A Routing Protocol and Addressing Scheme for Oil, Gas, and Water Pipeline Monitoring Using Wireless Sensor Networks

Imad Jawhar, Nader Mohamed, Mohamed M. Mohamed, and Junaid Aziz
United Arab Emirates University
P.O. Box 17551. Al Ain, UAE
Phone: +971-3-7135532, Fax: +971-3-7672018
E-mail: {ijawhar, nader.m, m.mohamed, mjunaid}@uaeu.ac.ae

Abstract—Wireless sensor networks have a vast amount of applications including environmental monitoring, military, ecology, agriculture, inventory control, robotics and health care. This paper focuses on the area of monitoring, and protection of oil, gas, and water pipelines using wireless sensor networks. ROLS: a ROuting protocol for Linear Structure wireless sensor networks is presented along with a new hierarchical addressing scheme for this type of networking environment. The networking framework and associated protocols are optimized to take advantage of the linear nature of the network to decrease installation, and maintenance cost, decrease energy requirements, increase reliability and improve communication efficiency. In addition, simulation experiments using the proposed model are presented.

Keywords: Ad hoc and sensor networks, routing, addressing schemes, wireless networks.

I. INTRODUCTION

Research in the field of Wireless Sensor Networks is relatively active and involves a number of issues that are being investigated. These issues are efficient routing protocols for ad hoc and wireless sensor networks [9], quality of service (QoS) support [8] [10], security [3], and middleware [5]. Most of these issues are investigated under the assumption that the network used for sensors does not have a predetermined infrastructure. Fortunately, the wireless sensor network needed for pipeline applications will be a structured network in which all sensor nodes will be distributed in a line. This characteristic can be utilized for enhancing the communication quality and reliability in the pipeline systems.

This paper addresses the issues and challenges of using wireless sensor networks for monitoring and protection of oil, gas and water pipeline infrastructures. Also, it presents a routing protocol and addressing scheme for this special kind of sensor networks. This architecture utilizes the special linear structure of the networks to solve some of communication reliability and security problems. The objective of the design is to reduce installation and maintenance costs, increase network reliability and fault tolerance, increase battery life for wireless sensors, reduce end-to-end communication delay for QoS sensitive data, and increase network lifetime by utilizing the special linear structure of the network.

The paper in [7] presents a framework for using wireless sensor networks for oil, gas, and water pipeline monitoring. This paper extends the model and architecture discussed in [7]. More details on the background, motivation, advantages, and applications for using linear structure wireless sensor networks can be found in that paper.

The rest of this paper is organized as follows. Section II discusses the different types of pipelines. Section III presents the networking model overview and hierarchy. Section IV presents the node addressing scheme and routing protocols. Section V presents the simulation and analysis of results. The conclusions and future research are presented in the last section.

II. TYPES OF PIPELINES

In this paper, the designed framework will be general and can be applied to any types of pipelines with some adaptations to the particular needs and requirements of that type. This section presents the different types of pipelines that can benefit from the application of the framework. [1][2][4][6][11][12].

A. Sub-sea pipeline

The ability to monitor flow and pressure build-ups of the multiple phase mixture (oil, gases, brine) through a pipeline in real-time is critical for the safe and efficient transport of fluids. Because pipelines may span many kilometers along the sea bed, normal maintenance procedures at depths of up to 10,000 feet are costly both in time and resources. Failures due to corrosion could cause release of oil and gas, which negatively impacts the environment, causes loss of production, and presented a significant safety hazard.

The ability to remotely measure pressure along the entire pipeline is important in the oil and gas industry for the following reasons:

1) Flow problems can be identified more quickly to avoid plugging and catastrophic failure.
2) Maintenance strategy on production wells and pipelines can be shifted from schedule-based to condition-based, resulting in dramatic improvements in efficiency.
3) Hydrocarbon delivery can be maximized.

This work was supported in part by UAEU Research grant 08-03-9-11/07.
III. NETWORKING MODEL OVERVIEW AND HIERARCHY

In this section, the architectural model of the sensor network is presented. Even though an overview of the model is presented, more details about it can be found in [7]. In addition, the routing protocol that is used to collect, and route sensor data from the sensing nodes to the data collection, dissemination, and base station nodes is discussed.

A. Node hierarchy

In the hierarchical model used, three types of nodes are defined:

- **Basic Sensor Nodes (BSN):** These are the most common nodes in the network. Their function is to perform the sensing function and communicate this information to the data relay nodes.
- **Data Relay Nodes (DRN):** These nodes serve as information collection nodes for the data gathered by the sensor nodes in their one-hop neighborhood. The distance between these nodes is determined by the communication range of the networking MAC protocol used.
- **Data Discharge Nodes (DDN):** These nodes perform the function of discharging the collected data to the Network Control Center (NCC). The technology used to communication the data from these nodes to the NCC center can vary. Satellite cellular technology can be used for example. This implies that each of the DDN nodes would have this communication capability. These nodes are less frequent than the DRN nodes. Each c DRN nodes report to one DDN node.

Figure 1 shows the hierarchical relationship between the various types of nodes in the sensor network. As shown in the figure, multiple BSN nodes transmit their data to one DRN node. In turn, several DRN nodes transmit their data to a DDN node. Finally, all DSN nodes transmit their data to the network control center. Figure 2 shows a graphic representation of the different types of nodes and their geographic layout. The figure also shows an example illustrating the addressing scheme used. More about the addressing scheme is discussed later in the paper.

IV. NODE ADDRESSING SCHEME AND ROUTING PROTOCOLS

In order to facility routing, a multi-layer addressing scheme is used. The following section describes the address assignment process.

A. Multi-Layer Addressing

The logical address of each node consists of three fields. Hexadecimal or dotted decimal notation can be used for these fields. The order of the fields is: DDN.DRN.BSN.

- **DDN address field:** If this is a BSN or a DRN node, then this field holds the address of its parent DDN node. Otherwise, if this is a DDN node this holds its own address.
- **DRN address filed:** If this is a BSN node, then this node holds the address of its parent DRN node. If this is a DRN node, then this field holds its own address. If this is a DDN node then this field is empty (i.e. holds a code representing the empty symbol, φ).
- **BSN address filed:** If this is a BSN node, then this node holds its own address. It this is a DRN or DDN node then this field is empty.

A typical full address for a BSN node would be: 23.45.19. This means that its own BSN id is 19, its parent DRN node id is 45 and its parent DDN node id is 23. A typical full address for a DRN node is: 23.45.φ. The empty symbol in the BSN field alone indicates that this is a DRN node. Finally, a
Fig. 2. Illustration of the addressing scheme used to assign DDN, DRN, and BSN address field values.

A typical full address for a DDN node is: 23.φ.φ.φ. The two empty symbols in both the BSN and DRN fields indicate that this is a DDN node.

**B. Address Assignment**

In this section, the process of assigning values to the different fields of the address of each node is described. Figure 2 shows an example linear alignment of DDN, DRN, and BSN nodes with the corresponding addresses for each node. In the figure, the number of DDN nodes is 10. Therefore the address range of the DDN nodes is from 0 to 9. For illustrative purposes, the figure only shows a network segment with two DDN nodes, nodes 2 and 3. The number of DRN nodes per DDN node is 4, with an address range of the DRN nodes from 0 to 3. The number of BSN nodes per DRN node is 6 with an address range of the BSN nodes of 0 to 5. In reality the numbers of DDN, DRN, and BSN nodes can be much larger depending on the network needs for reliability, accuracy of measurements, as well as other factors. Also, for simplicity, the full address of each node is not shown in the figure. Only the changing address field for each set of nodes is shown. The address in each field is assigned in the following manner:

- **DDN address field assignment**: The DDN nodes have an address field starting at 0, 1, and so on up to (NUM OF DDN - 1).

- **DRN address field assignment**: Each DRN node has as its parent the closest DDN node. This means that the set of DRN nodes belonging to a particular DDN node are located around it with the DDN node being at their center. The address fields of the DRN nodes on the left of the DDN node are assigned starting from 0, at the farthest left node, to (NUM DRN PER DDN/2 - 1), where NUM DRN PER DDN is the number of DRN nodes per DDN node. The address fields of the DRN nodes on the right start from (NUM DRN PER DDN/2) to (NUM DRN PER DDN - 1). Figure 2 illustrates this assignment process as well, where NUM DRN PER DDN = 6. The address fields of the BSN nodes on the left of each DRN node are from 0 to 2, and the address fields of the BSN nodes on the right are from 3 to 5. The address fields of the BSN nodes to the right of BSN node 5 start again from 0, because they now belong to the next DRN node, and so on.

- **BSN address field assignment**: The BSN addressing field assignment is similar to that of the DRNs with the DRN node being that parent in this case. Each BSN node has as its parent the closest DRN node. This means that the set of BSN nodes belonging to a particular DRN node are located around it with the DRN node being at their center. The address fields of the BSN nodes on the left of the DRN node are assigned starting from 0, at the farthest left node, to (NUM BSN PER DRN/2 - 1), where NUM BSN PER DRN is the number of BSN nodes per DRN node. The address fields of the BSN nodes on the right start from (NUM BSN PER DRN/2) to (NUM BSN PER DRN - 1). Figure 2 illustrates this assignment process as well, where NUM BSN PER DRN = 6. The address fields of the BSN nodes on the left of each DRN node are from 0 to 2, and the address fields of the BSN nodes on the right are from 3 to 5. The address fields of the BSN nodes to the right of BSN node 5 start again from 0, because they now belong to the next DRN node, and so on.

**C. Communication from BSN to DRN nodes**

As mentioned earlier each BSN node is within range of at least one DRN node. The BSN node will sign up with the closest DRN node. Subsequently, the BSN nodes transmit their information to the DRN node periodically. They also can be polled by the DRN node when the corresponding command is issued from the command center.

**D. Communication from DRN to DDN Nodes**

Communication between the DRN and DDN nodes is done using a multi-hop routing algorithm which functions on top of a MAC protocol such as Zigbee. In this paper two different routing protocols for multihop communication among the DRN nodes are presented. These protocol are discussed later in this section.

**E. Information discharge at DDN nodes**

Collected data at the DDN nodes can be transmitted to the NCC center using different communication technologies. This implies that different DDN nodes would have different communication capabilities to transmit their collected information.
to the NCC center, depending on their location. For example nodes that are located within cities can send their information via available cellular GSM, or GPRS networks. On the other hand, nodes which are located in remote locations far from larger metropolitan areas might not be able to use standard cellular communication and would have to rely on the more expensive satellite cellular communication for transmission of their data. Another alternative would be to deploy WiMax or other long range wireless network access points at each 30 Km of the designated area along the pipeline.

F. The routing algorithm at the source and intermediate DRN nodes

When the DRN node is ready to send the data collected from its child-BSN nodes, it uses a multi-hop approach through its neighbor DRN node to reach its parent DDN node. Normally, this parent DDN node is the closest one to it. The multihop algorithm uses the addressing scheme presented earlier in order to route the DRN packet correctly. Each DRN node keeps track of its connectivity to its neighbors through the periodic broadcast of hello messages among the DRN nodes. If the connection with the next hop is not available then the DRN node can execute one of two algorithms to overcome this problem.

Jump Always (JA) Algorithm:

In order to still be able to transmit its DRN data successfully despite the lack of connectivity to its immediate neighbor, the DRN node can increase its transmission power and double its range in order to reach the DRN node that follows the current one. If multiple consecutive links are lost, then the DRN node 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. In the protocol, this maximal DRN transmission power is represented by a network variable named MAX_TX_FACTOR which holds the maximum number of broken links or “disabled nodes” that a DRN transmission can bypass.

Redirect Always (RA) Algorithm:

In this variation of the routing protocol, the DRN source node sends its DRN data message to its parent DDN node. While the message is being forwarded through the intermediate DRN nodes, if it reaches a broken link then the following steps are taken. The DRN node 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 be 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 node is not functional.
successful transmitted packets increases from 33.36 with success and is only needed with a higher number of failures. To jump over more DRN nodes improves the probability of near the higher range of DRN failure rates since the ability transmitted DRN packets increases as well. This takes place is increased from 3, to 5, the percentage of successfully algorithm. Additionally, it is noted that as MAX node. This situation is not possible to overcome using the RA algorithm. Also the JA algorithm can overcome a situation where there due to the fact that the JA algorithm can overcome multiple to overcome intermediate DDN node failures. As DRN nodes fail, routing of the DRN packets to either the parent DDN node or the alternative one in the opposite direction is done. When a DRN node fails, the two routing protocols react differently to overcome the failures as specified earlier in the paper. In this simulation, we are focusing on testing the correctness of the protocols. In cases for both routing protocols, as more and more DRN nodes fail, the percentage of successfully transmitted packets decreases. The simulation results are presented in Figures 3, 4, and 5. In the figures the maximal transmission jump factor (MAX_TX_FACTOR) which corresponds to the maximum number of adjacent disabled DRN nodes that can be bypassed by a DRN transmission is varied. Namely, it is set to 3 in 3, 4 in 4, and 5 in 5. The results show that the JA algorithm outperforms the RA algorithm with respect to the percentage of successfully transmitted packets. This is due to the fact that the JA algorithm can overcome multiple adjacent disabled DRN nodes while the RA algorithm cannot. Also the JA algorithm can overcome a situation where there are two disabled DRN nodes on both sides of a source DRN node. This situation is not possible to overcome using the RA algorithm. Additionally, it is noted that as MAX_TX_FACTOR is increased from 3, to 5, the percentage of successfully transmitted DRN packets increases as well. This takes place near the higher range of DRN failure rates since the ability to jump over more DRN nodes improves the probability of success and is only needed with a higher number of failures. For example with a failure rate of 100, the percentage of successfully transmitted packets increases from 33.36 with

V. SIMULATION

Simulation experiments were performed in order to verify the operation, and evaluate the performance of the proposed framework and networking protocol. As indicated in Table 1, the number of DDN nodes used in the simulation is 5, the number of DRN nodes per DDN node is 20, and the number of BSN nodes per DRN node is 6. All nodes are assigned their hierarchical addresses according to the addressing scheme that was discussed earlier. In the simulation, the BSN nodes send their sensed data to their parent DRN node in a periodic manner. Then, the DRN nodes use the networking protocol to route this information to their parent DRN node. In order to verify and test the JA and RA routing protocols and their ability to route the generated packets correctly to the DDN nodes using intermediate DRN nodes, a number of DRN failures were generated using the Poisson arrival distribution with a certain average arrival rate. The average arrival rate of the DRN failures was varied in order to verify the addressing scheme and evaluate the capability of the routing protocol to overcome intermediate DDN node failures. As DRN nodes fail, routing of the DRN packets to either the parent DDN node or the alternative one in the opposite direction is done. When a DRN node fails, the two routing protocols react differently to overcome the failures as specified earlier in the paper. In this simulation, we are focusing on testing the correctness of the protocols. In cases for both routing protocols, as more and more DRN nodes fail, the percentage of successfully transmitted packets decreases. The simulation results are presented in Figures 3, 4, and 5. In the figures the maximal transmission jump factor (MAX_TX_FACTOR) which corresponds to the maximum number of adjacent disabled DRN nodes that can be bypassed by a DRN transmission is varied. Namely, it is set to 3 in 3, 4 in 4, and 5 in 5. The results show that the JA algorithm outperforms the RA algorithm with respect to the percentage of successfully transmitted packets. This is due to the fact that the JA algorithm can overcome multiple adjacent disabled DRN nodes while the RA algorithm cannot. Also the JA algorithm can overcome a situation where there are two disabled DRN nodes on both sides of a source DRN node. This situation is not possible to overcome using the RA algorithm. Additionally, it is noted that as MAX_TX_FACTOR is increased from 3, to 5, the percentage of successfully transmitted DRN packets increases as well. This takes place near the higher range of DRN failure rates since the ability to jump over more DRN nodes improves the probability of success and is only needed with a higher number of failures. For example with a failure rate of 100, the percentage of successfully transmitted packets increases from 33.36 with

MAX_TX_FACTOR=3, to 40.56 with MAX_TX_FACTOR=4, to 43.26 with MAX_TX_FACTOR=5.

VI. CONCLUSIONS AND FUTURE RESEARCH

This paper presented an addressing scheme and routing protocol for monitoring oil, gas and water pipelines. The design was done to meet the objective of taking advantage of the linear structure of the network to increase its efficiency, and cost-effectiveness. In addition, increased reliability is reached by overcoming faulty intermediate node failures, maximizing node battery life, and extending network lifetime. Simulation experiments were conducted to test and evaluate the proposed addressing scheme and routing protocol. In the future, more detailed analysis of other aspects of the model, including security, will be done. In addition, performance optimizations will be considered for various sensing and monitoring applications which generate different network traffic conditions and varied QoS requirements.

REFERENCES


<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of DDN Nodes</td>
<td>5</td>
</tr>
<tr>
<td>Total Number of DRN Nodes Per DDN Node</td>
<td>20</td>
</tr>
<tr>
<td>Total Number of BSN Nodes Per DRN Node</td>
<td>6</td>
</tr>
<tr>
<td>DRN Transmission Rate</td>
<td>2 Mb/s</td>
</tr>
<tr>
<td>Periodic Sensing Interval</td>
<td>10 s</td>
</tr>
<tr>
<td>DRN Data Packet Size</td>
<td>512 bytes</td>
</tr>
</tbody>
</table>