Monitoring Linear Infrastructures Using Wireless Sensor Networks ⋆

Imad Jawhar, Nader Mohamed, Khaled Shuaib and Nader Kesserwan

College of Information Technology
United Arab Emirates University
P.O. Box 17551, Al Ain, UAE
E-mail: {ijawhar, nader.m, k.shuaib, nkesserwan}@uaeu.ac.ae

Abstract. This paper presents and evaluates a protocol for Linear Structure wireless sensor networks which uses a hierarchical addressing scheme designed for this type of networking environment. This kind of linear structure exists in many sensor applications such as monitoring of international borders, roads, rivers, as well as oil, gas, and water pipeline infrastructures. The networking framework and associated protocols are optimized to take advantage of the linear nature of the network to decrease installation, maintenance cost, and energy requirements, in addition to increasing reliability and improving communication efficiency. In addition, this paper identifies some special issues and characteristics that are specifically related to this kinds of networks. Simulation experiments using the proposed model, addressing scheme and routing protocol were conducted to test and evaluate the network performance under various network conditions.

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

1 Introduction

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 [1]. These tiny sensor nodes are low cost, low power, easily deployed, 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.

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 [8], QoS support [7][9], security [2], and middleware [4]. Most of these issues are investigated under the assumption that the network used for sensors does not have a predetermined infrastructure [3][5][10][11]. Fortunately, the wireless sensor network needed for monitoring linear infrastructures

---

⋆ This work was supported in part by UAEU Research grant 08-03-9-11/07.

---

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 this kind of networks.

This paper addresses the issues and challenges of using wireless sensor networks that are aligned in a linear formation for monitoring and protection of critical infrastructures and geographic areas. Also, it presents a routing protocol and addressing scheme for this special kind of sensor networks. As mentioned earlier, this kind of alignment of sensors can arise in many applications such as the monitoring and surveillance of international boundaries for illegal crossing, or smuggling activities, monitoring of roads, or long pipelines carrying oil, gas and water resources, river environmental monitoring, as well as many other such uses. The presented 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 quality of service (QoS) sensitive data, and increase network lifetime by utilizing the special linear structure of the network. This paper extends the model and architecture discussed in [6]. More details on the background, motivation, advantages, and applications for using linear structure wireless sensor networks can be found in that paper.

There are many advantages for using wireless sensor network technology to provide protection and monitoring of linear infrastructures such as oil, water, and gas pipelines, international borders, roads and rivers. Some of these advantages are: (1) Faster and less costly network deployment. (2) Additional savings in network maintenance and necessary personnel expertise. (3) Increased reliability and security due to the ability to disseminate collected information at designated wireless access points, and the ability to introduce flexible multihop routing which can overcome intermediate node failures.

The rest of the paper is organized as follows. Section II presents the networking model overview and hierarchy. Section III presents the node addressing scheme and routing protocols. Section IV presents the simulation and analysis of results. Section V presents additional optimizations that can be used to further improve the performance of the network. The conclusions and future research are presented in the last section.

2   Networking Model Overview and Hierarchy

In this section, the architectural model of the sensor network is presented.

2.1   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
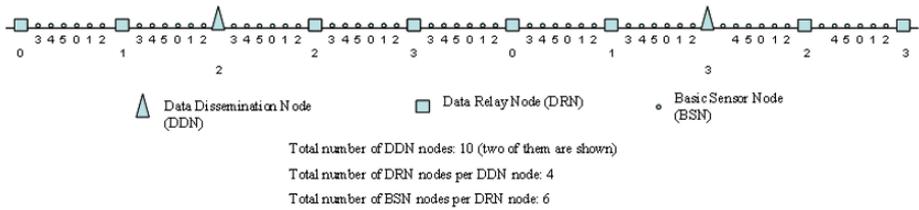
Fig. 1. Illustration of the addressing scheme used to assign DDN, DRN, and BSN address field values.
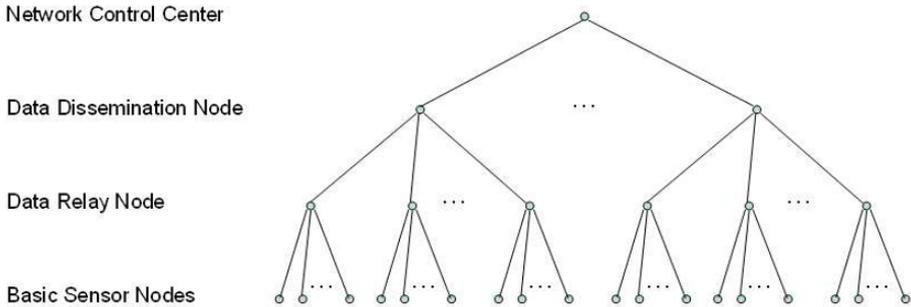

Fig. 2. A hierarchical representation of the linear structure sensor network, showing the parent/child relationship of the various types of nodes.

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.

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 DRN 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 DRN node. In turn, several DRN nodes transmit their data to a DDN node. Finally, all DDN nodes transmit their data to the network control center.

3   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.

3.1   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 field:* 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 field:* If this is a BSN node, then this node holds its own address. If 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 typical full address for a DDN node is: 23.ϕ.ϕ. The two empty symbols in both the BSN and DRN fields indicate that this is a DDN node.

3.2   Address assignment

In this section, the process of assigning values to the different fields of the address of each node is described. Figure 1 shows an example linear alignment of DDN, DRN, and BSN nodes with the corresponding addresses for each node. The addresses in each field are assigned in the following manner:

- *DDN address field assignment:* The DDN nodes have a DDN 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 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).

   – *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 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).

3.3 Communication between different types of nodes

   – *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.

   – *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 three different routing protocols for multihop communication among the DRN nodes are presented. These protocol are discussed later in this paper.

   – *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 communications 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.

3.4 The routing algorithms at the source and intermediate 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.

As mentioned earlier, 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. 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. In order to increase network reliability, if the connection with

the next hop is not available then the DRN node can execute one of three algorithms to overcome this problem.

Jump Always Algorithm (JA):

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_JUMP_FACTOR which holds the maximum number of broken links or "disabled nodes" that a DRN transmission can bypass.

Redirect Always Algorithm (RA):

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. 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 node is larger. In that case, each DRN node 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 is a combination of the first two algorithms JA and RA. We define as *sibling DRN nodes* to a particular DRN node x, the DRN nodes that have the same parent DDN node as x. We also define as *secondary sibling DRN nodes* to x the DRN nodes that have as parent DDN node the secondary parent DDN node (i.e. the DDN node that is on the opposite side of the parent DDN node with respect to x) of x. In this algorithm, each node contains information about the operational status of its sibling and secondary sibling DRN nodes. Consequently, before dispatching the message, it

calculates the total necessary energy it needs to reach its parent DDN node E_x^p and the total energy it needs to reach its secondary parent E_x^{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 $E_x^p \leq E_x^{sp}$ then the message is sent towards the parent DDN node. Otherwise, the message is sent towards the secondary parent DDN node. 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 DRN nodes is cached by the DRN nodes from participations in previous packet transmissions. More research is being conducted for the most efficient means of gathering such information by the DRN nodes.

Table 1. Simulation Parameters

Parameter	Value
Total Number of DDN Nodes	5
Total Number of DRN Nodes Per DDN Node	100
Total Number of BSN Nodes Per DRN Node	6
DRN Transmission Rate	$2\ Mb/s$
Periodic Sensing Interval	$10\ s$
DRN Data Packet Size	512 bytes
MAX_JUMP_FACTOR	3

4   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, and the number of BSN nodes per DRN node is 6. The number of DRN nodes per DDN node was varied between 100, 120, and 140. The results are presented in figure 3. For the JA and SRJ algorithms the MAX_JUMP_FACTOR is set to 3. 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 the 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, 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 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 three 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 operation of the protocols and assessing their performance with respect to each other. In figure 3, the number of DRN
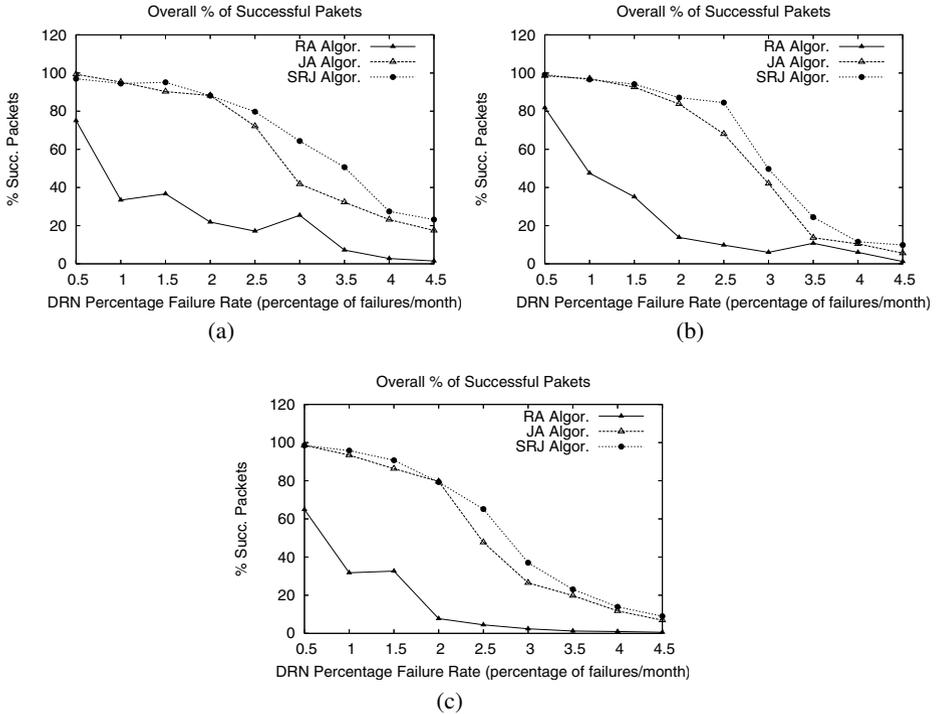
Fig. 3. Simulation results. (a) NUM_DRN_PER_DDN=100. (b) NUM_DRN_PER_DDN=120. (c) NUM_DRN_PER_DDN=140.

nodes per DDN node was varied in order to study the impact of increasing the number of DRN nodes per DDN node on network performance. The percentage of successfully transmitted packets was measured as the DRN percentage failure rate (percentage of DRN failures per month) was varied. As can be seen in all three parts of figure 3, the percentage of successfully transmitted packets decreases as the percentage of DRN failures increases. Also, it can be clearly seen that the SRJ algorithm provides the best performance followed by the JA algorithm and the RA algorithm respectively. This is expected since the RA algorithm does not try to jump over a failed DRN node, and only tries redirecting the packet once. If it encounters another failed DRN node in the opposite direction then the packet is dropped. The performance of the JA algorithm is better than that of the RA algorithm. This is also expected since the JA algorithm allows a DRN transmission to overcome failed nodes by jumping over them. However, if more than maximum number consecutive failed DRN nodes is encountered, then the packet is dropped without trying to go in the opposite direction, which might ensure successful transmission of the packet. The SRJ algorithm offers the best 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 DRN

nodes, the SRJ algorithm also ensures a smaller number of DRN failures due to battery depletion which increases network lifetime and improves its performances.

Additionally, the results show that as the number of DRN nodes per DDN node increases from 100 to 120, to 140, the percentage of successfully transmitted packets decreases for all three algorithms. For example, for the SRJ algorithm case, with a percentage failure rate of 3 percent failures per month, the percentage of successfully transmitted packets decreases from 64.35 for DRN_PER_DDN = 100, to 49.72 for DRN_PER_DDN = 120, to 37.04 for DRN_PER_DDN = 140. This decrease in performance as the number of DRN nodes per DDN node increases is expected due to the linear structure of the network. With the increased number of DRN nodes that a packet has to use to reach the DDN node, the probability of encountering a more than maximum number of consecutive failed DRN nodes which prevents it from going further increases. Therefore, when designing such a network, the number of DRN nodes per DDN node must not be too large in order to ensure good network performance.

5   Additional Optimizations

This section presents some of the issues, observations, problems, possible solutions, and optimizations that are being considered for current and future research this area.

5.1   DRN types of failures

Two types of failures of DRN nodes can be identified depending on the cause of the failure:

- Normal-life DRN failures: These failures are due to the normal battery depletion of the DRN nodes.
- *Sub-normal-life DRN failures:* These failures are due to the expiration of a DRN node due to factors other than normal battery depletion from energy consumption. Such failures can be caused by physical damage, environmental damage, a manufacturing defect, a hardware or software problem, and so on. Such failures can happen at any time and to any DRN node regardless of its position with respect to the other nodes in the network. These failures can cause a black hole effect when using certain routing protocols. These effects will be discussed in a later section.

5.2   Proportional depletions: the suspension bridge effect

One important observation that is noted is that the energy consumption is higher in the DRN nodes that are closer to the DDNs. Specifically, the total energy consumption in the DRN nodes is inversely proportional to the number of hops of that node to the DDN nodes. This is due to the fact that as a node is closer to a DDN node, it will be a part of a proportionally higher number of paths from farther nodes that are trying to reach the DDN node. In other words, more farther nodes will use it as an intermediate node send their messages to the DDN node. This means that assuming that all DRN
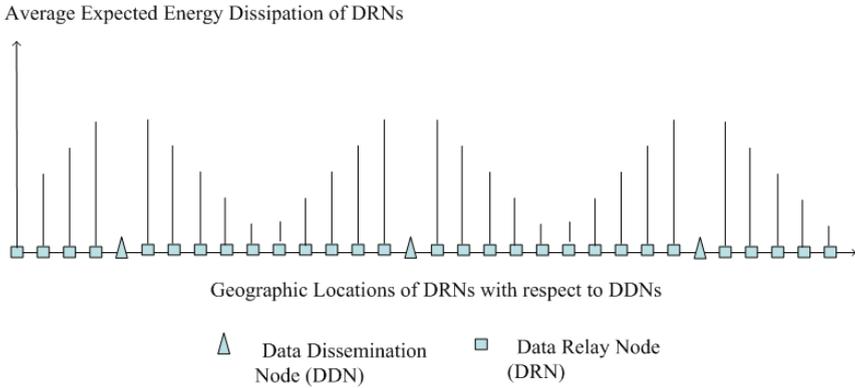
Average Expected Energy Dissipation of DRNs

Fig. 4. Illustration of the suspension bridge effect: the average expected energy dissipation of DRN nodes according to their respective distance from DDN nodes.

node failures are due to normal-life failures, the DRN nodes that are within one hop of the DDN nodes will fail first, followed by the DRN node within 2 hops of the DDN nodes, then by the nodes within 3 hops and so on. If one is to plot the average expected energy dissipation of DRN nodes (on the y-axis) versus distance (on the x-axis) we get a suspension bridge-like figure where average expected energy dissipation of the one-hop DRN nodes (one hop from the DDN nodes) is the highest, followed by the 2-hop DRN nodes, and so on. figure 4 Shows an illustration of the average expected energy dissipation requirements of DRN nodes according to their respective distance from the DDN nodes. The figure shows that the closer a DRN node is to the DDN nodes the higher its average expected energy dissipation requirements.

5.3 Possible remedies to the suspension bridge effect

Two possible solutions can be used to remedy the rapid expiration of the DRN nodes closest to the DDN nodes.

Variable distance between DRN nodes: One solution would be to exponentially decrease the distance between DRN nodes as they get closer to the DDN nodes. This decrease in distance would require them to spend less energy to hop to the next node on the way to the DRN node. This will compensate for the higher number of transmissions that this node must do being a part of more paths that go through it. The change in the density of the DRN nodes can be done in such a way that the total energy consumption of the DRN nodes is the same regardless of their proximate position from the DDN nodes.

Variable initial energy capacity of DRN nodes: Another possible solution for this problem is to simply equip the nodes closer to the DDN with higher initial energy assuming. This solution is only possible if such feature or option is available with the type of technology and product that is used to implement the DRN nodes.
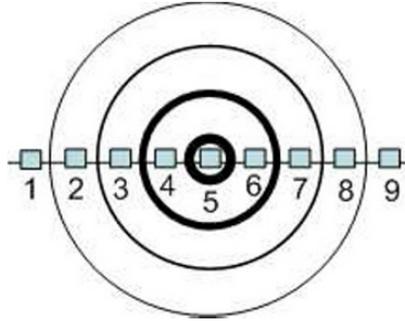
Fig. 5. An illustration of the black hole effect.

5.4   Depletions around a failed node: the black hole effect

Another type of effect can happen when a DRN node has a sub-normal-life failure. Due to this type of failure's unpredictable causes, it can happen to any DRN node at any given location with respect the DDN nodes and at any time. If the routing protocol that is used overcomes such a failure by jumping over the failed DRN node then this requires a higher energy consumption for transmission from the two surrounding DRN nodes. This means that the expected battery lifetime of these nodes is shortened. When these two nodes fail due to their decreased battery lifetime, the live DRN nodes next to them must now multiply their transmission power in order to overcome multiple adjacent DRN nodes that failed, the original one and the one next to it. In turn this will increase their energy consumption and cause them to fail when their batteries are depleted. The DRN nodes that are next to the three failed DRN nodes will now have to spend even more energy to jump over them, and so on. We name this process the *black hole effect*. The initialled failed DRN node is compared to a black hole that causes other adjacent DRN nodes to fail, which subsequently cause nodes adjacent to them to fail and widening the diameter of the failed DRN nodes. This is comparable to a widening black hole of failing DRN nodes with the initial failed DRN node at is center. This effect is illustrated in figure 5. In the figure, DRN node 5 fails first, and starts the process which causes the surrounding nodes to fail in sequence according to their proximity to the initial failed node. In this case, the failure of node 5 is followed consecutively by the failures of nodes 4/6, 3/7, and 2/8. This process continues until the number of failed adjacent DRN nodes is so high that it cannot be overcome by the maximum transmission range of DRN nodes. This results in partitioning of the linear network at this location.

6   Conclusions and Future Research

In this paper, an addressing scheme and routing protocol for linear structure wireless sensor networks was presented. This architecture and routing protocol are designed to meet the objectives of efficiency, cost-effectiveness, and reliability. The routing protocol is used to relay sensor information from the field nodes to a designated control

center. The protocol has the features of increased reliability by overcoming intermediate node failures, maximizing individual node battery life as well as extending network lifetime with minimal maintenance requirements. Simulation experiments were conducted to test and evaluate the efficiency of the network protocol and underlying addressing scheme. Future work involves providing more detailed design and analysis of the various aspects of the model, as well as further optimization of the routing protocol and strategy. Security considerations will also be addressed and incorporated into the design. In addition, more extensive simulation experiments will be conducted to evaluate the performance of the proposed model and its associated protocols under various network conditions.

References

1. 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.
2. E. Fernandez, I. Jawhar, M. Petrie, and M. VanHilst. *Security of Wireless and Portable Device Networks: An Overview.*
3. 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.
4. 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.
5. Y. Hwang and P. Varshney. An adaptive QoS routing protocol with dispersity for ad-hoc networks. *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, pages 302–311, January 2003.
6. I. Jawhar, N. Mohamed, and K. Shuaib. A framework for pipeline infrastructure monitoring using wireless sensor networks. *The Sixth Annual Wireless Telecommunications Symposium (WTS 2007), IEEE Communication Society/ACM Sigmobile, Pomona, California, U.S.A.*, April 2007.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.