A Framework for Pipeline Infrastructure Monitoring Using Wireless Sensor Networks

Imad Jawhar and Nader Mohamed and Khaled Shuaib
College of Information Technology
United Arab Emirates University
Al Ain, UAE

***Abstract*— Ad hoc and sensor networks is a new area of research which is rapidly growing due to the development of new technologies in inexpensive sensors. These electronic devices have increased capabilities in processing speed, memory, communication and networking [21][22]. Such sensor networks have a vast amount of applications including environmental monitoring, military, ecology, agriculture, inventory control, robotics and health care. This paper discusses the issues and challenges in the use of this new and very promising technology in the protection and monitoring of the critical and essential infrastructures of pipelines carrying oil, gas, water, and other important resources. The paper presents an architectural model that can be used to provide this monitoring and control functions. The model includes an overview of networking and routing protocols that can be used to provide the necessary communications. In addition, the paper provides discussions and recommendations concerning network reliability and the use of different wireless sensor technologies and protocols.**

Keywords: Ad hoc and sensor networks, quality-of-service (QoS), routing, wireless networks, pipeline protection.

I. Introduction

With the fast development of the oil producing countries and increase of demand for energy and water in these areas and the rest of the world, petroleum, natural gas, and water resources and facilities have become important assets for the these countries. Maintaining the economic progress of these countries is strongly depending on protecting these resources and facilities. One of the main and important facilities for these resources is the pipelines used to transfer water, petroleum, and natural gas. Oil, gas, and water pipelines are considered one of the main infrastructures in many countries. Protecting the pipeline infrastructure is one of the important priorities for their economies.

There are a number of technologies to monitor pipelines. These technologies were designed to provide a remote facility to monitor and to report needed pipeline systems status. A network is needed in a pipeline facility for different applications. Examples of these applications are to take measurements inside or outside the pipelines. Inside measurements can be pressure, flow, and temperature measurements. Examples of outside measurements are pipeline area monitoring, pipeline protection cameras, pipeline fire detection, and pipeline liquid leakages. A network is usually spread through a pipeline to transfer the measurements collected from different distributed sensors scattered through a pipeline. Wired networks for pipeline face a number of reliability and security problems.

This paper discusses the advantages and challenges of using ad hoc and wireless sensor networks for monitoring and protecting pipeline infrastructure. This paper also proposes a framework for pipeline infrastructure protection using wireless sensor networks. This framework utilizes the special line structure of wireless sensor networks to solve some of communication reliability and security problems for pipeline monitoring and protection systems. This framework is part of a large project that aims 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 quality of sensors, (QoS) sensitive data, and increase network live time by utilizing the special line structure of pipeline systems.

In the rest of this paper, we outline the needs for monitoring and protecting pipeline infrastructure, in addition to discussing some related work in Section II. Section III discusses some of the advantages of using wireless sensor networks for pipeline protection and monitoring. Section IV describes the proposed framework. Network reliability for the pipeline protection and monitoring system is discussed in Section V. Section VI discusses existing wireless sensor technologies and their use in the proposed sensor network. Section VII concludes the paper.

II. Background

Long pipelines are used in many countries for a number of applications. For example, long pipelines are used to transfer water from desalination plants, which usually are located close to the sea, to cities that are far from the sea. In the Middle East, a big city like Riyadh, home to over four million people, is completely dependant on the water transferred through huge and long pipelines from the Shoaiba Desalination Plant in Al-Jubail in the eastern part of Saudi Arabia. Saudi Arabia is now the world's largest producer of desalinated water supplying major urban and industrial areas through a network of water pipes which run for more than 3,800 km. Furthermore, Oil and gas Industries in the Arabian Gulf heavily depend on oil pipelines for connecting shipping ports, refineries, and oil and gas wells. For example in the United Arab Emirates, there are 2,580 km of gas pipelines, 300 km of liquid petroleum gas pipelines, 2,950 km of oil pipelines, and 156 km of refined products pipelines (2006).

This work was supported in part by UAE Research grant 01-03-9-11/06.
E-mail: {ijawhar, Nader.M, k.shuaib}@uaeu.ac.ae

There are a number of technologies to monitor and to protect pipelines. Most of these technologies are designed specifically for detecting and locating pipeline leakages [7]. These technologies were designed to provide a remote facility to detect and to report the positions of any leakage. Most of these available solutions rely on the availability of a network to transfer the information and report the leakages [23]. These networks are usually wired using copper or fiber optic cables [3][19]. The wired networks are usually connected to regular sensor devices that measure specific attributes such as flow rate, pressure, temperature, etc. There are a number of problems using wired networks with regular sensors for monitoring pipelines. These problems are:

- If there is any damage for any part of the wires of the network, the whole pipeline monitoring system will be compromised.
- It is easy for unauthorized people to disable the monitoring system by cutting the network wires.
- It is difficult to locate the position of the fault in a wire. This problem is more difficult with underground pipelines.
- Different types of information are reported through the network. Some of this information is considered more important to be delivered to the control station than others. For example information reporting a fire is more important than information about pressure measurement. In addition, Duplicate and unwanted information can be transferred on the network causing significant delay for other more important information. This is due to the lack of quality of Service (QoS) support in these existing networks.

The advent of technology in computing and electronics is pioneering an emerging field of tiny wireless sensors, offering an unprecedented opportunity for a wide array of real time applications. In recent years, wireless Sensor Networks are emerging as a suitable new tool for a spectrum of new applications [3]. These tiny sensor nodes are low cost, low power, easily deployable, and self-organizing. They are usually capable of local processing. Each sensor node is capable of only a limited amount of processing, but when coordinated with the information from a large number of other nodes, they have the ability to measure a given physical environment in great detail. Thus, a sensor network can be described as a collection of sensor nodes which co-ordinate to perform some specific action. Unlike traditional networks, sensor networks depend on dense deployment and co-ordination to carry out their tasks. These unique characteristics make them advantageous over traditional networks. Sensor networks applications were originally motivated by military applications such as target detection, surveillance of enemy activities in a battlefield environment and counterterrorism; however, their many advantages over traditional networks resulted in the development of many other potential applications [4] that range from infrastructure security to industrial sensing. Some examples are: environment and habitat monitoring, health applications, home automation, traffic control, etc. Another possible example is using Wireless Sensor Networks for protecting and monitoring pipeline systems.

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 [16], QoS support [14][16][17], security [8], and middleware [11]. Most of these issues are investigated under the assumption that the network used for sensors does not have a predetermined infrastructure [6][9][12][13][15][18][20]. 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.

III. Advantages of the Wireless Sensor Network for Pipeline Protection

This section discusses sum of the advantages of using wireless sensor network technology to provide protection and monitoring of pipeline infrastructures.

A. Network Deployment

The deployment costs of the network of sensors is greatly reduced due to the lack of the need for laying down costly wiring which is also much more involved to connect requiring specialized expertise. On the other hand, wireless sensors are much easier to deploy, since they only need to be individually affixed properly to the pipelines with proper distance from each other.

B. Network maintenance process and personnel

Network maintenance expertise and cost are very inexpensive. If sensors fail due to any reasons such as battery depletion, environmental damage, or malicious actions, this failure will be easily and quickly detected by other sensors as well as many other means which can be redundant in order to maximize security. Once the malfunctioning sensors are detected and located they can be easily replaced by simply physically removing the failed sensor and installing a new one. There will be no need to hardwire the new sensor to the network or program the new sensor. The latter will quickly, automatically and seamlessly register with the ad hoc sensor network and start to perform its required functions. Consequently, the maintenance personnel need very little expertise and they do not need to have specific engineering or programming skills, which reduces the labor cost that is required.

C. Reliability and Security

As is discussed later in this paper, using wireless communication technology allow the addition of low cost, and easily installable redundant sensing and communication nodes which increase the reliability of the network. In addition, important sensor information is disseminated in parallel at numerous intermediate nodes and does not have to travel all the way across the pipeline infrastructure. This makes it much less vulnerable to many types of attacks and failures. Furthermore, many security provisions can be employed to further enhance the security and robustness of the network against many types of attacks. The security aspects of the network will be analyzed and discussed in more detail in future work.

IV. Networking Model Overview and Hierarchy

In this section, the architectural model of the sensor network is presented. This includes network deployment, setup, discovery, and maintenance. 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. Network discovery phase: node location discovery

Once the sensors are physically installed, they will automatically and quickly join the network and begin to perform their required functions. The GPS sensors will determine their locations using the corresponding GPS locating mechanism. Afterwards, the non-GPS less-expensive sensors will run algorithms which will determine their locations in reference to the GPS nodes using measure received signal strength.

B. Data collection and communication packet structure

Each sensor collects data from its environment. The sensor data may relate to different sensing parameters such as temperature, pressure, chemical composition, acoustic signal, and so on. The data will then need to be placed in communication packets which contain the following main fields:

- Type of data. This is one byte. Up to 256 different types of data can be supported. For example, 00 is for temperature, 01 is for pressure, and so on.
- Sensing location. This is the geographical address of the sensor. This is determined after location during the network initialization phase.
- Source sensor address. This field contains the networking address of the source sensor.
- Measurement value. This This is the actual measurement. This is a four byte field, which allows a measurement resolution of up to 2^{32} different values.

C. Node sleep and wake-up times

In order to save battery life, sensors will have a short period of activity during which they will be sensing and sending their readings. During the other part of the duty cycle, the sensors will be in sleep mode. This mode of operation is selected at network configuration time. Such options are available in most sensor MAC protocols which will be discussed later. in this paper.

D. Information coalescing

Nodes are grouped into zones. Each zone will collect data from sensors which are awake and will take the average and send the information to the data collection center in a multi-hop fashion. This is done in order to minimize the amount of data that is transmitted which will in turn contribute to energy savings. This reduction is significant since transmission of data packets is one of the largest contributor to battery depletion in sensor networks. In addition, when the average value for a zone is computed, highest and lowest readings may be dropped. This is done in order to avoid failed sensor readings which can be unusually high or low and inconsistent with values from other sensors in the same area from affecting the average. This process of dropping such reading must be done in a way that does not loose valid sensor readings which happen to be out of the usual range.

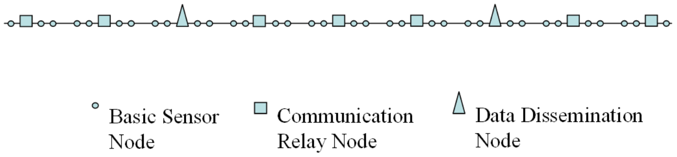

Fig. 1. A pipeline sensor network showing various types of nodes in linear alignment.

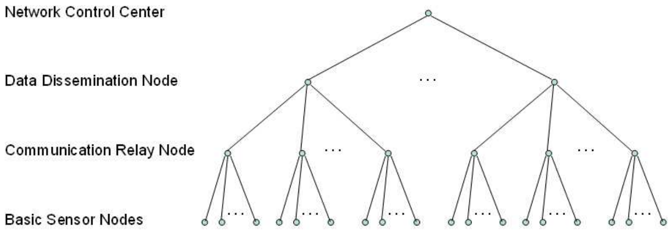

Fig. 2. A hierarchical representation of the pipeline sensor network, showing the parent/child relationship of the various types of nodes.

E. Geographic distance between nodes

The distance between each physically neighboring nodes must be shorter than the transmission range of the nodes. However, in order to increase network reliability and protect against sensor node failure, the transmission range of each node should include a number of nodes. For a node i this number is k_i. During network installation, k_i is set to a starting constant value of k_{max}. During the lifetime of the network, some nodes are expected to fail due to different reasons such as physical damage, battery depletion, or other factors. In such case, the network is still considered connected as long as for each node i in the network, $k_i \geq 1$. Let k_{th} be the minimum acceptable value for k_i such that the network is still operational within a specified reliability level. Therefore, failing nodes are expected to be repaired within a time period such that $k_i > k_{th}$ for each node i in the network. Different strategies can be employed in order to maximize the maintenance process. A greedy approach would be to favor repairing the nodes whose neighbors have the smallest k_i value. Also, the strategy can favor sending repair personnel to areas with higher density of failing nodes.

F. Node hierarchy

All of the nodes in the network will be the same or have the same capabilities. 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 communication relay nodes.
- **Communication Relay Nodes (CRN):** 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. In order to increase reliability, it is recommended that the distance between the nodes be considerably less than the maximum communication distance. This geographic distance can be half of the transmission range for example. More theoretical and experimental analysis can be done in order to determine the optimal distance for a given desirable level of reliability.
- **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 CRN nodes. Each c CRN nodes report to one DDN node.

The DDN nodes 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 CRN center. This distance is usually very long and can be hundreds of kilometers. This would make it vulnerable to a large number of possible failures, unacceptable delay, higher probability of error, and security attacks. The DDN nodes allow the network to discharge its sensor data simultaneously in a parallel fashion. Additionally, the distance between the DDN nodes is important and affects the reliability of the network. A small distance between the DDN nodes 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 1 shows a graphic representation of the different types of nodes and their geographic layout. Figure 2 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 CRN node. In turn, several CRN nodes transmit their data to a DDN node. Finally, all DSN nodes transmit their data to the network control center.

G. GPS capabilities of nodes

The sensor nodes in the network need to be able to determine their geographic locations automatically and seamlessly. In order to achieve this objective some nodes will have GPS capabilities. Upon network initialization, these nodes will determine their geographic locations using their GPS capability. The other sensor nodes in the network do not have to have this feature. They will determine their location with reference to the GPS nodes using signal strength measurements and a localization algorithm.

H. Network routing protocols

Communication of information in the network is done at the following levels.

I. Communication from BSN to CRN nodes

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

J. Hop and skip protocol: Communication from CRN to DDN Nodes

Communication between the CRN and DDN nodes is done using a multi-hop routing algorithm which functions on top of a MAC protocol such as Zigbee. This protocol is referred to as the *Hop and Skip Protocol (HSP)*. The HSP protocol works in the following manner.

Information coalescing at the source CRN node:

When the CRN receives its information from the sensors that are registered with itself, it performs the task of data coalescing and summarization of information. This process consists of the following actions. The CRN node constantly receives sensor readings from its registered sensors. However, it processes this information and summarizes it into one or more attributes. For example, it receives multiple temperature readings from its child sensors during a period of time named “sensing interval”, t_{si}. During this period, each sensor S_i might have reported several readings, which are elements in the set R_i^j, where j is the sensing period number. The CRN node can calculate the average of all elements in the set R_i^j for period j. This average is termed Avg_i^j. The CRN node can then do one of the following actions, depending on the design specifications chosen at network installation time:

- Send the value Avg_i^j for each node registered BSN node i during sensing period j.
- Calculate and send the average value, Avg^j, for all Avg_i^j values for all of its registered BSN nodes for period j.

After calculating the average values, the CRN node can do one of the following actions depending on the network configuration:

- **Send actual value:** Send the actual current value, V_c.
- **Send significant changes only:** Compare the calculate value with a reference value and only send this information in the case the difference is greater than a threshold value Δ_{th}, where(V_c-V_{ref}) $> \Delta_{th}$.

The second option of transmission of “significant changes only” is desirable in order to preserve valuable transmission energy, which is a critical factor in sensor networks. However, if this policy is adopted, the reference values must be periodically synchronized between the network control center and the CRN nodes.

Algorithm at the source and intermediate CRN nodes:

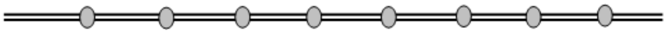

Fig. 3. A pipeline monitored by a wireless sensor network.

Each CRN node is within range of 2*k CRN nodes (k nodes in each direction), where k is the overlapping factor of the range of the CRN nodes defined earlier. Each set of consecutive CRN nodes consider their nearest DDN node their parent. A CRN node will transmit its packet in the direction of its parent DDN node using a multihop approach to reach it. Since k CRN nodes are within its range, each CRN node has k 1-hop neighbors, and it will send its packets in a rotation manner through these neighbors. A node y has k nodes, z_1, z_2, through z_k as its 1-hop neighbors. Node y will transmit its first packet to node z_1, the second to node z_2, the k^{th} to z_k, and the $k^{th}+1$ to z_1 and so on. This is done in order to spread the transmission load between the k neighbors in order to use their valuable energy evenly, maximize network lifetime and prevent early network partitioning.

In order to achieve this rotation mechanism, each CRN node maintains a counter named RC. The RC counter is initialized at 1 and is incremented by 1 each time a packet is transmitted by the CRN node. The counter rolls back to 1 each time it reaches its maximum value which is k.

Algorithm at the destination DDN node:

When the destination DDN node receives the packet, it transmits it to the NCC center. An acknowledgment mechanism can be adopted in which the DDN sends a positive acknowledgment to the sending CRN node. However, in order to save battery life, no acknowledgments are sent in our protocol. A positive acknowledgement mechanism can however be employed for more sensitive data.

K. 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.

V. Network Reliability

One of the main advantages of using wireless sensor networks for monitoring and protecting pipelines is communication reliability. A network is needed in a pipeline facility for different applications. Examples of these applications are to take measurements inside or outside the pipelines. Inside measurements can be pressure, flow, and temperature measurements. Examples of outside measurements are pipeline area monitoring, pipeline protection cameras, pipeline fire detection, and pipeline liquid leakages. A network is usually spread through a pipeline to transfer the measurements collected from different distributed sensors scattered through a pipeline. The reliability degree of the whole pipeline monitoring and protection system is highly depending on the reliability of the network. Using a network with low reliability levels will be negatively reflected on the monitoring and protection system of the pipeline. For example wired networks are very unreliable. Any fault in the wires of the network may suspend the whole monitoring and protection system, while wireless networks are less susceptible to these failures. Using wireless communication networks instead of wired networks for pipeline monitoring and protection applications has a number of tradeoffs for communication reliability. For example, the pipeline in Figure 3 is monitored by a wireless sensor network. Each node in the figure represents a communication relay node (CRN) which collects and filters information collected by other basic sensor nodes located close to it. The sensed data is transferred from one communication relay node to another communication relay node until it researches a data dissemination node (DDN) which will transfer it to the pipeline control station though another communication media.

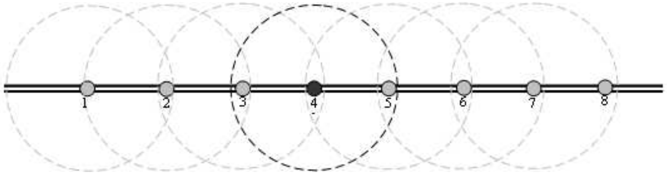

Fig. 4. The wireless signal range is limited. Sensed data from node 4 can be sent to the control station through node 3 or node 5.

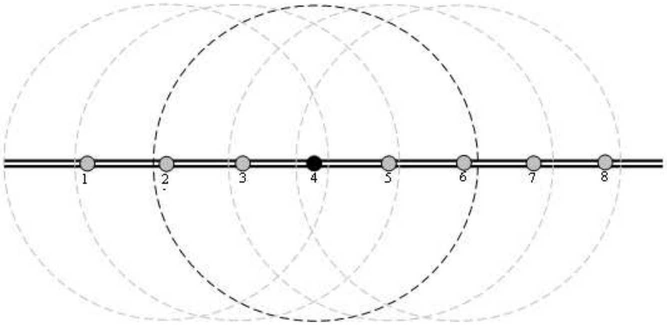

Fig. 5. Each node can communicate with four nodes.

Wireless signals are used for communication among the nodes. The wireless signal range can be as in Figure 4 where the signal range for each node can reach only one node to the left and another node to the right. The major problem with this model is that if there is any problem with any node in the network the connectivity of the nodes will be lost and the network is partitioned. Using a limited wireless range will reduce power consumption in the nodes; however, a connectivity problem may occur. In other words, damaging a single node may suspend the whole monitoring and protection system for a pipeline.

A wider signal range can be used among senor nodes. This

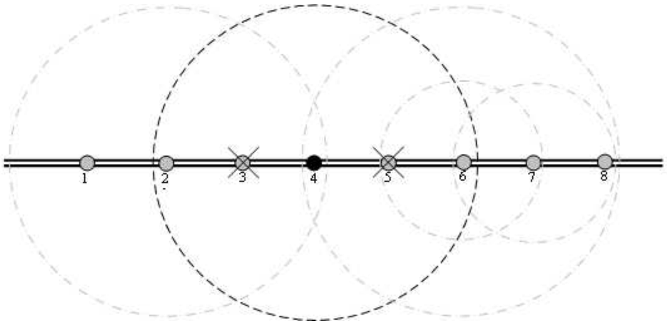

Fig. 6. Automatic wireless range configuring. Nodes can have different wireless range to stay connected.

will consume more energy from senor batteries; however, it can provide better reliability in case there is any problem with some nodes. For example, each node in Figure 5 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.

Although increasing the range can provide better reliability, more energy will be consumed from the communication relay nodes. A dynamic configuration for wireless range can provide better power management. An example of this configuration is in Figure 6. In this network, failure occurs at nodes 3 and 5. Therefore, the wireless range for node 4 is increased to reach nodes 2 and 6.

VI. Wireless Sensor Technologies

Recently many wireless sensor technologies have been introduced for a wide range of applications. The choice of a particular technology over another is mandated by the application's requirements, usability, availability, surrounding environment, power consumption, security features and other factors. In this project, any chosen wireless sensor technology to be implemented as the network nodes should be capable of satisfying the following requirements:

1) Low power consumption.
2) Support for various data rates.
3) Availability of security features such as authentication and encryption.
4) Support for various network topologies.
5) Support for QoS when needed.
6) Support for full or reduced functionalities as needed.
7) Support for various transmission ranges.
8) Support for standard based protocols.
9) Cost effective.
10) Available as an existing product.
11) Support both line of sight and non-line of sight RF communication.
12) Self configurable and support for mesh networking.
13) Multi sensing capability.

In this section we look at several wireless sensor network technology standards and their suitability for this project.

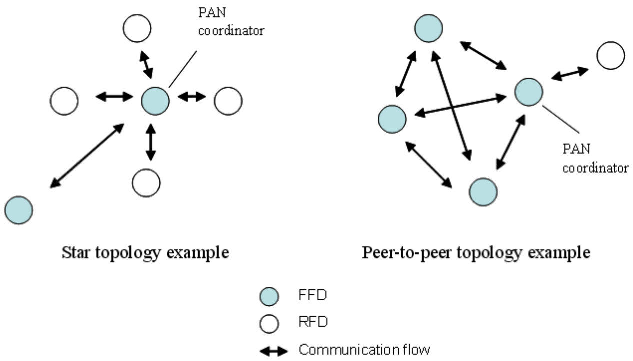

Fig. 7. Zigbee star and peer-to-peer example topology.

A. Bluetooth

The Bluetooth (BT) [1] standard is a specification for Wireless Personal Area Networks(WPAN). Although products based on the Bluetooth standard are often capable of operating at greater distances, the targeted operational area is the area around an individual, e.g. within 10 meters of the user. Bluetooth utilizes a short range radio link that operates in the 2.4 GHz industrial scientific and medical (ISM) band similar to WLAN. However, the radio link in Bluetooth is based on frequency hopping spread spectrum techniques. Although at any point in time, the Bluetooth signal occupies only 1MHz, the signal changes center frequency (or hops) deterministically at a rate of 1600 hops per second. Bluetooth hops over 79 center frequencies, so over time the Bluetooth signal actually occupies 79MHz. Bluetooth is most suitable for small ad hoc network configurations, where devices can be operating either in a master or slave mode. Bluetooth power consumption is high as compared to other wireless sensor devices, and therefore will not be considered as an appropriate technology option for a large scale project such as the one proposed here.

B. IEEE 802.15.4 (Zigbee)

The new short range, low power, low rate wireless networking Zigbee standard, IEEE 802.15.4 [5] [10] [2] complements the high data rate technologies such as WLAN and open the door for many new applications. This standard operates at two bands, the 2.4 GHz band with a maximum rate of 250 kbps and the 868-928 MHz band with data rates between 20 and 40 kbps. Zigbee is based on DSSS and it uses binary phase shift keying (BPSK) in the 868/928 MHz bands and offset quadrature phase shift keying (O-QPSK) modulation at the 2.4 GHz band. While Bluetooth devices are more suited for fairly high rate sensor applications and voice applications, Zigbee is better suited for low rate sensors and devices used for control applications that do not require high data rate but must have long battery life, low user interventions and mobile topology.

Zigbee is designed as a low complexity, low cost, low power consumption and low data rate wireless connectivity standard. Zigbee supports scalable data rates, for example, it can be used for medical file transfer at the rate of 250 kbps while supporting sensor based applications at the rate of 20 kbps.

The range for Zigbee is between 100 and 300 feet, but it can be extended using a Zigbee bridge up to 40 miles.

The Zigbee standards define two types of devices, a full-function device (FFD) and a reduced function device (RFD). The FFD can operate in three different modes, a personal area network (PAN) coordinator, a coordinator or a device. The RFD is intended for very simple applications that does not require the transfer of large amount of data and needs minimal resources. A WPAN is formed when at least two devices are communicating one being an FFD assuming the role of a coordinator. Depending on the application requirements, Zigbee devices might operate either in a star topology or a peer-to-peer topology. Figure 7 shows both topologies. As seen in the figure, in a star topology the flow of communication is established between devices and an FFD acting as the PAN coordinator. The PAN coordinator is a device that is responsible for initiating, terminating and routing information around the network. The star topology is mostly used in small areas such as home automation, personal health care management and hospital rooms while the peer-to-peer topology is used in larger scale and more complex networks.

Zigbee MAC layer is designed with QoS in mind for applications that demands low delay and guaranteed bit rate. This is accomplished in Zigbee by defining a super frame MAC layer structure that contains a contention free period to be used when QoS data need to be transferred.

ZigBee provides layer based security where security can be applied by the different layers, application , network and data link layer independently. End to end security can be achieved without the need for data to be decrypted and re-encrypted at each hop. ZigBee uses the 128-bit Advanced Encryption Standard (AES) to protect data and can utilize Elliptical Curve Cryptography (ECC) as a public-key encryption algorithm for scalability and to achieve robust wireless network security. Zigbee can be considered the best available sensor MAC technology for this network since it satisfies most of the needed requirements.

VII. Conclusions

In this paper, a wireless sensor network framework for oil, gas, and water pipeline protection and monitoring was presented. This framework is designed in order to meet the objectives of efficiency, cost-effectiveness, security, and reliability. A routing protocol that is used to relay sensor information from the field nodes to designated base nodes was introduced. The protocol has the features of load balancing, maximizing individual node battery life as well as extending network lifetime with minimal maintenance requirements. Future work involves providing more detailed design and analysis of the various aspects of the model. Security considerations will also be addressed and incorporated into the design. In addition, simulation experiments will be conducted to evaluate the performance of the proposed model and its associated protocols.

References

[1] Specifications of the bluetooth system - version 1.2. 2003.

[2] P. Baronti, P. Pillai, V. Chook, S. Chessa, and F. Gotta, A. andFun Hu. Wireless sensor networks: a survey on the state of the art and the 802.15.4 and zigbee standards. *Communication Research Centre, UK*, May 2006.

[3] A. Carrillo, E. Gonzalez, A. Rosas, and A. Marquez. New distributed optical sensor for detection and localization of liquid leaks. *Pat I. Experimental Studies, Sens, Actuators*, A(99):229–235, 2002.

[4] C. Chong and S.P. Kumar. Sensor networks: Evolution, opportunities, and challenges. *The proceedings of the IEEE*, 91(8), August 2003.

[5] IEEE P802.15.4 / D18. Low rate wireless personal area networks. 2003.

[6] S. De, S.K. Das, H. Wu, and C. Qiao. A resource efficient RT-QoS routing protocol for mobile ad hoc networks. *Wireless Personal Multimedia Communications, 2002. The 5th International Symposium on*, 1:257–261, 2002.

[7] I. Ellul. Pipeline leak detection. *Chem. Eng.*, pages 40–45, June 1989.

[8] E. Fernandez, I. Jawhar, M. Petrie, and M. VanHilst. *Security of Wireless and Portable Device Networks: An Overview.*

[9] I. Gerasimov and R. Simon. Performance analysis for ad hoc QoS routing protocols. *Mobility and Wireless Access Workshop, MobiWac 2002. International*, pages 87–94, 2002.

[10] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile. Ieee 802.115.4; a developing standard for low power, low cost wireless personal area networks. *IEEE Network*, 15(5):12–19, Sept/Oct 2001.

[11] S. Hadim, J. Al-Jaroodi, and N. Mohamed. Trends in middleware for mobile ad hoc networks. *The Journal of Communications*, 1(4):11–21, July 2006.

[12] S. Hadim and N. Mohamed. Middleware challenges and approaches for wireless sensor networks. *IEEE Distributed Systems*, 7(3), March 2006.

[13] Y. Hwang and P. Varshney. An adaptive QoS routing protocol with dispersity for ad-hoc networks. *System Sciences, 2003. Proc. of the 36th Annual Hawaii International Conference on*, pages 302–311, January 2003.

[14] I. Jawhar and J. Wu. Qos support in tdma-based mobile ad hoc networks. *The Journal of Computer Science and Technology (JCST)*, 20(6):797–910, November 2005.

[15] I. Jawhar and J. Wu. Quality of sevice routing in mobile ad hoc networks. *Resource Management in Wireless Networking, M. Cardei, I. Cardei, and D. -Z. Du (eds.), Springer, Network Theory and Applications*, 16:365–400, 2005.

[16] I. Jawhar and J. Wu. Race-free resource allocation for QoS support in wireless networks. *Ad Hoc and Sensor Wireless Networks: An International Journal*, 1(3):179–206, May 2005.

[17] I. Jawhar and J. Wu. Resource allocation in wireless networks using directional antennas. *The Fourth IEEE International Conference on Pervasive Computing and Communications (PerCom-06), Pisa, Italy. Publisher IEEE Computer Society*, pages 318–327, March 2006.

[18] W.-H. Liao, Y.-C. Tseng, and K.-P. Shih. A TDMA-based bandwidth reservation protocol for QoS routing in a wireless mobile ad hoc network. *Communications, ICC 2002. IEEE International Conference on*, 5:3186–3190, 2002.

[19] W. Lin. Novel distributed fiber optic leak detection system. *Opt. Eng.*, 43:278–279, 2004.

[20] S. Nelakuditi, Z.-L. Zhang, R. P. Tsang, and D.H.C. Du. Adaptive proportional routing: a localized QoS routing approach. *Networking, IEEE/ACM Transactions on*, 10(6):790–804, December 2002.

[21] C. E. Perkins. *Ad Hoc Networking*. Addison-Wesley, Upper Saddle River, NJ, USA, 2001.

[22] C. E. Perkins and E. M. Royer. Ad hoc on demand distance vector (AODV) routing. *Internet Draft*, August 1998.

[23] Y. Tu and H. Chen. Design of oil pipeline leak detection and communication systems based on optical fiber technology. *proc. SPIE*, 3737:584–592, August 1999.