transmitted by the various DDN nodes to the control center in parallel. In the simulation, the BSN nodes send their sensed data to their parent DRN node in a periodic manner. The sensing period that was used in the simulation is 10 seconds. This value may be varied depending on the requirements of the application used and the type of parameters sensed. After collecting the information from the BSN nodes, the DRN nodes use the networking protocol to route this information to their parent DRN node. The DRN data packet size was set to 512 bytes, which is a common size and it is sufficient to include the sensed information. For the SRJ algorithm the MAX_JUMP_FACTOR is set to 3. To verify and test our RA, and SRJ routing protocols and their ability to route the generated packets correctly to the DDN nodes using intermediate DRN nodes, a number of DRN failures have been intentionally generated using the Poisson arrival distribution with certain average arrival rate. The average arrival rate of the DRN failures was varied to evaluate the capability of the routing protocol to overcome intermediate DDN node failures.

Table 2. Case study simulation parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of DDNs</td>
<td>10</td>
</tr>
<tr>
<td>Total Number of DRNs Per DDN</td>
<td>50, 100</td>
</tr>
<tr>
<td>Total Number of BSNs Per DRN</td>
<td>6</td>
</tr>
<tr>
<td>Periodic Sensing Interval</td>
<td>10 seconds</td>
</tr>
<tr>
<td>Data transmission rate</td>
<td>4800 bps</td>
</tr>
<tr>
<td>DRN Data Packet Size</td>
<td>1200 bytes</td>
</tr>
<tr>
<td>MAX JUMP FACTOR</td>
<td>3</td>
</tr>
</tbody>
</table>

The results are presented in the Figures 8 and 9. As DRNs fail, routing of the DRN packets to either the parent DDN or the alternative one in the opposite direction is done. In Figures 8 and 9, the number of DRNs per DDN was varied in order to study the impact of increasing the number of DRNs per DDN on network performance. The percentage of successfully transmitted packets was measured as the DRN percentage failure rate (percentage of DRNs failures per month) was varied. As can be seen in the two figures the percentage of successfully transmitted packets decreases as the percentage of DRN failures increases. This is consistent with the expected and logical behavior of the system and can further be used to validate the simulation. Also, it can be clearly seen that the SRJ algorithm provides the better performance compared to the RA algorithm respectively. This is expected since the RA algorithm does not try to jump over a failed DRN, and only tries redirecting the packet once. If it encounters another failed DRN in the opposite direction then the packet is dropped. The SRJ algorithm offers a better performance since it considers both directions and dispatches the packet only in the direction with the smallest required energy. In addition to providing more alternatives for overcoming failed DRNs, the SRJ algorithm also ensures a smaller number of DRN failures due to battery depletion which increases network lifetime and improves its performance.

Additionally, the results show that as the number of DRNs per DDN increases from 50 to 100, the percentage of successfully transmitted packets decreases for both algorithms. For example, for the SRJ algorithm case, with a percentage failure rate of 4 percent failures per month, the percentage of successfully transmitted packets decreases from 90.18 for DRN_PER_DDN = 50 to 48.26 for DRN_PER_DDN = 100. This decrease in performance as the number of DRNs per DDN increases is expected due to the linear structure of the network. With the increased number of DRNs that a packet has to use to reach the DDN, the probability of encountering a more than maximum number of consecutive failed DRNs, which prevents it from going further increases. When designing such a network, the number of DRNs per DDN must not be too large in order to ensure good network performance. Consequently, the choice of the number of DRN per DDN nodes is an important parameter which is affected by the communication range of the protocol used, as well as the desired quality of service (QoS) such as end-to-end delay, bandwidth, and throughput. For example, real-time, audio/video monitoring would have more stringent QoS requirements. This also depends on the application, the particular type of pipeline and the desired monitoring specifications.

![Figure 8](image.png)  
Figure 8. Simulation results for the hierarchical underwater pipeline model. Percentage of successfully transmitted packets. NUM_DRN_PER_DDN=50.

![Figure 9](image.png)  
Figure 9. Simulation results for the hierarchical underwater pipeline model. Percentage of successfully transmitted packets. NUM_DRN_PER_DDN=100.
VII. RELATED WORK

There are a number of technologies to monitor, maintain, and protect pipelines. Examples of these technologies are sensors, mobile robots, algorithms [9][10][11][12]. Most of these technologies are designed specifically for detecting and locating pipeline leaks [13], corrosions, and damages. These technologies were designed to provide a remote facility to detect and to report the positions of any defect. Some of these available solutions rely on the availability of a network to transfer the information and report the defects or any important sensed information [14]. These networks are usually wired such using copper or fiber optic cables [1][2]. There are some efforts to develop wireless sensor network based algorithms to detect defects. One example is PipeNet [15]. PipeNet is a wireless sensor network for monitoring large diameter bulk-water transmission pipelines. The network collects hydraulic and acoustic/vibration data at high-sampling rates. Algorithms for analyzing the collected data to detect and locate leaks were developed. In addition, a general framework using acoustic sensor networks to provide continuous monitoring and inspection of pipeline defects was developed [16]. In this framework sensor networks can detect, localize, and quantify bursts, leaks, and other anomalies in pipelines. Acoustic wave propagation theory, distributed control, and statistical signal processing are used to analyze signals for defects detection and localization. In another project, a wireless sensor network for a team of collaborative autonomous agents has been developed [17]. This system was developed to locate and repair scale formations in tanks and pipeline within inaccessible areas such as underwater environments.

We have previously developed a framework and protocols for monitoring above-ground long pipelines using wireless sensor networks [4]. In addition, we have developed a fault-tolerant wired/wireless sensor network architecture for monitoring above-ground pipeline infrastructures [18]. Although several of the mentioned projects are based on different network technologies, none of them studied the design of sensor networks for monitoring long underwater pipelines.

VIII. CONCLUSION

The reliability issues of five sensor network architectures for monitoring long underwater pipelines were discussed in this paper. These architectures are underwater wired sensor networks, underwater acoustic wireless sensor networks, RF wireless sensor networks, integrated wired/acoustic wireless sensor network, and integrated wired/RF wireless sensor networks. Each architecture has its own advantages and disadvantages in terms of reliability. However, integrated wired/wireless networks can provide better reliability in terms of network connectivity, continuity of power supply, and physical network security. These architectures are new and require new technologies to develop and implement them. Therefore, they can be costly. As future work we plan to design, analyze and evaluate in details the integrated wired/wireless sensor network architectures for monitoring long underwater pipelines. In addition, we plan to develop reliability analytical models for the discussed architectures.