MITIGATION TECHNIQUES FOR THE ENERGY HOLE PROBLEM IN WIRELESS SENSOR NETWORKS

by

Ilir Bojaxhiu

B.S., in Computer Engineering, Boğaziçi University, 2006

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Computer Engineering

Boğaziçi University

2009

MITIGATION TECHNIQUES FOR THE ENERGY HOLE PROBLEM IN WIRELESS SENSOR NETWORKS

APPROVED BY:

Prof. Cem Ersoy .....
(Thesis Supervisor)

Assist. Prof. Ertan Onur .....
(Thesis Co-supervisor)

Assoc. Prof. Necati Aras .....

Assist. Prof. Haluk Bingöl .....

Assoc. Prof. Tuna Tuğcu .....

DATE OF APPROVAL: 09.06.2009

ACKNOWLEDGEMENTS

I would like to thank my thesis supervisor Prof. Cem Ersoy and my thesis co-supervisor Assist. Prof. Ertan Onur for their continuous support, motivation and lasting guidance throughout this thesis. I would also like to thank Assoc. Prof. Necati Aras, Assist. Prof. Haluk Bingöl and Assoc. Prof. Tuna Tuğcu for being part of my thesis committee and for their comments and suggestions.

I am thankful to the NETLAB members for all the valuable discussions and feedback. I am thankful to Assist. Prof. Ertan Onur for the deployment quality calculation library which is used throughout my simulations. I would like to thank Rabun Koşar for his support, suggestions and the MATLAB redeployment functions which are used in the simulations . I would also like to thank Atay Özgövde, Yunus Durmuş and Dr. İlker Demirkol for introducing me to the OPNET simulator and their sensor MAC implementation. I am also thankful to my friends and my coworkers at Karash Software Technologies for their support and friendship.

Last but not least, I am grateful to my family and my fiancée Erisa for their patience, encouragement, energy and motivation, without whom the completion of this thesis would have not been possible.

This work has been supported by TUBİTAK under the grant number 106E082 and by BAP under the grant number 09A101P.

ABSTRACT

MITIGATION TECHNIQUES FOR THE ENERGY HOLE PROBLEM IN WIRELESS SENSOR NETWORKS

Uneven energy consumption in wireless sensor networks can drastically reduce the network lifetime. The large number of sensors reporting to a single data collection sink exposes the sensors around the sink to a higher traffic load. This causes the energy at these nodes to be consumed more rapidly which is known as the energy hole problem in wireless sensor networks. Although this problem is inherent to the network topology, several strategies can be developed to delay the hole formation and thus extend the network lifetime.

In this work, we measure the performance of three different approaches used to mitigate the energy hole problem in surveillance wireless sensor networks. We evaluate the surveillance quality of the network over time for different network configurations and mitigation strategies using realistic sensor models, MAC and routing protocols in simulations.

ÖZET

KABLOSUZ ALGILAYICI AĞLARDA ENERJİ BOŞLUĞU PROBLEMİNİ HAFİFLETMEK İÇİN TEKNİKLER

Kablosuz algılayıcı ağlarda dengesiz enerji tüketimi sistem ömrünü ciddi şekilde etkileyebilir. Tek bir veri toplama merkezine bağlı olan algılayıcılar merkez etrafındaki algılayıcıların yüksek bir veri trafiğine maruz kalmalarına sebep olurlar. Yüksek trafik, algılayıcıların enerjisinin daha hızlı tüketilmesine sebep olur ve merkez etrafında delikler oluşmaya başlar. Bu problem, enerji deliği problemi olarak bilinir. Her ne kadar bu problem ağ topolojisine bağlı bir problem olsa da, ağ ömrünü uzatmak ve deliklerin oluşmasını geciktirmek icin değişik stratejiler geliştirilebilir.

Bu çalışmada, gözetim amaçlı telsiz algılayıcı ağlarda enerji deliklerinin etkisini azaltmak için geliştirdiğimiz üç yaklaşımın başarımını inceledik. Farklı ağ ayarları ve stratejilerinin sistem gözetim kalitesine etkilerini analiz edebilmek için benzetimlerimizde gerçekçi bir algılayıcı modeli, ortama erişim kontrolü ve yönlendirme protokolleri kullandık.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS/ABBREVIATIONS

d	Distance between the sensor and the intruder
r	Average detection range of the sensor
r_e	Uncertainty in the detection range of the sensor
α	Distance of the intruder form the start of the uncertainty region $(d-(r-r_e))$
β	Parameter for shaping the detection probability in the uncertainty region of the sensor
λ	Parameter for shaping the detection probability in the uncertainty region of the sensor

CBR	Constant bit rate
DQM	Deployment Quality Measure
FoI	Field of Interest
MAC	Medium Access Control
NDC	Neighborhood Density Control
RX	Reception
S-MAC	Medium Access Control for Wireless Sensor Networks
SWSN	Surveillance Wireless Sensor Network
TX	Transmission
WDQM	Watershed Deployment Quality Measure
WSN	Wireless Sensor Network

1. INTRODUCTION

Wireless sensor networks (WSN) are composed of tiny sensors each of which has limited computational capabilities, a limited and generally non-renewable energy source, and a small communication device attached. WSN can be particularly useful in applications that require periodic monitoring for some events of interest. Some of the most common applications of WSNs are habitat monitoring, intrusion detection, forest fire detection and chemical contamination detection.

The major expectation from a WSN is to provide its functionality for a specific period of time, generally as long as possible, with a certain degree of accuracy. One of the main causes for failure in WSNs is the limited battery of the sensors which is mainly consumed for radio communication [1].

Border surveillance is one of the most prominent applications where WSNs have found usage. In this kind of applications, the WSN is configured to monitor a given area against intrusion. Sensors are deployed over the field-of-interest (FoI) represented as a long narrow strip. The sensors are expected to sense the area and report their detection decisions to a data collection center (sink). The WSN is considered functional if the surveillance quality of the network is above a certain level.

Surveillance quality is related to the ability of sensors both detecting the intruders and reporting their detection decisions to the sink. The surveillance quality of the system is also related to the network coverage provided by the sensors, which is called the deployment quality. The temporal resilience of the deployment quality has been analyzed in [2] using the watershed deployment quality measure (WDQM) described in [3] for different intruder characteristics.

One of the problems faced in border surveillance applications, and more broadly in many-to-one WSNs is the uneven energy consumption [4]. The large number of sensors reporting to a single data collection sink exposes the sensors around the sink

to a higher traffic load. This causes the energy at these nodes to be consumed more rapidly. The nodes around the sink begin to die off and the sink becomes unreachable to other sensors in the network. This is known as the energy hole problem in wireless sensor networks [5]. Mitigation of the energy holes is crucial to extend the network lifetime in surveillance applications of WSNs.

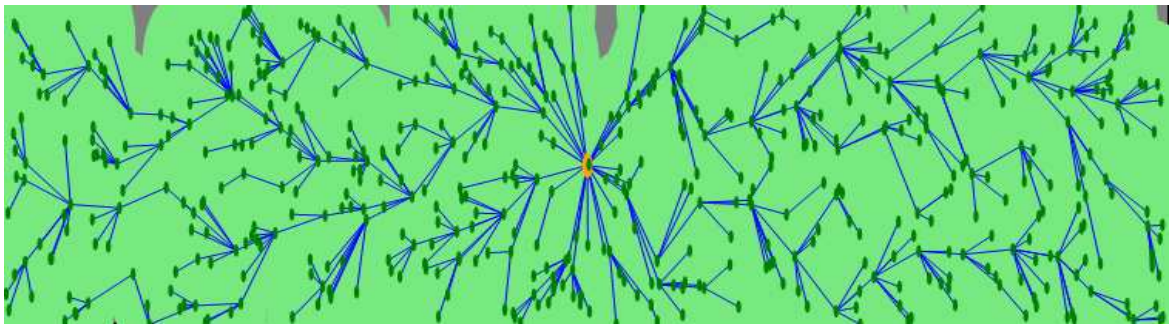
Three kinds of problems caused by exhausted nodes are shown in Figure 1.1. Initial network status where all the nodes are alive is shown in Figure 1.1 (a). The first problem is the network partitioning (one part of the network may become disconnected from the sink) as shown in Figure 1.1 (b). The second problem is the formation of breach paths through which the intruder may pass undetected as shown in Figure 1.1 (c). The path between the two bold vertical lines shows the path through which the intruder may pass with the minimum probability of being detected. The third problem emerges in cases when the sink becomes unreachable to the network although the sensing quality of the network may be above the required level as shown in Figure 1.1 (d).

Nodes that are living and connected to the other parts of the network are shown by • marks. Nodes that have consumed all their energy are shown by ▲ marks, and ■ marks represent nodes that have not consumed all their energy yet but are not connected to the network.

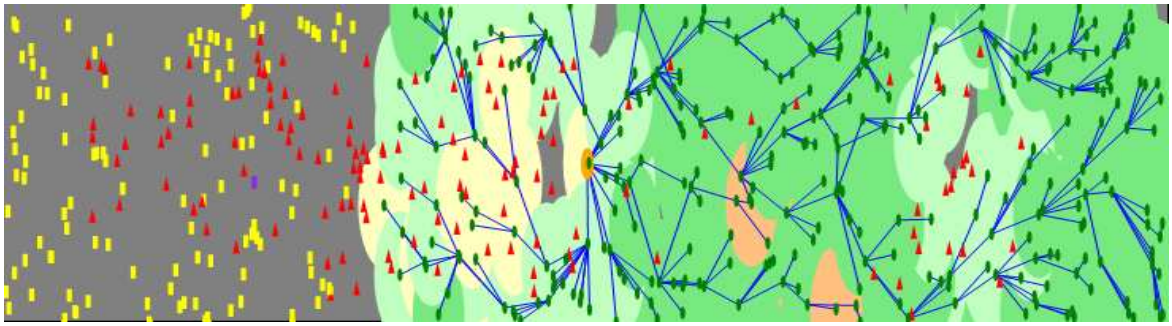
In this thesis, we measure the performance of three different approaches used to mitigate the energy hole problem in surveillance wireless sensor networks. We evaluate the surveillance quality of the network over time for different network configurations and mitigation strategies. We implement our simulation model based on realistic MAC and routing layers and perform our simulations using OPNET discrete event simulator [6]. S-MAC [7] is chosen as the MAC layer due to its energy efficiency. Min-Hop routing is chosen as the routing layer due to its simplicity and ability to balance the network load in the long run [8]. The techniques that we analyze in this work are data aggregation using a time window, sensor redeployment and neighborhood density control. For each of the techniques, we analyze the effects of the related key parameters

and discuss the results. Moreover, we combine the proposed techniques and analyze the results of the proposed hybrid strategies. All of the approaches try to increase the network lifetime without impacting the sensing quality of the network.

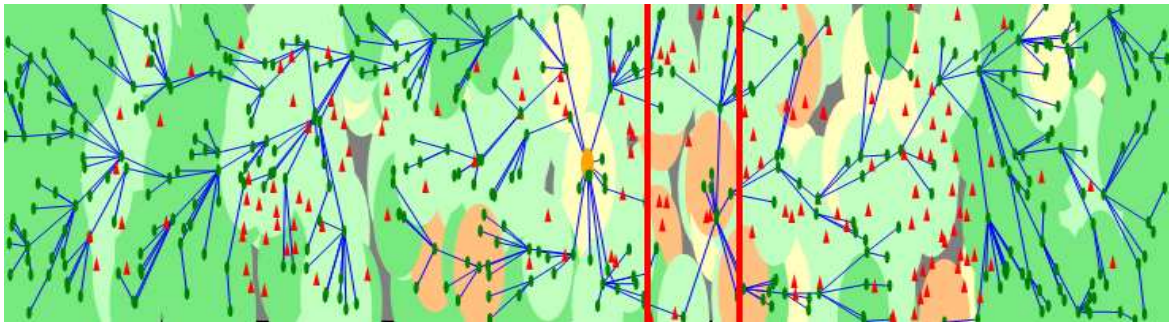
The rest of this thesis is organized as follows. In Section 2, we present a literature survey on the energy hole, coverage and lifetime maximization problems. In Section 3, we describe the proposed strategies for mitigating the effects of the energy hole problem. Then, we present the system model and simulation parameters in Section 4. The results of our simulations are presented in Section 5. Finally, we present the conclusions and future work in Section 6.



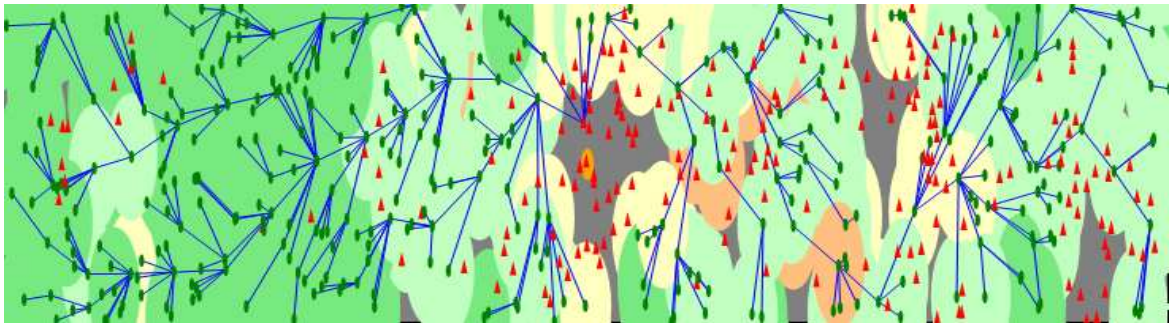
(a) Initial network state



(b) Left part of the network becomes disconnected



(c) Formation of a breach path



(d) Sink becomes unreachable

Figure 1.1. Problems caused by exhausted nodes

2. LITERATURE SURVEY

Border surveillance applications are generally used to monitor a given area for intrusion detection. In these applications, a large number of sensors are deployed over the area which is generally in the form of a long narrow strip. The wireless sensors are expected to sense the area and report the information to a main data collection sink. The system is considered to be still functional if the intrusion detection probability is above a certain threshold level over all the area of the system. Intrusion detection depends not only the ability of the sensor to sense the intruder, but also the ability to report the intrusion to the data collection sink.

Due to the properties of the many-to-one architecture used in these networks, the wireless nodes in the proximity of the data sink will act as a relay between the sink and the other nodes in the network. A higher load on these nodes will cause faster battery depletion. In this way, the relay between the data sink and the wireless sensors will be destroyed and the whole system will become useless. This problem is known as the energy hole problem in wireless sensor networks and is crucial to the network lifetime in border surveillance applications.

Jamming is another important issue in wireless sensor networks. Jamming is an external signal that may be introduced by the intruder in order to impair the network functionality. The jammer may occupy the transmission channel at all time, at random time intervals, or only during transmission periods so that the nodes cannot communicate with each other. Moreover, the jammer may be static or moving in some direction. Although the sensors may have detected the intruder, they cannot report the intrusion detection to the sink in the presence of a jamming source. JAM is a protocol for handling jamming holes that has been proposed in [9]. The network tries to identify jammed regions and reconfigure itself so that packets are not routed over that region. The protocol relies on the assumption that the nodes in the jammed region can notify the nodes in the clean region about the jamming. This assumption may not be hold if the nodes have only one communication channel and the jamming is continuous.

There have been various analysis and models for the energy hole problem but often incomplete. In [4], an analytical model for the energy hole problem is presented, the results show the energy consumption rates of the nodes as a function of the distance from the data sink. It is true that the nodes near the sink have higher energy consumption, but the model is very simple and assumes that constant bit rate (CBR) data is sent from each node and nodes are uniformly distributed. It also shows that hierarchical deployment reduces the energy consumption of the nodes near the sink.

A modeling for the energy hole problem is presented in [10] but it assumes mobile sources and sinks which is not very realistic in wireless sensor network deployments where even energy required for communication is to be reduced. The proposed model mostly prevents the formation of holes by keeping both sources and sinks in constant movement so that energy consumption is not concentrated in a single region, however neither the complexity of a suitable routing protocol for this scenario nor the energy efficiency of the proposed solution have been analyzed.

The uneven energy consumption observed in many-to-one sensor networks is analyzed in [11]. It is shown that for energy consumption models having path loss value of 2.0, there is no routing strategy that can avoid the energy hole creation around the sink. When hole formation cannot be avoided, routing protocols try to forward packets along hole boundaries. The nodes on the hole perimeter start to die out faster due to increasing traffic and thus the hole diameter gets even larger, which is known as the hole diffusion [5] problem.

What makes it difficult to deal with holes in border surveillance applications is that generally we do not want to just route around holes, but prevent the holes from appearing in the first place. Moreover, holes are to be prevented at the least energy cost, and incurring little or no additional complexity to the routing protocol. Another important problem in border surveillance applications is the determination of the optimal number of data sinks that should be placed in the network and the optimal sink positions. This problem further depends on other network parameters such as the expected sensing quality and the required network lifetime of the sensor network.

There exist various proposed algorithms [12] and protocols for the minimization of energy consumption or hole avoidance in wireless sensor networks. These solutions directly or indirectly affect the appearance time and diffusion rate of holes in WSN. Each of the approaches generally based on some common and not always correct assumptions such as the *unit disk model* and the *flat world model* as described in [13]. Most of the approaches try only to minimize the energy consumption within the network without considering the resulting network performance or sensing quality. These approaches are adaptive duty cycling and data reduction. Energy holes cause nonuniform coverage and decrease the sensing quality of the network. They can be avoided by trying to balance energy consumption in the network or trying to maintain uniform coverage.

The adaptive duty cycling method is based on the idea that there is no need to keep all the sensors on when the sensor density in a given area is large enough. Therefore, nodes in a given area are allowed to sleep for a predefined period of time, and then wake up to sense the environment or switch duties with neighbor nodes. Special attention is paid to make sure that the given area is always covered by the non-sleeping sensors. Another form of reducing the communication costs is to equip the wireless sensors with two radios, one low power wakeup radio [14], [15] and a transmission radio. In this way the costs for wakeup and sleep signaling are further reduced.

Reducing the energy costs of the sensor nodes only delays the formation of energy holes since the flow pattern in the network does not change. These approaches cannot completely solve the problem but can help delay hole formation and increase the network lifetime. Some protocols that use similar approaches are S-MAC [7], ASCENT [16], and STEM [17]. These protocols consider the energy efficiency of the sensor network but the impact of energy saving on the overall network performance is not considered. A comprehensive study of medium access protocols is given in [18].

The data reduction method is based on the idea that the data sensed from neighbors in a given area is likely to be highly correlated [12]. It is possible to design

protocols that exploit the spatial and temporal correlation of the data. In this way only the valuable data are selected for transmission and transceiver usage frequency is decreased. One of the methods used for data reduction is directed diffusion [19]. Directed diffusion may delay the appearance of holes in the network and increase network lifetime, but it cannot prevent or heal energy holes. An approach for data aggregation based on a dynamic tree structure is proposed in [20]. The tree root responsible for the aggregation process is chosen based on the energy level of the nodes in the neighborhood. A solution to the hole diffusion problem is given by [21] which tries to avoid holes before meeting them. This approach may delay the enlargement of the hole but may cause another hole on the alternate path in the network. Moreover, the proposed solution is not very applicable to many-to-one network topologies where avoiding the hole may mean avoiding the data sink.

Dynamic clustering is proposed in [22] as a self-deployment method for wireless sensor networks. Dynamic clustering is based on the assumption that mobile nodes exist within the network and can position themselves to locations of low node density to heal the network. This approach can mitigate the energy hole problem but availability of mobile nodes in the network may not be always possible.

The authors in [23] propose a self deployment technique for mobile sensors based on potential fields to achieve uniform coverage through the network. This approach has been shown to provide good coverage and can be used to maintain sensing quality above critical values but is not applicable in the case of static sensors. Another self deployment algorithm for maximizing three dimensional coverage of underwater surveillance sensors is proposed in [24]. Underwater sensors are equipped with multiple sensors and a data mining algorithm is used for the target classification.

A binary integer programming approach for effective sensor placement when there exist various sensor types with different sensing quality and cost is proposed in [25]. It is also suggested that the usage of a probabilistic approach in cases when calculation of effective positions is not feasible. Another algorithm that addresses placement of sensors for effective coverage is proposed in [26]. The algorithm has polynomial

time complexity, optimizes the number of sensors and determines the sensor positions. Moreover, the algorithm assumes imprecise sensor detections and takes into account terrain properties. In [27], an algorithm for density control in which sensors decide whether to participate in the network by using the incoming packet information is proposed. This approach can be helpful in reducing the network traffic and minimizing the overhearing.

In [28] the authors propose a sensor redeployment method that can be used to mitigate sensing holes. Initially only a portion of the available sensors are deployed and the rest are spared. Whenever a hole emerges in the network, sensors are redeployed over poorly covered regions to maximize the deployment quality of the network. The deployment quality is measured using the techniques proposed in [3]. Networks using the proposed redeployment technique achieve better sensing quality than networks using the same total number of sensors at once. However, the effects of redeployment on the network lifetime are not considered.

One form of measuring the deployment quality in surveillance wireless sensor networks (SWSN) is the *path exposure* concept proposed in [29]. The authors define exposure as the amount of energy emitted by the target that is received by the sensor. The energy received by the sensor is compared to a minimum threshold to decide whether the target can be detected. The path exposure is defined as the amount of energy received by the sensors along the intruder path. To calculate the paths with minimum exposure the authors also describe algorithms using Voronoi diagrams and Delaunay triangulation. The path with minimum exposure is the path where the intruder may pass with low probability of being detected and defines the quality of the deployment. The authors in [30] use the path exposure concept as a measure of the deployment quality and propose an algorithm for random sensor deployment that maximizes the deployment quality of the network by using sequential deployment steps. Since every deployment step and every sensor has a cost, the authors develop an algorithm that tries to achieve the desired deployment quality at minimum cost. Moreover, the authors in [31] extend the deployment algorithm to take into account for obstacles.

An energy efficient algorithm for random sensor deployment which takes into account for the quality of monitoring and network lifetime constraints is proposed in [32]. The quality of monitoring of the network represents the similarity between the actual value and the measured value of some event in the region of interest. The algorithm considers only the spatial distortion of the measured event for calculating the quality of monitoring. This metric can be suitable for networks that monitor and periodically report information such as temperature. In applications such as intrusion detection the information provided by this metric is not very important and cannot be used to measure the quality of monitoring of the system.

Other forms of reducing the energy consumption of wireless sensors include designing intelligent routing algorithms that can send a packet to a given destination using the least amount of energy or using an optimal amount of energy while considering the remaining available energy of the nodes. Some routing algorithms include GPSR [33], GEAR [1] and RTLD [34]. GPSR tries to route a packet using the minimum energy and thus can cause hole diffusion. On the other hand, GEAR and RTLD consider the level of energy at each node thus delaying hole creation. Both of the above protocols do not consider directly the energy hole issue.

In some cases, hole formation may be the result of intentional node destruction. An information theoretic approach for detecting systematic node destructions is proposed in [35]. This can be helpful in detecting intrusions which cannot be sensed by the sensors.

When designing a border surveillance application there are a number of factors that should be considered to make the application more realistic and functional. These factors include choosing the kind of sensor to be used and the sensing probability function. Before deploying the sensors some decisions about the MAC and routing layers to be used must be made. Afterward, the way in which the sensors will be deployed must be decided. This may be aerial, human, or robot assisted deployment. After the deployment, an assumption about the sensor density function must be made. The sensor density may be uniform or not.

Finally, there must be a monitoring system such as eScan [36] or digest [37] which will report the state of the network at any time and gather the surveillance information. A detailed survey on WSN and design factors is presented in [38]. Some surveillance quality measures similar to the ones proposed in [3] must be calculated to keep the desired security level in the border surveillance.

3. ENERGY HOLE MITIGATION STRATEGIES

3.1. Introduction

In a surveillance system, a FoI is to be monitored against unauthorized intrusion. We model the SWSN as a number of fixed sensor devices randomly deployed over a FoI. Sensors monitor the area and send intrusion detection information to the sink which is placed at the center of the field as shown in Figure 3.1.

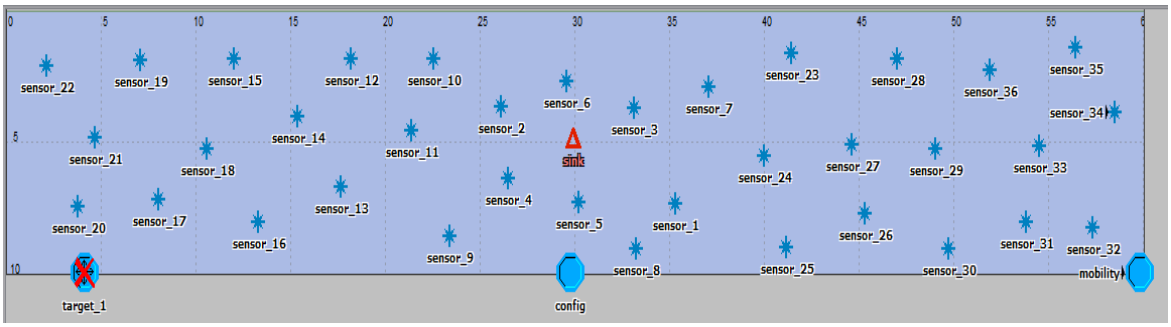


Figure 3.1. Sample OPNET simulation scenario

In this thesis, by the network lifetime, we mean the period of time over which the network is functional and the surveillance quality provided by the system is above the minimum level allowed. The network is considered to be functional if the provided surveillance quality is above the minimum level allowed. To increase the lifetime and the surveillance quality in border surveillance applications, we need to cope with the energy holes that may form. There exist two dominant approaches that try to minimize the energy consumption within a WSN. The first one, which is called as *adaptive duty cycling*, aims to reduce communication costs by keeping the transceiver of the node off as long as possible without affecting the network functionality. The second approach, which is also called as *data reduction* or *in-network processing*, tries to reduce communication costs by transmitting only useful data to the destination.

While minimizing energy consumption can significantly extend network lifetime, formation of holes cannot be always prevented. In these cases, the network should

be repaired periodically to maintain its functionality. The most common approaches for repairing a WSN are sensor redeployment and long term scheduling. Since trying to extend the network lifetime and trying to increase the surveillance quality of a WSN are two conflicting goals, we propose different strategies that have good effects in maximizing one of the goals and then combine these strategies to obtain solutions that are optimal for a given WSN application. In the following sections, we first describe the method used for calculating the surveillance quality of the WSN and then present the strategies that we propose for reducing the energy consumption and mitigating the effects of the energy hole.

3.2. Surveillance Quality Calculation

To quantify the security level provided by the network, we use the watershed deployment quality measure (WDQM) presented in [40]. Before describing the WDQM calculation method we will first describe the sensing model assumed for each sensor.

3.2.1. Sensing Model

Sensor's detection ability is modelled probabilistically as defined by Elfes [39]. The probability of a sensor detecting a target at a distance d is

$$p_{(detection)} = \begin{cases} 0 & \text{if } d \geq r + r_e, \\ e^{-\lambda \alpha^{\beta}} & \text{if } |d - r| < r_e, \\ 1 & \text{if } d \leq r - r_e, \end{cases} \tag{3.1}$$

where $r_e < r$ are the thresholds for the sensing distance, d is the distance between the sensor and the target and $\alpha = d - r + r_e$. The parameters λ and β can be used to model sensors with different sensing characteristics. The detection probability for a sensor with parameters $r = 20$, $r_e = 5$, $\beta = 0.9$ and $\lambda = 0.1$ is shown in Figure 3.2.

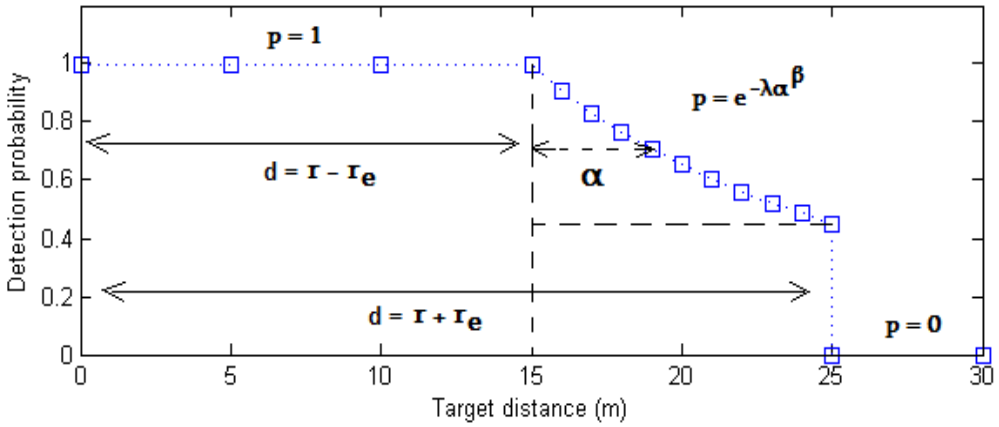


Figure 3.2. Elfes's probabilistic detection model

The binary detection model can be treated as a special case of the Elfes's probabilistic detection model with $r_e = 0$. Binary detectors can detect any target at a distance $d < r$ with probability one and cannot detect anything that is beyond r. Since a given point in the network can be covered by more than one sensor at a time, the detection probability at that point is calculated as maximum of the detection probabilities of the sensors.

3.2.2. WDQM Calculation

By modeling the field as a two-dimensional grid and adding the detection probability as the third dimension, we obtain a three dimensional surface which shows the sensing graph of the network [40]. A sample sensing coverage graph and the detected breach path are shown in Figure 3.3.

The WDQM calculation method is based on watershed segmentation algorithm [41]. The three dimensional sensing map is firstly inverted and then water pumps are used to fill the resulting valleys. The remaining hill contours show the breach paths of the network. The WDQM is the minimum of the maximum detection probabilities of these contours and gives an insight about the security level provided by the network.

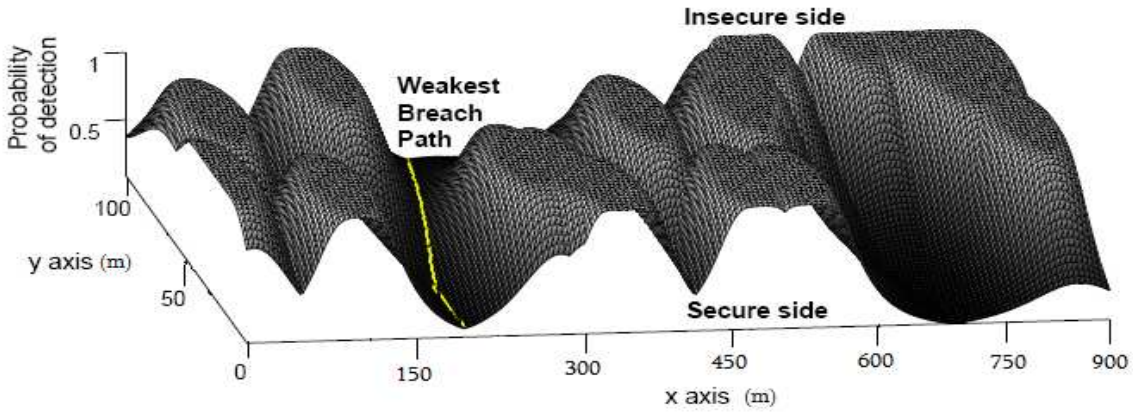


Figure 3.3. Network sensing coverage and brach path detection

Another way of calculating the minimum of the maximum detection probabilities is to use the Dijkstra's shortest path algorithm. The surveillance field is divided into one meter by one meter squares and the maximum detection probability available on each square is calculated. One fictitious starting point is added to the insecure side of the border and a finish point is added to the secure side of the border. The shortest path algorithm is then applied to find the path where an intruder may pass with minimum probability of being detected.

3.3. Sensor Redeployment

During the operational lifetime of a WSN, several regions of the network may become uncovered due to intentional node destructions, weather conditions or uneven energy consumption. To maintain the required quality of surveillance, uncovered regions should be repaired. One way of repairing weak or empty regions is by deploying additional sensors to those sites when needed. In our sensor redeployment strategies, we spare a portion of the sensor budget and use it in emergency cases to repair damaged regions. This technique is known as sensor redeployment.

Another reason for using sensor redeployment is to minimize the deployment cost and maximize the coverage provided by the available sensors. The deployment cost

is minimal when all the sensors are deployed at once, but this does not result in the best possible coverage and uses all the sensors. On the other hand, to use the smallest number of sensor to cover a given region sensors may be deployed one by one until the required coverage level is reached. However, this incurs an additional cost for each deployment step. To achieve an acceptable coverage and deployment cost, several things such as the cost of each deployment step and the cost of each sensor must be taken into consideration. In this study, we assume that the deployment cost is higher than the benefit of sparing some sensors. For this reason, we use only two deployment steps.

There are several methods of achieving the desired deployment depending on the application terrain and size. For large scale WSNs aerial deployment can be a suitable choice. On the other hand, deployment by small vehicles is more effective for deployments over small sites. In cases where large scale deployment and repairing of small regions are required, a combination of both options as shown in Figure 3.4 can be used.

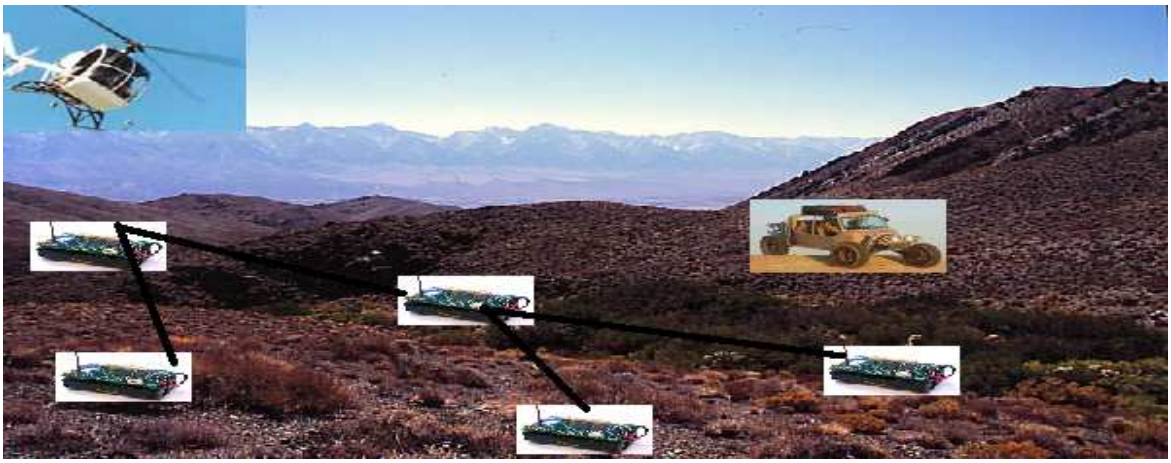


Figure 3.4. Sensor deployment by different vehicles

We propose different redeployment strategies that may be used for mitigating hole effects and increasing the quality of surveillance in WSNs. This work assumes two deployment steps: an initial mass random deployment step and a redeployment step that positions remaining sensors according to the redeployment strategy used. We

started our redeployment strategies from the most intuitive ones and then optimized or combined them to obtain more powerful strategies. The redeployment strategies we propose are: random redeployment, MaxDQM redeployment, hybrid redeployment, adaptive hybrid redeployment and proactive redeployment.

In the following sections, we describe the motivation behind each mitigation strategy and discuss their implementation costs, effectiveness in extending the network lifetime and ability to maintain the required surveillance quality. We also discuss some further optimizations that can be done over the proposed strategies.

3.3.1. Random Redeployment

We propose a redeployment strategy that deploys initial sensors randomly and redeploys spare sensors in a random fashion when WDQM value falls below some threshold value. The effect of this strategy is similar to deploying all the sensors at once but activating only a portion of the sensors until the surveillance quality drops below the threshold value.

The strategy is expected to have good results in scenarios where deploying all the sensors at once would just increase the sensor density and thus increase packet collisions and retransmissions. By leaving a portion of the sensors for latter redeployment, we avoid unnecessary density of operational sensors and reinforce the network with new sensors only when needed.

Random redeployment is more suitable for scenarios where sensors fail independently or the region to be covered is large and precise deployment would be too costly. Random redeployment has the disadvantage of deploying a considerable portion of the spare sensors on unnecessary regions in cases where node failures are correlated and located on a small number of sites. This makes random redeployment ineffective in covering damaged regions and thus increasing the sensing quality.

3.3.2. MaxDQM Redeployment

Correlated node failures cause void regions in particular areas of the network. This may be caused by intentional node destruction or due to the energy hole problem. To repair these void regions, aerial node deployment may not be effective and a more precise deployment approach such as vehicular deployment should be used. To cover void regions where intruders are highly probable of passing undetected we implement the redeployment strategy proposed in [28].

The strategy detects the regions that have lower sensing quality and need reinforcement. The detected regions are generally areas in the network where nodes are exhausted or intentionally destroyed. The algorithm decides how many remaining sensors will be deployed over each of the weak regions detected so that the overall WDQM is maximized. To detect the poorly covered regions the algorithm constructs a map of the detection probabilities of the sensors on each point as shown in Figure 3.5. Paths of lower intensity represent areas where the intruder may pass with minimum probability of being detected.

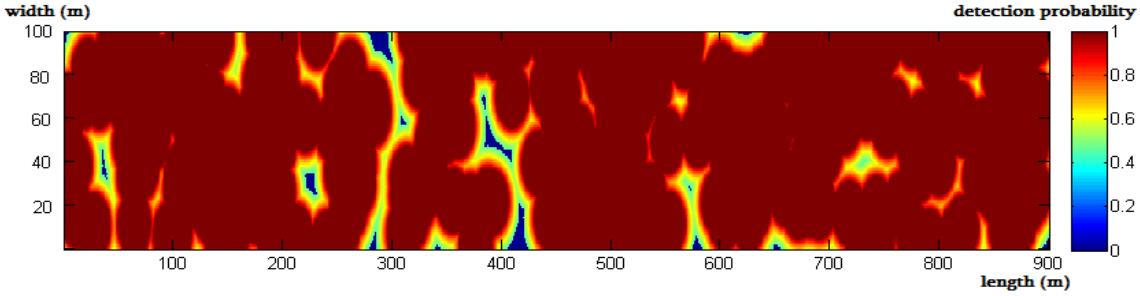


Figure 3.5. Detection probability map

The redeployment step is performed when WDQM value falls below some threshold value. This redeployment strategy will be called the MaxDQM redeployment strategy. We should note that this strategy has higher precision and requires less sensors for covering a void region compared to the random redeployment. However, we should carefully consider the tradeoff between the benefit of using less sensors and the cost of vehicular deployment.

The MaxDQM strategy is very effective in maximizing the WDQM of the network with the given number of spare sensors. Moreover, this strategy can extend the network lifetime by repairing void regions and stopping hole diffusion. However, MaxDQM strategy will not be able to prevent the appearance of new holes nearby the repaired regions where sensors may have been weakened by the hole diffusion phenomenon.

3.3.3. Hybrid Redeployment

To benefit from the combined effect of the two redeployment strategies described above, we propose a redeployment strategy that redeploys a portion of the spare sensors using MaxDQM strategy and the remaining part using random redeployment strategy. The mixed strategy will be called hybrid redeployment strategy.

The hybrid redeployment strategy is expected to give better results than each of the strategies separately since it covers weak regions and also reinforces the whole network by random redeployment. This strategy can be tuned to provide larger network lifetime and sensing quality by finding the optimal ratio of the sensors to be deployed by each strategy. The most straightforward hybrid redeployment strategy is to divide spare sensors into two halves and deploy them using the respective strategies. In terms of cost, the strategy can be more expensive if the random redeployment part is performed by aerial means and the MaxDQM redeployment part is performed by vehicular means. The strategy can become cheaper and more effective if both random and MaxDQM redeployment are performed by vehicular means.

3.3.4. Adaptive Hybrid Redeployment

The MaxDQM redeployment strategy uses a static approach to determine the amount of spare sensors to deploy at each redeployment step. However, depending on the size and number of holes in the network, different number of sensors may be required for repairing the network. If the number of sensors required for covering a void region could be dynamically calculated, we could increase the efficiency of deployed sensors for covering holes.

We propose a dynamic method for calculating the number of sensors needed to cover a void region by MaxDQM redeployment strategy. We integrate this approach into the Hybrid redeployment strategy. In this way, instead of dividing the spare sensors in two halves and using the hybrid redeployment strategy, we implement a more adaptive technique that decides the number of sensors that should be deployed using MaxDQM redeployment strategy and deploys the remaining sensors using random redeployment strategy.

This redeployment strategy enables us to use just enough sensors to maximize the surveillance quality and use the remaining spare sensors to reinforce the overall network structure. From the cost point of view, this strategy has similar cost to the hybrid redeployment strategy.

3.3.5. Proactive Redeployment

To detect holes formed in a network, we classify the sensors as living or exhausted. The hole is seen as a cluster of exhausted nodes where redeployment should be made. Nodes in the hole boundary are generally the next candidates for being exhausted due to the hole diffusion phenomenon. The MaxDQM redeployment strategy detects void regions in the network and performs redeployment over those regions.

Note that the MaxDQM redeployment strategy uses a snapshot of the current network status for calculating node deployment positions. Instead, if we use a snapshot of the expected network future status for calculating current sensor deployment, we can prevent formation of some holes. In the simplest approach, future hole positions can be predicted by looking at the current sensor conditions such as energy levels and energy consumption rates.

To prevent future hole formation in a region where sensors are going to be redeployed, we propose a proactive redeployment approach. The approach considers nodes that have less than E_{min} remaining energy as exhausted since they are going to be exhausted in the near future. To detect potential void regions, the strategy uses the

same approach as the MaxDQM strategy but uses an energy map as shown in Figure 3.6 to classify sensors as living or exhausted.

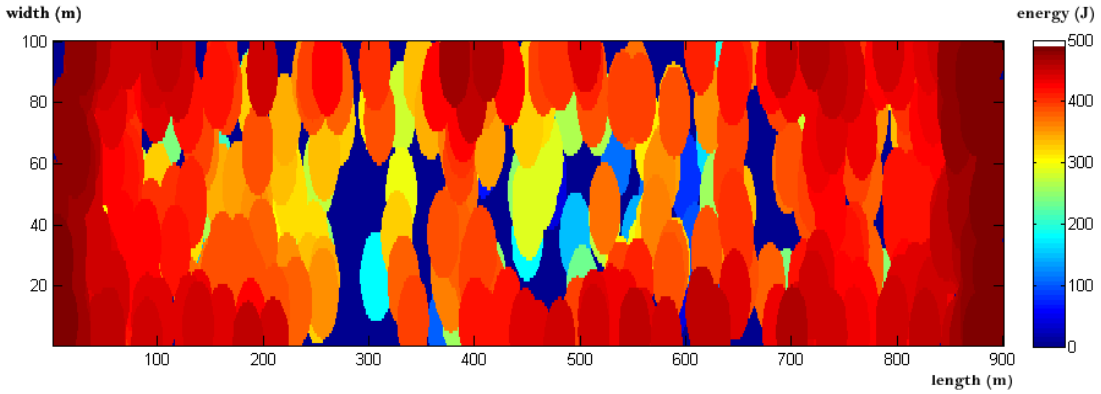


Figure 3.6. Energy map

This strategy will make it more difficult for holes to appear in the same region in the future since deployment will be made over a wider area covering also the sensors that are about to be exhausted. Moreover, the strategy also causes node deployment over regions where there is not any hole yet but a hole is expected to appear. The proactive redeployment strategy is expected to give longer network lifetime and better sensing quality compared to the MaxDQM redeployment approach. In terms of redeployment cost, the strategy has similar cost to the MaxDQM redeployment strategy.

3.4. Packet Aggregation for Overreporting Avoidance

In SWSNs the data sensed from neighbor sensors in a given area is likely to be highly correlated [12]. All sensors in a given neighborhood will report the same intruder at the same time and at approximately the same position. Moreover, the intruder is assumed to be moving and the sensors along the intruder path will also report the intruder after a small period of time. Since SWSNs are generally required to only report the presence of the intruder with some approximate time and location information, it is possible to design protocols that exploit the spatial and temporal correlation of the data. In this way, only the valuable new information is transmitted and transceiver usage is decreased.

There are two common approaches for information fusion, known as *value fusion* and *decision fusion* [42]. In the value fusion approach, all the gathered information about a local event is processed from a single node and a decision is made based by comparing aggregated value of the event to a reference value. The decision fusion approach each node makes a decision about the measured event by comparing its value to a reference value, then all the decisions are gathered and processed from a single node which makes the final decision by comparing the aggregated decisions to a reference value.

By exploiting the correlation between the target detection packets, we can avoid reporting the same information to the sink continuously. We propose a packet aggregation approach for avoiding overreporting of target detections. Our aggregation approach uses a time window for grouping transmitted packets. All the packets arriving to a sensor within a time window are considered to be temporally correlated and are replaced by a single equivalent packet. The first arriving packet in the window is forwarded toward the sink, while the latter packets in that group are blocked. Our approach can be considered as a decision fusion approach since all the sensors make local decisions about target detection while the relay sensor fuses the detection information and forward only one detection packet to its neighbor.

This approach decreases the network traffic and also limits the amount of delay caused by the aggregation process since the first detection report in a time window is immediately forwarded to the sink while other reports from the same neighborhood are discarded. The aggregation approach is expected to significantly reduce energy consumption in SWSNs and delay the formation of holes and extend the network lifetime. In terms of implementation cost, the strategy's cost is completely dependent on the deployment strategy that will be used.

Notice that our SWSN model assumes that intruders enter the border only one at a time, but there can be more than one intruder in the network at any given time depending on the intruder speed and interarrival period. Otherwise, the aggregation approach may discard detection reports about different intruders that come to a relay

node at the same time. To avoid such situations, the aggregation approach should be modified to analyze packet contents before aggregating them. One simple aggregation rule may be that only detection report packets coming from sensors that are not further than twice their sensing distance from each other may be aggregated.

3.5. Neighborhood Density Control for Overhearing Avoidance

A significant portion of node's energy is wasted due to overhearing. That is, receiving packets that are destined to another node in their proximity. In the tree structure of the SWSN network in Figure 3.7, we notice that many sensors that are at the leaves of the tree are connected to the same parent. These are the areas where the overhearing effect is felt the most.

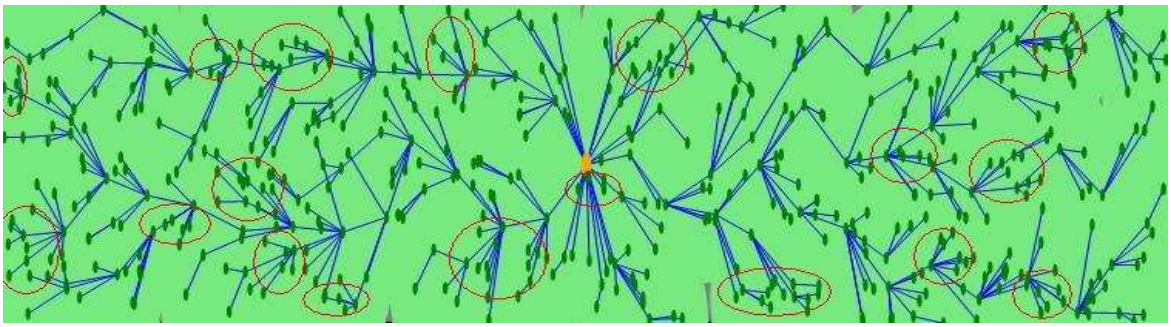


Figure 3.7. Main overhearing regions

To alleviate the effects of overhearing, we propose an algorithm for locating regions with crowded leaf nodes and putting some of these nodes to long term sleep. This strategy will be called neighborhood density control (NDC). After all sensors have discovered their neighbors and have chosen their relays, the NDC algorithm is performed in a distributed fashion. Every node that is at the leaves of the routing tree reports itself to its relay, which is the parent node in the tree. The parent decides if the leaf node will be active or sleeping by checking the current neighborhood conditions.

In order for a leaf node to become active, the parent-leaf distance must be larger than the minimum parent-leaf distance, the current number of leaves must be less than the maximum number of leaves per parent and the leaf-leaf distance must be greater

than the minimum leaf-leaf distance. When the WDQM value of the network drops below the threshold value the NDC conditions are modified in order to allow a larger number of active nodes and increase the sensing quality. Since leaf nodes are not used as relay by any node, putting these nodes to long term sleep does not affect other nodes.

This strategy is expected to significantly decrease the number of packets received by each node. This will directly affect the energy consumption rate of the sensors which in turn will extend the network lifetime and delay the formation of energy holes. In terms of implementation cost, the cost of the NDC strategy depends on the deployment approach used. It is important to notice that the NDC parameters used for choosing active leaf nodes must be carefully tuned in order to maintain the required network coverage.

3.6. Strategy Combination Possibilities

The energy hole mitigation strategies described above fix different causes of energy consumption and repair holes using different approaches. Some of these strategies can be combined to form double or triple strategies as shown in Table. 3.1. If two strategies can be combined with each other, the corresponding cell is marked with + sign or with - sign otherwise.

Table 3.1. Combinations of energy hole mitigation strategies

	Random	MaxDQM	Adaptive	Proactive	Aggregation	NDC
Random		+	-	-	+	-
MaxDQM	+		+	+	+	-
Adaptive	-	+		+	+	-
Proactive	-	+	+		+	-
Aggregation	+	+	+	+		+
NDC	-	-	-	-	+	

To further optimize the number of sensors placed on each deployment site and their effectiveness, we can combine the adaptive and proactive redeployment strategies to form a double strategy. In this way, we obtain a strategy that is similar to the hybrid redeployment strategy from the cost perspective but has many additional advantages in terms of network lifetime and sensing quality. Moreover, the new strategy can be combined with the aggregation strategy to form a new triple strategy.

3.7. Proactive Redeployment Optimization Possibilities

Prediction of the network status at a future time is important for the Proactive redeployment strategy. One way of predicting the lifetime of the sensors is to use their current energy level and classify sensors below a certain energy level as exhausted. However, this approach may not be always correct since it does not consider the time when the sensor started working from which we can deduce the average consumption rate of the sensor.

We can construct a more accurate prediction model about the state of the sensors at any given time by including their energy consumption rate. We can extend this concept to define the expected time of exhaustion or remaining lifetime of a sensor. In this way, we can modify our Proactive redeployment strategy to consider sensors that have a remaining lifetime smaller than a given T_{min} to be considered as already exhausted.

3.8. Complexity comparison of proposed mitigation strategies

The mitigation strategies proposed in the previous sections were analyzed from the cost and effectiveness point of view. It is natural to expect that the cost of the mitigation strategies is related to their complexity. We can classify the mitigation strategies into low complexity and average complexity classes. We consider only the difficulty of network setup and maintenance and do not consider the algorithm complexity or the number of CPU cycles into the complexity classification.

We can classify mitigation strategies such as Aggregation and NDC as low complexity strategies since thy do not require any extra effort from the network administrator point of view. Random redeployment strategy can also be considered as a low complexity strategy since it does not require any precise location for deploying the sensors. Other mitigation strategies such as MaxDQM, Proactive and Adaptive can be classified as average complexity strategies since they require precise deployment of spare sensors.

4. SIMULATION MODEL

We define the network lifetime as the time from the initial network deployment until the time when the WDQM value drops below the acceptable level or the sink becomes unreachable. The surveillance quality of the system is calculated in real-time by integrating MATLAB [43] for WDQM calculations inside the OPNET [6] simulation loop. This allows us to monitor the network sensing quality in real time during the simulation. Online WDQM calculations are performed after every node failure. Simulation results are also logged in external files for further offline analysis which can be done using an offline analyzer that we have implemented for this purpose. In the following sections, we describe the components of our simulation model, the software configuration and the integration of MATLAB into the OPNET simulation loop.

4.1. SWSN Modelling in OPNET

The SWSN used in our simulations is modeled in OPNET as a rectangular field with many sensors, one sink and a number of randomly moving intruders that cross the border. The network terrain is considered to be flat and does not contain any obstacles. The model contains five components:

- Wireless sensor
- Sink
- Intruder
- Mobility configuration
- Network configuration

4.1.1. Wireless Sensor Model

The wireless sensor is composed of three main components: the intruder detector, the periodic data generator and the data handler as shown in Figure 4.1. The sink is similar to the wireless sensor except that it has an infinite amount of energy.

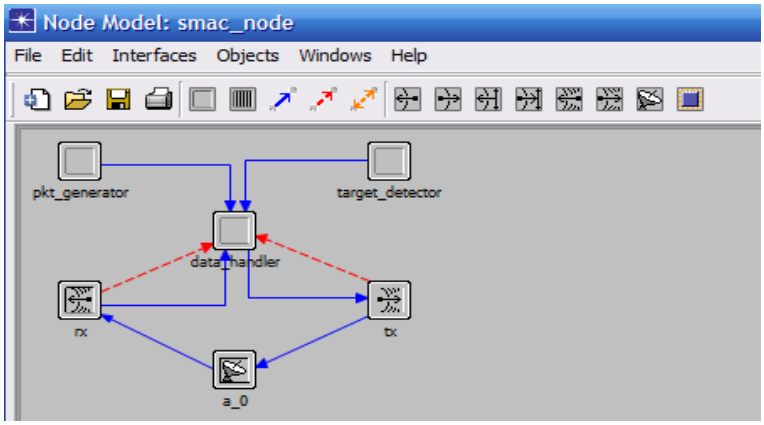


Figure 4.1. OPNET node model for wireless sensor

4.1.1.1. Detector Model. The intruder detector can be configured to work in one of the two available detection models: binary detection model and Elfes's probabilistic detection model. Detector wakes up periodically to monitor its perimeter and reports intruder detections to the data handler component. The periodic data generator component sends sensor health information to the sink. In this way, network health can be monitored periodically and exhausted or destroyed nodes can be deduced.

4.1.1.2. Periodic Data Generator. The periodic data generator component is configured to report sensor's conditions periodically to the sink. The periodic report inter-arrival time follows uniform distribution in order to avoid network congestions. By analyzing the health reports received from each sensor, the sink can calculate the overall network conditions or deduce which nodes have been exhausted or intentionally destroyed.

4.1.1.3. Data Handler. The data handler is composed of the Routing, MAC and Physical Layers. Packets received from the upper layer, which can be intruder detector or

periodic data generator component, are passed through the routing layer in order to decide the packet relay and then put into the MAC queue to wait for their transmission slot. Packets arriving from the physical channel are passed to the MAC layer and processed. If the final recipient of the packet is the data collection sink, the packet is forwarded by the Routing layer. We use the S-MAC implementation provided in [44] with some minor modifications for redeployment and NDC scenarios as our MAC layer. We implement min-hop routing as our routing layer due to its simplicity and ability to balance the network traffic in the long run [8].

4.1.1.4. Energy Consumption Model. In our model, the wireless sensor consumes energy in the following four states: transmission, reception, idle and sleeping. Energy consumed for sensing the environment is not considered since the energy required for this process is very low [45]. The actual amount of energy consumed in each of the states above depends on the sensor circuitry properties such as the current drain of the transceiver and transceiver voltage. In our simulations, we use the sensor properties of the Chipcon CC1000 [46] wireless sensor.

4.1.2. Mobility Model

The intruder is modeled as a mobile object that can be detected by the sensors. Intruder movements are modelled by a linear random mobility model. The intruder starts moving through the network starting from the upper boundary at a constant predefined speed in a forward random direction and periodically changes its direction to a random angle making zig zags. Intruder is not allowed to make backward movements and it is reflected from lateral borders in order to avoid going out of the field.

The mobility parameters of the intruder such as speed, interarrival period, simultaneous intruder count and direction update period are managed by the mobility configuration shown in Figure 4.2.

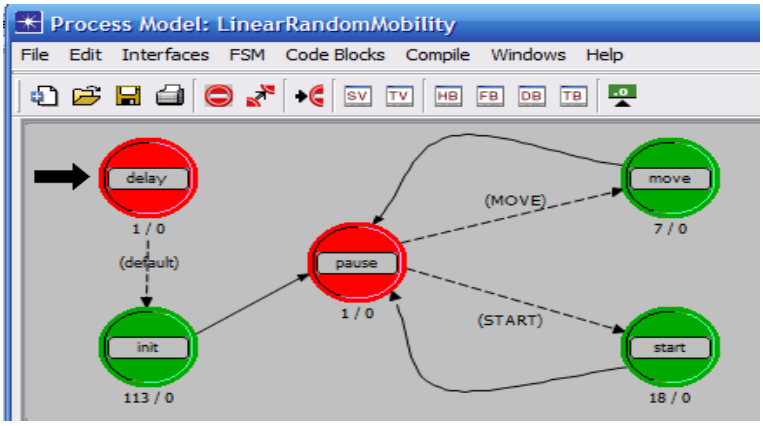


Figure 4.2. OPNET process model for the linear random mobility configuration

4.1.3. Application Layer

The main requirement for a SWSN application is to monitor a given area against intrusions with a certain degree of accuracy. Whenever a sensor is exhausted, the surveillance quality of the system is recalculated. If the surveillance quality of the system drops below the trigger value, countermeasures are taken to improve the surveillance quality of the system. The WDQM feedback loop enables the system to react quickly, thus minimizing the risk of missing any intruders. When a part of the network becomes disconnected, the sink broadcasts a neighborhood update message. All the sensors receiving the broadcast message start advertising their information and update their neighborhood.

Common application configuration parameters such as the WDQM trigger value and the mitigation strategy to be used are managed by the network configuration component as shown in Figure 4.3 .

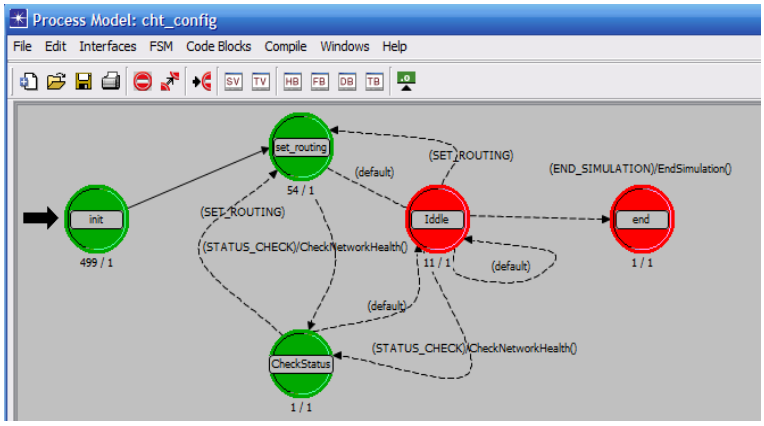


Figure 4.3. OPNET process model for the network configuration

4.2. OPNET Settings and MATLAB Integration

During the implementation of our simulations, we generally used the default compilation and simulation settings provided by OPNET. One of the settings that needed to be changed to get consistent results from different simulation scenarios using the same simulation seed is the random number generator module. In the screen appearing before the simulation execution, we change the Random Number Generator setting found in kernel preferences to "one per module". Otherwise, running another simulation scenario using the same simulation seed may produce different initial sensor deployment. More detailed information about this topic can be found in OPNET FAQ ID: 1327.

One of the most challenging parts of the implementation process was the integration of MATLAB into the OPNET simulation loop. To call MATLAB engine from the C++ code written in OPNET, we must include the following libraries into the shared object libraries (bind_shobj_libs): "libmat.lib", "libeng.lib", "libmex.lib", "libmx.lib". Moreover, the path where MATLAB's external libraries are installed must be included into the shared object flags (bind_shobj_flags), in our case the path is: "C:\MATLAB7\extern\lib\win32\microsoft". More detailed explanation of the integration process can be found in [47] and in OPNET FAQ ID: 1600.

In order to execute the external C++ code files from OPNET, all the files must be of the format "*.ex.cpp"and must be included into the OPNET project by declaring them as external files. In order to debug the OPNET simulations, we used the Visual Studio 2005 [48] C++ debugger. Simulation bugs such as memory leaks were hunted using OPNET commands to show the current packets in the system and IBM Purify [49]. A detailed explanation of the usage of these commands and tools can be found in OPNET FAQ ID: 662 and FAQ ID: 517.

4.3. Offline Simulation Analyzer

To analyze the network behavior through time, we log the network status periodically to a text file. The log file contains the position, energy, relay, number of intruders detected, number of packets sent and received and energy consumed by each sensor at a particular instant. We implemented the offline network analyzer shown in Figure 4.4 to visualize the network state at any time or replay some particular instants.

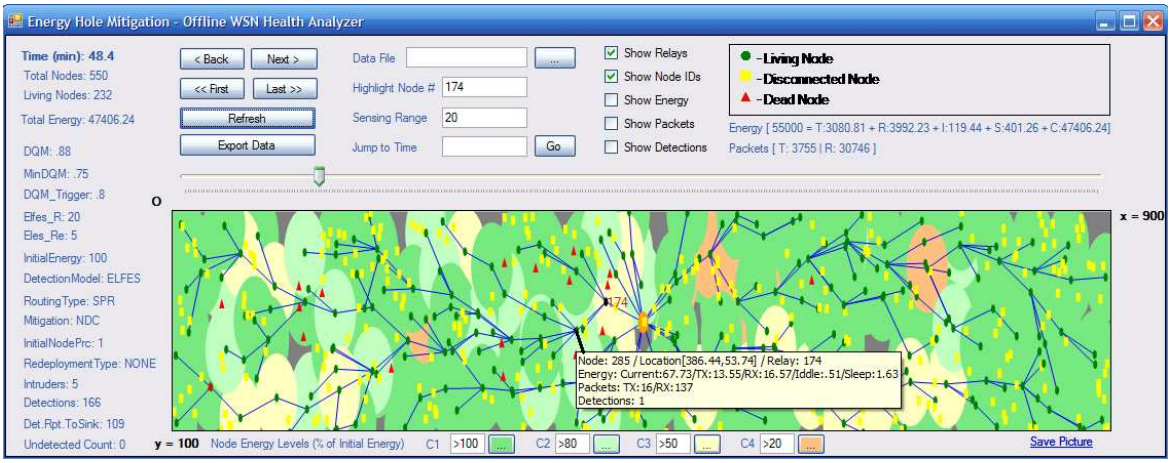


Figure 4.4. Offline simulation analyzer

4.4. Simulation Parameters

In the initial scenario, the network is modelled as a $900 \times 100\ m^2$ rectangle and 550 sensors are deployed in the field. There exists only one sink located at the center of the field. The sensors are not mobile and their positions follow the uniform distribution.

The intruder starts moving through the network starting from the upper boundary at a constant speed of two meters per second in a forward random direction and changes its direction randomly every five seconds. Intruder is not allowed to make backward movements and it is reflected from lateral borders in order to avoid going out of the field. When a sensor detects the presence of an intruder, it sends a packet toward the sink to report the intrusion. Intruder interarrival period is uniformly distributed between 500 and 700 seconds. All the wireless sensors have a sensing range of 20 meters and the maximum communication range of 40 meters.

The radio circuitry is modeled similar to the Chipcon CC1000 radio chip [46]. The S-MAC layer consumes 1.0 μA in idle state and 0.2 μA in sleep state. The receiver consumes 7.4 mA and the transmitter consumes between 5.3 mA and 26.7 mA. The channel data rate is 38.4 *kbps*. S-MAC layer has a duty cycle of two per cent. All the sensors have a sensing interval of 10 sec and use the Elfes's [39] probabilistic detection model with parameters β=0.9, λ=0.1, r=20 m, r_e=5 m. Sensors are equipped with a 3V Li-Ion Cell that can supply 2100 mAh.

In all the simulation scenarios, the total network area is fixed to 900×100 m^2. The system is configured to check the network health status (WDQM measure) at every 120 seconds and the network is considered dead if the WDQM value drops below the minimum value of 0.75 or the sink becomes unreachable. The redeployment process is initiated if the WDQM of the monitored network drops below the threshold value of 0.8 and further redeployment is possible. We study the effect of six main factors on the network lifetime:

- Sensor density
- Detector wakeup frequency
- Intruder interarrival
- Aggregation
- Redeployment
- Neighborhood density control

For each of these factors, we have prepared scenarios using parameter values specified in the following tables. Typical parameters used for the sensor model such as the energy model and detector parameters are shown in Table. 4.1. Other simulation parameters used for S-MAC layer, WDQM calculations and energy hole mitigation strategies are shown in Table. 4.2. Parameters used for intruder mobility modeling are shown in Table. 4.3.

Each of the simulation scenarios is repeated five times and the averages are considered. Simulation duration for the default scenario is about four hours but can vary up to 24 hours for other scenarios. Default parameter values are marked with a star. No intruder was able to cross the border without being detected in any of the scenarios.

Table 4.1. Sensor parameters

Sensor	
Data Packet Size (b)	1024
Buffer Size ($packets$)	10
Periodic Data Reporting (s)	1800
Data Rate (bps)	38,400
Max TX Distance (m)	40
Path Loss Factor	2
Energy	
Initial Energy (J)	100
TX Current (max) (mA)	26.7
TX Current (min) (mA)	5.3
RX Current (mA)	7.4
IDLE Current (mA)	0.001
SLEEP Current (mA)	0.0002
Transceiver Voltage (V)	3
Detection	
Detection Model	ELFES
r (m)	20
r_e (m)	5
β	0.9
λ	0.1
Sensing Interval (s)	2/5/*10/15/20

Table 4.2. Network parameters

Network	
Dimensions X x Y (m^2)	900x100
Number of Sensors	450/*550/650/750/850
Routing Type	Min-Hop
MAC Type	S-MAC
Mitigation Strategy	None/Redeployment Aggregation/NDC
S-MAC	
Setup Duration (s)	10
Duty Cycle Percentage	2
WDQM	
WDQM_Trigger_Limit	0.8
MIN_WDQM	0.75
Monitor Period (s)	2
Redeployment	
Redeployment Type	Random/MaxDQM/Hybrid
Initial Deployment Prc.	0.8
Redeployment Prc.	0.2
Aggregation	
Aggregation Window (s)	0/5/10/*15/20
Neighborhood density control (NDC)	
Max Leaf Sensors	4
Leaf Sensors Delta	1
Min Leaf Distance (m)	15
Leaf Distance Delta (m)	4
Sleep Rounds	100

Table 4.3. Intruder mobility parameters

Intruder	
Speed (m/s)	2
Direction Update Period (s)	5
Intruder interarrival (s)	uniform(50-70) *uniform(500-700) uniform(3000-4200) uniform(36000-50400) uniform(72000-100800)
Forward Movement Angle (deg)	uniform(0-180)
Target Batch	1

5. SIMULATION RESULTS

In order to analyze the energy hole problem faced in WSNs in detail, we prepared one default simulation with characteristic application values. We vary only one parameter over a range of possible values and analyze its effect to the network lifetime and sensing quality. In this section, we firstly show the effects of some common parameters that should be tuned by the network designer. Then we proceed with the effect of the proposed mitigation strategies on the network lifetime and sensing quality. Finally, we compare the proposed strategies with each other to show their effectiveness and their difference from the combined strategies.

5.1. The Total Number of Sensors Used

We study the effect of the number of sensors on the network lifetime by keeping the network dimensions fixed to 900x100 m^2, and simulate five different scenarios with 450, 550, 650, 750 and 850 nodes. Each scenario is simulated using four different configurations: firstly without any strategy for energy hole mitigation, then using Random sensor redeployment strategy and MaxDQM redeployment strategy and lastly using the Hybrid redeployment strategy described above.

As can be seen in Figure 5.1, as the total number of sensors used increases, the network lifetime increases. For small number of sensors, the MaxDQM redeployment strategy gives better results since it uses the spare sensors more effectively. When the number of sensors is high, Random and MaxDQM redeployment strategies have similar results since the amount of spare sensors is larger and the created holes are covered anyway.

Random redeployment gives similar results to the default scenario for small number of sensors, but better results than the default scenario for larger number of sensors since it avoids overhearing problems by using smaller number of sensors initially and increases network's overall resilience by redeploying sensors randomly. The hybrid rede-

ployment strategy gives always better results since it combines the ability of MaxDQM to cover holes effectively and the ability of Random redeployment to increase the network's overall robustness. The small decrease in network lifetime at the third data point of Hybrid redeployment is due to the small number of repetitions which results a high variance.

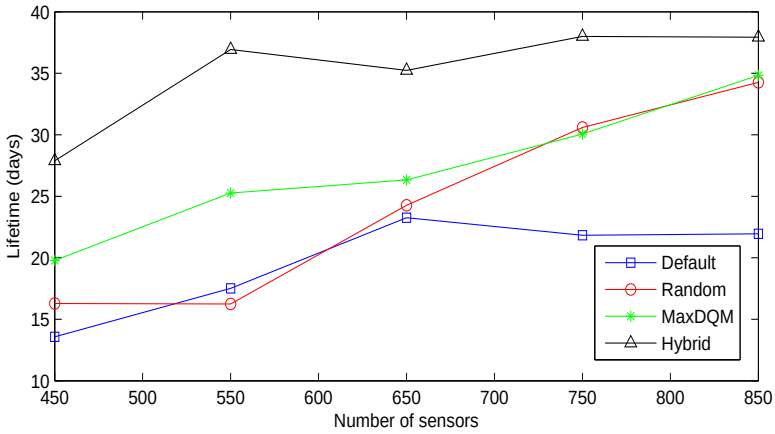


Figure 5.1. Total sensors used vs. lifetime

5.2. Detector Wakeup Period

Sensors periodically wake up to sense the environment and the number of detections reported to the sink depend on the detector wakeup period and intruder speed. In Figure 5.2, the network lifetimes for five different wakeup periods are shown. It is natural to expect that the network lifetime will increase as the detector wakeup period decreases, since the number of detections will decrease.

Knowing the average speed of the intruder, we can calculate the mean time that the sensor can sleep and still detect an intruder passing on its sensing range [50]. In our simulations, we use a detector wakeup frequency of 10 seconds and notice that no intruders are missed.

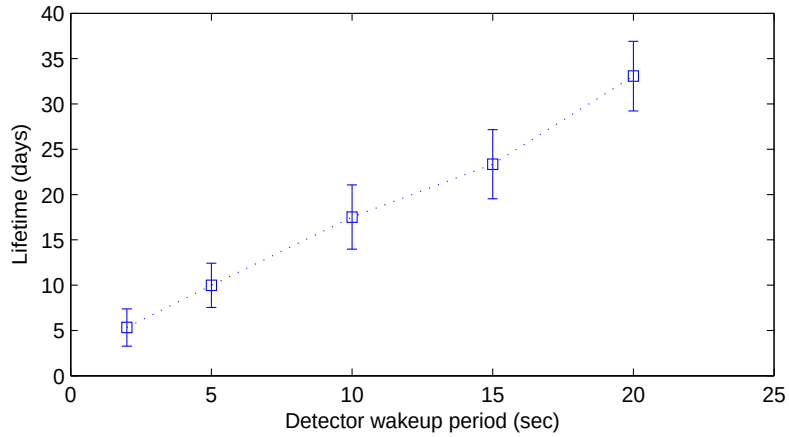


Figure 5.2. Detector wakeup period vs. lifetime

5.3. Intruder Interarrival

The energy consumed by the nodes during idle or sleep periods is some orders of magnitude smaller than the energy consumed during transmission or reception. Since nodes communicate with the sink only when an intruder is detected, the intruder interarrival period directly affects the network lifetime. The relation between the intruder interarrival period and the network lifetime is shown in Figure 5.3.

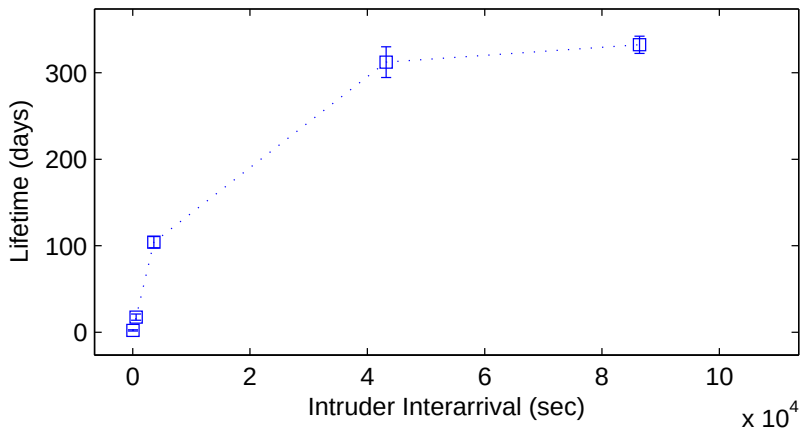


Figure 5.3. Intruder interarrival vs. lifetime

We notice that by increasing the intruder interarrival time, there is a sharp increase in the network lifetime since the network traffic caused by the intruder detection is initially dominant. Further increasing the intruder interarrival time has little effect on the network lifetime since the traffic caused by intrusion detection is negligible com-

pared to the traffic caused by the sensors reporting their health condition periodically to the sink.

5.4. Data Aggregation for Overreporting Avoidance

In order to study the effects of data aggregation on the network lifetime, we keep the network dimensions fixed to 900x100 m^2, the number of sensors to 550 and simulate six different scenarios, one without aggregation (zero aggregation window) and five other scenarios with data aggregation time window of 2, 5, 10, 15 and 20 seconds respectively. As seen in Figure 5.4, using aggregation increases the network lifetime and delays the formation of energy holes.

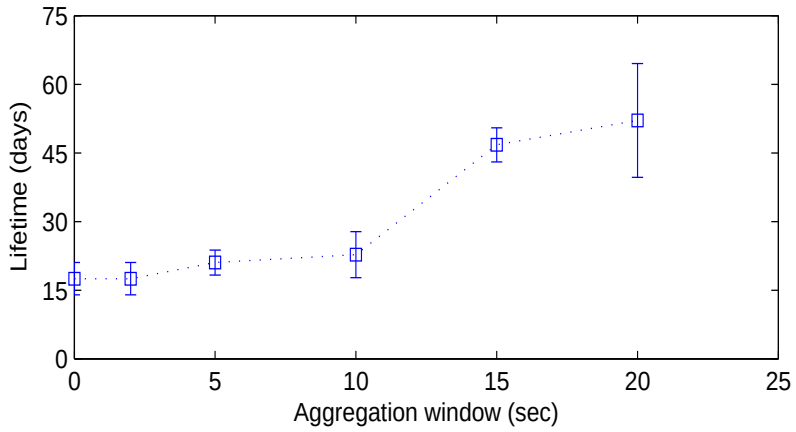


Figure 5.4. Aggregation window vs. lifetime

We notice that using aggregation time window smaller than 10 seconds has little effect on the network lifetime. Since the target detector wakeup period is 10 seconds, detection packets are not generated earlier than 10 seconds from each other. Using an aggregation time window smaller than 10 seconds allows more packets related to the same detection to be forwarded. So almost all of the intrusion detection packets generated are forwarded to the sink.

5.5. Redeployment for Coverage Improvement

We use five different redeployment approaches for improving the network coverage: MaxDQM, random, hybrid, adaptive hybrid and proactive redeployment. In all approaches, 80 per cent of the available sensors are initially deployed and the remaining part is deployed when the network sensing quality drops below the threshold value. Random redeployment deploys spare sensors randomly over the network, while MaxDQM redeployment deploys spare sensors in areas which need urgent care. Deploying spare sensors in areas which need urgent care improves the sensing quality of the network as shown in Figure 5.5. On the other hand, random sensor deployment does not guarantee any improvement in areas which need urgent care but increases the overall network robustness as shown in Figure 5.6. In terms of lifetime and sensing quality, MaxDQM redeployment outperforms Random redeployment in cases where the sensor density is not very high.

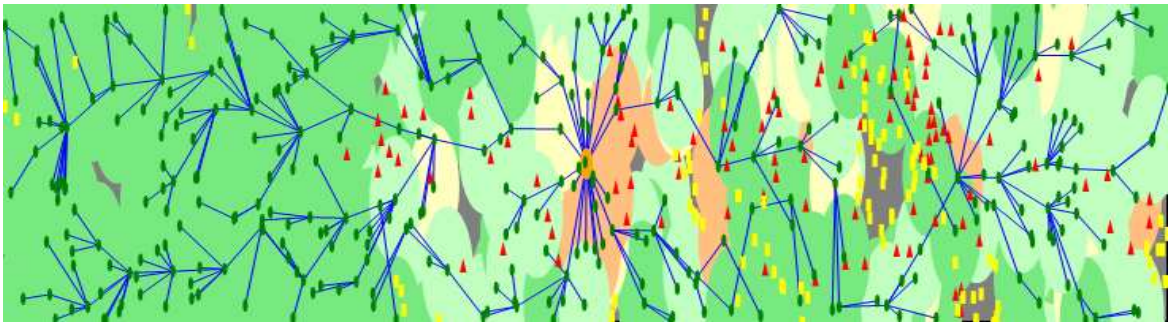


Figure 5.5. MaxDQM redeployment

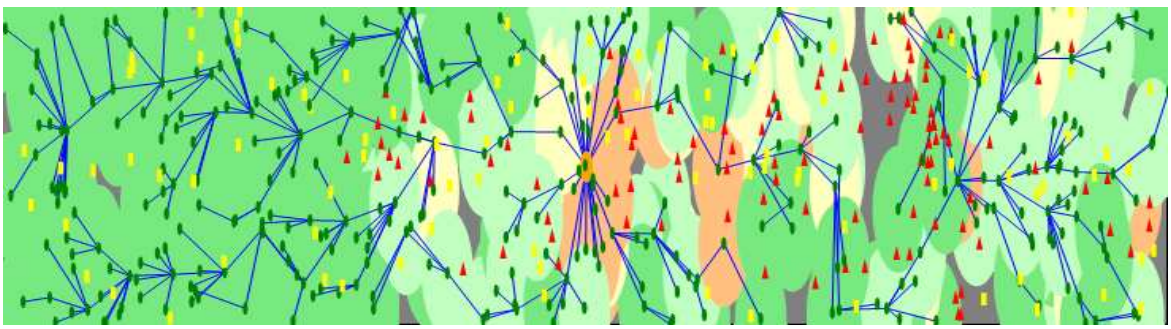


Figure 5.6. Random redeployment

Since Hybrid redeployment strategy uses both Random and MaxDQM redeployment strategies, holes that need immediate care are covered and also improvements the overall network coverage are made by using half of the spare sensors with each strategy as shown in Figure 5.7. The resulting lifetime and sensing quality of Hybrid redeployment is higher than each of the strategies used separately.

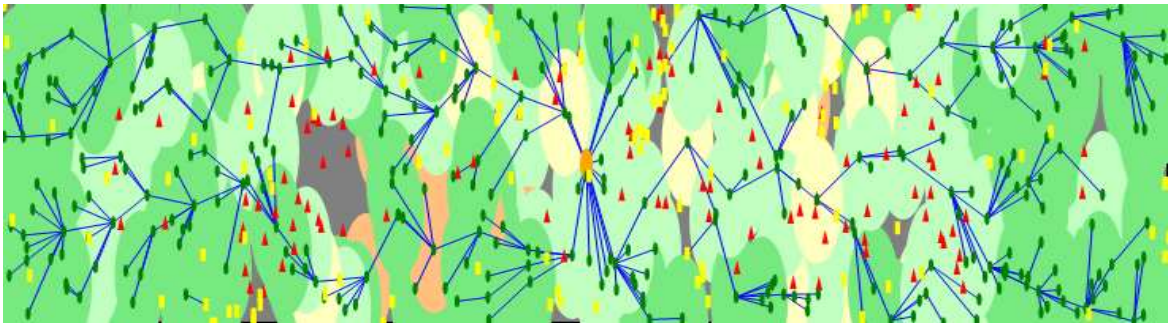


Figure 5.7. Hybrid redeployment

Proactive redeployment places sensors over areas wider than the hole to prevent immediate reappearance of the hole. Sensors are also deployed in areas where sensors are about to be exhausted in order to prevent holes from appearing in those areas just after the redeployment process as shown in Figure 5.8.

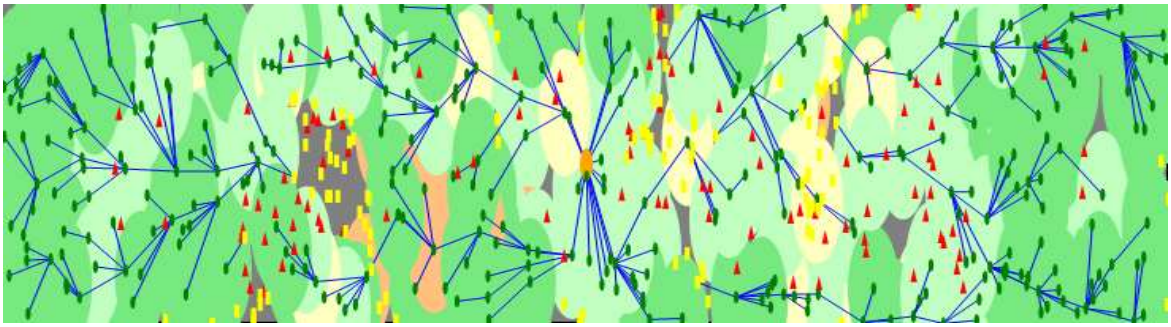


Figure 5.8. Proactive MaxDQM redeployment ($E_{min} = 50$)

In Figure 5.9 we notice that proactive redeployment performs slightly better than MaxDQM redeployment in terms of the network lifetime. Moreover, it achieves better sensing quality since it performs deployment over weak regions in addition to exhausted regions.

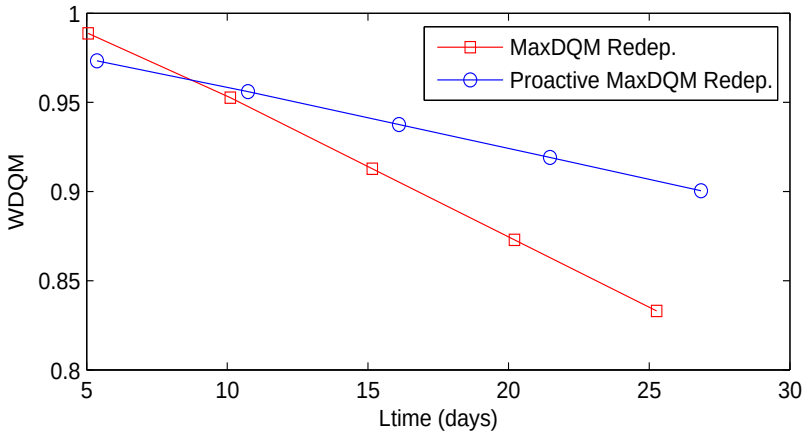
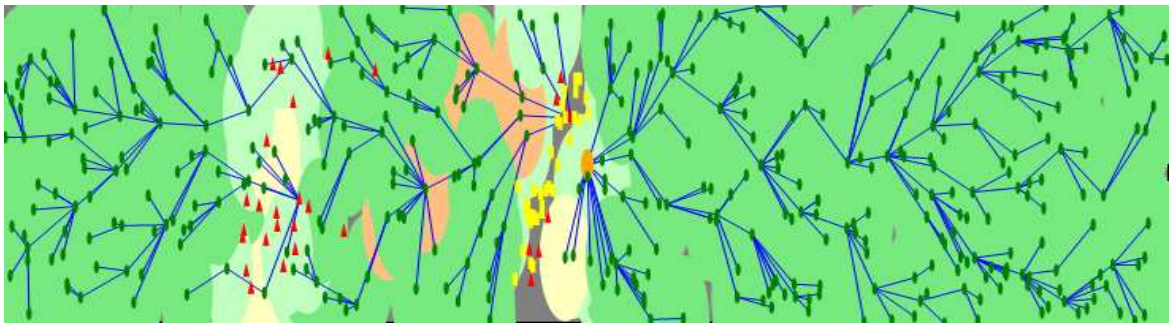
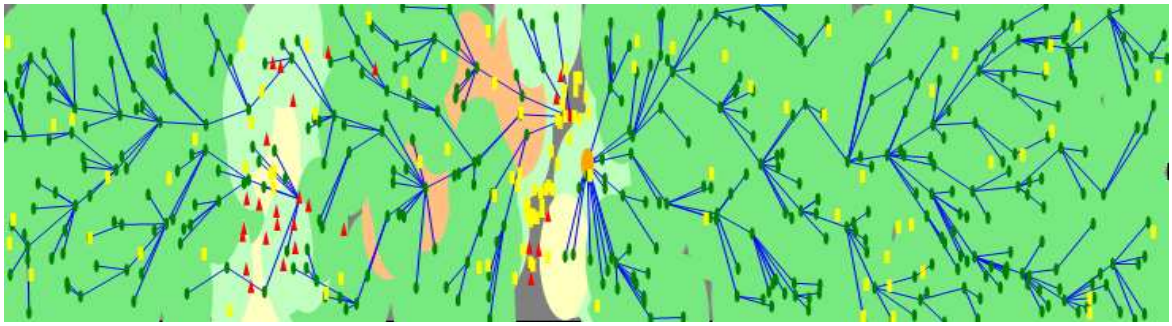


Figure 5.9. Effect of proactive redeployment to surveillance quality

Adaptive redeployment dynamically decides the portion of sensors that should be used by MaxDQM for covering weak regions as shown in Figure 5.10 (a). The remaining sensors after MaxDQM redeployment are then deployed randomly throughout the network as shown in Figure 5.10 (b).



(a) Adaptive redeployment part I (MaxDQM)

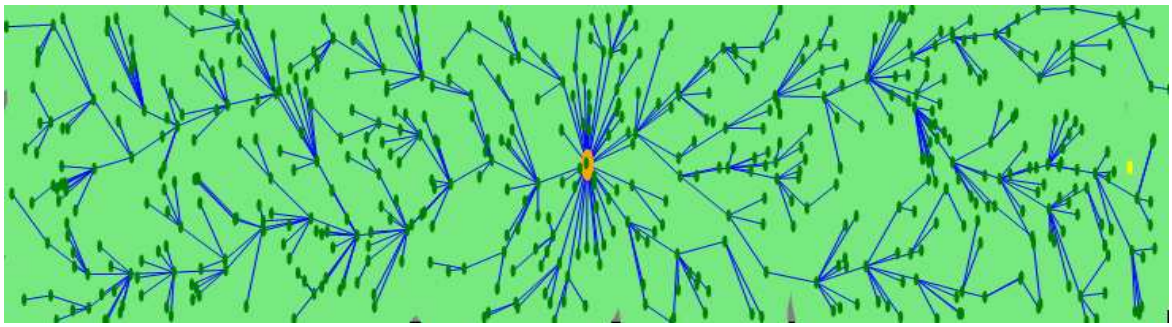


(b) Adaptive redeployment part II (Random)

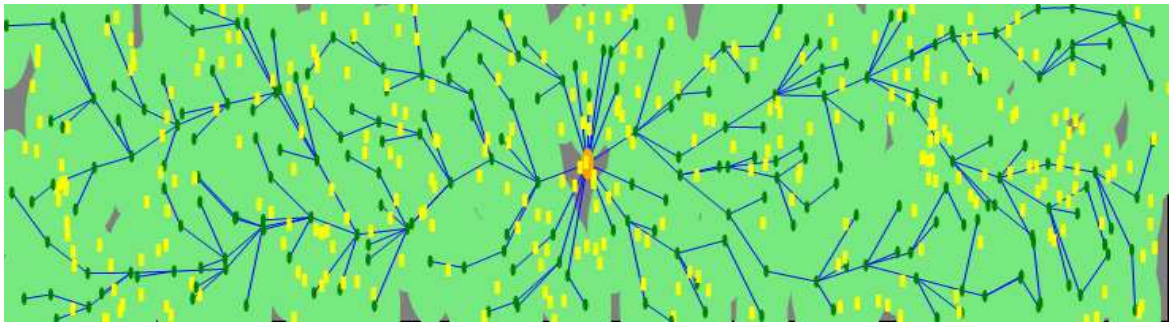
Figure 5.10. Adaptive redeployment steps

5.6. Neighborhood Density Control for Overhearing Avoidance

In Figure 3.7, the initial coverage provided by 550 sensors was shown. Neighbor density control algorithm decides in a distributed fashion which leaf nodes should be disabled. The simulations use an initial minimum leaf-leaf distance of 15 meters and a maximum of four leaf nodes per parent. Whenever a sensor is exhausted, the NDC decides if any inactive sensor in the neighborhood should be activated. When the WDQM value of the network drops below the trigger limit of 0.8, the NDC constraints are relaxed to increase the number of active sensors and the WDQM as shown in Figure 5.12. The initial network coverage provided by NDC shown in Figure 5.11 (b) uses only 245 nodes and is similar to the initial coverage provided by 550 nodes in Figure 5.11 (a). Here, we notice that more than 50 per cent of the sensors are leaf sensors which can be put to long term sleep without affecting the communication backbone.



(a) Initial coverage of normal scenario



(b) Initial coverage provided by NDC

Figure 5.11. Effect of NDC to network coverage

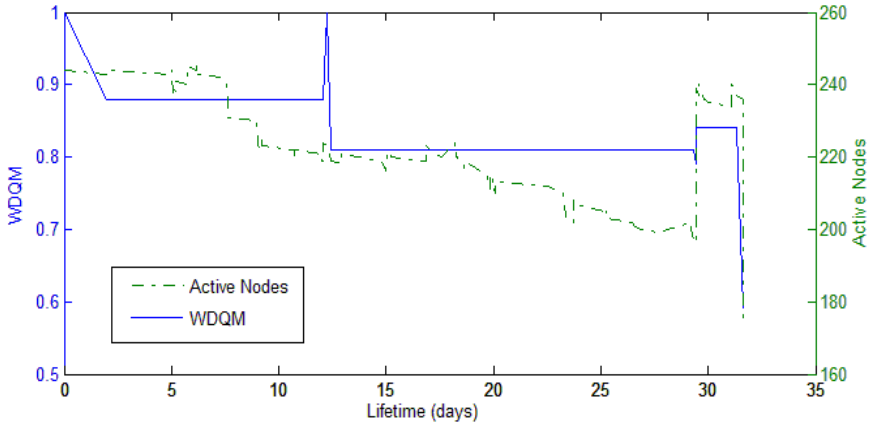


Figure 5.12. WDQM and Active Nodes vs. time for single NDC run

In Figure 5.12 we show the WDQM values of a single NDC simulation run. NDC comes into action at 29th day when the WDQM value drops below 0.8. The algorithm decreases the minimum leaf-leaf distance allowed and increases the maximum number of leafs allowed per parent. In this way, the number of active sensors increases from 200 to 240.

5.7. Combined Strategies

The above described strategies can also be combined with each other in order to achieve better results in terms of the network lifetime and sensing quality. We simulate scenarios using such as aggregation combined with MaxDQM redeployment or NDC. Simulation results show that the combined strategies have better effect on mitigating the energy hole problem. The network lifetime of scenarios that use combined mitigation strategies can be up to four times greater than the network lifetime of the default scenario. Other combined strategies such as a combination of MaxDQM, random, adaptive and proactive redeployment strategies are also possible.

5.8. Network Lifetime and Sensing Quality

To understand the state of the network at a specific instant, we may look at different indicators such as the WDQM measure or the number of connected sensors.

We simulate different hole mitigation strategies as long as the surveillance quality is above the given threshold.

Firstly, we study the effect of each mitigation strategy on the network lifetime. We notice that in the Random redeployment scenario, sensors have the shortest lifetime while in the hybrid combined with aggregation and aggregation combined with NDC sensors have the longest lifetime as shown in Figure 5.13. Here, we notice that some strategies do not have significant differences from each other. However, some strategies such as Aggregation combined with NDC have a network lifetime four times greater than the lifetime of the default scenario.

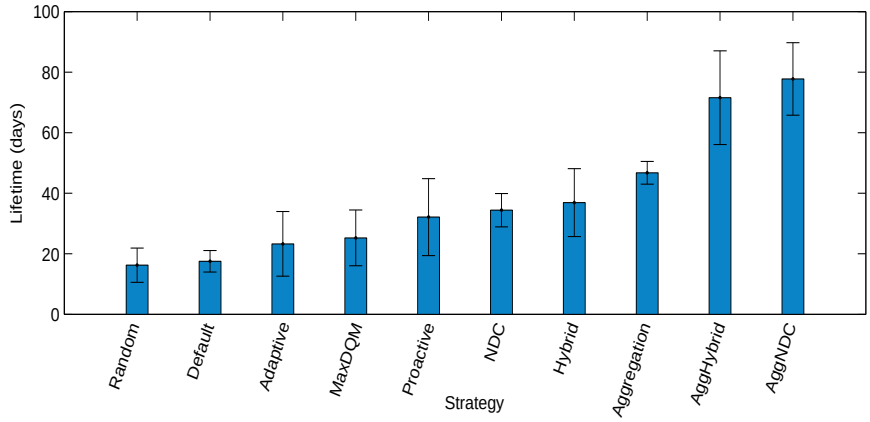


Figure 5.13. Lifetime comparison

Redeployment strategies start with 440 sensors deployed initially, and spare sensors are redeployed when the WDQM value drops below the threshold value. Hybrid redeployment gives the longest lifetime among redeployment strategies, while Proactive redeployment gives slightly better results than MaxDQM redeployment. Adaptive redeployment has shorter lifetime than MaxDQM redeployment since it deploys just enough sensors to cover the created hole and deploys remaining sensors randomly. We notice that the NDC strategy gives longer lifetime than all redeployment strategies except Hybrid redeployment.

The variation of the WDQM with time is shown in Figure 5.14. We notice that aggregation gives longer lifetime and higher WDQM values. The default scenario gives

higher WDQM value than Redeployment scenarios but has shorter lifetime. Redeployment approaches give lower WDQM values since they use smaller initial number of sensors but give a longer lifetime than that of the default scenario. NDC strategy has lower initial WDQM value due to the smaller number of sensors initially activated, but gives longer lifetime than the redeployment strategies due to the minimization of overhearing costs and resilience to failures. Hybrid redeployment gives higher WDQM values and longer lifetime compared to NDC and other redeployment strategies.

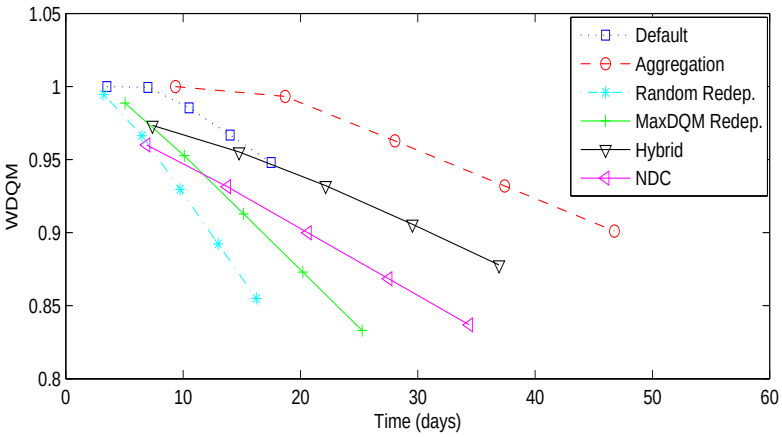


Figure 5.14. WDQM vs. time

The effects of different mitigation strategies on the network lifetime were described in the previous sections. We saw that each strategy improves the network lifetime up to some extent. However, some strategies make much more improvement than others. In this section, we compare the network lifetime obtained for each mitigation strategy. The network lifetimes are shown in Figure 5.15 in descending order. Besides the above described strategies, we also include the results of some strategy combinations such as using Aggregation and MaxDQM redeployment simultaneously or using Aggregation and NDC simultaneously.

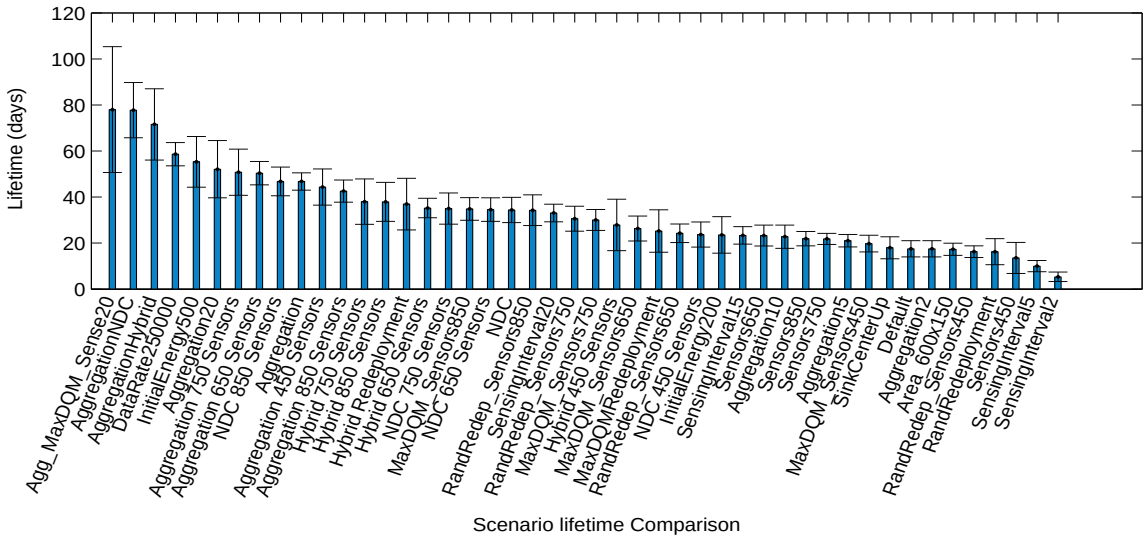


Figure 5.15. Lifetime of different scenarios

5.9. Other Parameters

There are many other parameters that affect the lifetime of SWSN, some of them can be tuned according to the specific requirements while others are bounded to the physical characteristics of the sensor or the intruder behavior.

S-MAC duty cycle can be tuned while considering the detection reporting delay. If the reporting delay is not crucial, we can decrease S-MAC duty cycle to reduce the energy consumption which some sort of short term sleep scheduling. Other parameters such as the channel data rate directly affect the network lifetime. From our simulations, we notice that if we replace our sensor that has a data rate of 38,400 bps to a sensor with a data rate of 250,000 bps, the lifetime of the network increases approximately three times. If a longer network lifetime is required, we must use sensors with a higher transmission data rate.

We also investigate the effect of the sink location on the network lifetime. The sink is originally placed at the center of the FoI and in the second scenario at the center of the upper border. From our simulations we notice that changing the y-coordinate of

the sink position does not have any significant effect on the network lifetime. However, if the sink is placed at the left or right border of the field, we should expect a decrease in the network lifetime since the sensors nearer to the sink will be exposed to a higher traffic.

Another parameter that might affect the network lifetime is the geometry of the FoI. In order to investigate the effects of field dimensions on the network lifetime, we keep the area of the FoI fixed and change the field dimensions from 900x100 m^2 to 600x150 m^2. We notice that both scenarios have similar network lifetimes.

6. CONCLUSIONS

The simulation results show that intruder mobility can have a significant impact on the network lifetime and should not be underestimated when designing a specific surveillance network. Also, the number of deployed sensors is an important issue and only the required number of sensors should be deployed since deploying more sensors than necessary will just increase the packet traffic and will not affect the sensing quality.

Another issue to keep in mind while solving the energy hole problem is that minimizing energy consumption is not the only goal of wireless sensor networks, the network performance is another goal that should be considered [13]. Especially in surveillance networks, one of the most important requirements of the system is the surveillance quality. Hence, we must be careful when trying to put some extra effort to minimize the energy consumption, since it will probably affect the surveillance quality of the system. There is a set of conflicting goals such as extending the network lifetime, improving the sensing quality and network performance that co-exist in border surveillance applications. These parameters must be carefully tuned in order to achieve the desired functionality.

We saw the efficiency of some possible approaches against the formation of energy holes and discussed their feasibility in real applications. We notice that MaxDQM redeployment gives better coverage than Random redeployment at the redeployment instant, but random redeployment can increase the overall network resilience. Hybrid redeployment covers created holes and prevents new hole formation up to some extent thus giving longer network lifetime in addition to better sensing quality. Neighborhood density control avoids overhearing by keeping only the required number of sensors in active state. In scenarios where precise deployment is not feasible a good network performance can be achieved by deploying all the sensors randomly by aerial means and then using NDC in combination with Aggregation strategy. However, if vehicular deployment is possible, we can use Adaptive and Proactive redeployment strategies combined with Aggregation strategy to achieve a good network performance.

Other techniques that might be used in order to mitigate energy hole formation can be the usage of multiple sinks either simultaneously or in a round-robin fashion in the area. In this way, the formation of the energy hole can be partially avoided by having different nodes in the network act as a bridge for the sink. This could have the same effect as using a mobile sink but no real physical movement of the data sink itself will be required. Another possible solution might be to deploy a higher node density around the sink so that the load per sensor node is more balanced and nodes can have equal expected lifetime throughout the network. Since in Border Surveillance Applications generally the mission is to detect intruders coming from outside, keeping the border width narrow can help reduce the redundant messages transmitted but the network may become disconnected more easily.

Finally, we notice that no matter what the intruder mobility or the number of deployed sensors, the networks cause of death is the same. The energy hole causes the sink or some other part of the network to become disconnected. It is desirable to have a network where the nodes fail more independently and the network lifetime is longer.

REFERENCES

1. Pottie, G.J. and W.J. Kaiser, *Wireless integrated network sensors*, Communications of the ACM, Vol. 43, No. 5, pp. 51–58, New York, USA, 2000.

2. Onur, E., C. Ersoy and H. Delic, *Temporal Resilience of the Deployment Quality in Surveillance Wireless Sensor Networks*, IEEE WCNC, Las Vegas, USA, 2008.

3. E. Onur, *Deployment Quality Measures in Surveillance Wireless Sensor Networks*, PhD Thesis, Bogazici University, 2007.

4. Li, J. and P. Mohapatra, *An analytical model for the energy hole problem in many-to-one sensor networks*, 62nd IEEE Vehicular Technology Conference, Dallas, USA, 2005.

5. Ahmed, N., S. S. Kanhere and S. Jha, *The holes problem in wireless sensor networks: a survey*, Mobile Computing and Communications Review, ACM Press, New York, USA, 2005.

6. OPNET Modeler 14.0 *OPNET Technologies Inc.*, Bethesda, MD 20814, USA, http://www.opnet.com, 2009.

7. Ye, W., J. Heidemann and D. Estrin, *An energy-efficient MAC protocol for wireless sensor networks*, Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies, New York, USA, 2002.

8. Kwon, S. and N. B. Shroff, *Paradox of Shortest Path Routing for Large Multi-Hop Wireless Networks*, 26th IEEE International Conference on Computer Communications, Anchorage, Alaska, USA, 2007.

9. Wood, A. D., J. A. Stankovic and S. H. Son, *JAM: a jammed-area mapping service for sensor networks*, 24th IEEE Real-Time Systems Symposium, pp. 286–298, Cancun, Mexico, 2003.

10. Yu, F., Y. Choi, S. Park, D. Lee and S. H. Kim, *A modeling for hole problem in wireless sensor networks*, Proceedings of the 2007 international conference on Wireless communications and mobile computing, ACM Press New York, NY, USA, 2007.

11. Olariu, S. and I. Stojmenovic, *Design guidelines for maximizing lifetime and avoiding energy holes in sensor networks with uniform distribution and uniform reporting*, IEEE INFOCOM, Barcelona, Spain, 2006.

12. Ganesan, D., A. Cerpa, W. Ye, Y. Yu, J. Zhao and D. Estrin, *Networking issues in wireless sensor networks*, Journal of Parallel and Distributed Computing, Vol. 64, No. 7, pp. 799 – 814, 2004.

13. Ali, M., A. Dunkels, K. Römer, K. Langendoen, J. Polastre and Z. A. Uzmi, *Medium access control issues in sensor networks*, ACM SIGCOMM Computer Communication Review, ACM Press, New York, USA, 2006.

14. Gu, L. and J. A. Stankovic, *Radio-Triggered Wake-Up Capability for Sensor Networks*, 10th IEEE Real-Time and Embedded Technology and Applications Symposium, Toronto, Canada, 2004.

15. Goldberg, D. H., A. G. Andreou, P. Juliá, P. O. Pouliquen, L. Riddle and R. Rosasco, *VLSI implementation of an energy-aware wake-up detector for an acoustic surveillance sensor network*, ACM Transactions on Sensor Networks, Vol. 2, No. 4, pp. 594 – 611, 2006.

16. Cerpa, A. and D. Estrin, *ASCENT: adaptive self-configuring sensor networks topologies*, IEEE Transactions on Mobile Computing, Vol. 3, No. 3, pp. 272 – 285, 2004.

17. Schurgers, C., V. Tsiatsis, S. Ganeriwal and M. Srivastava, *Optimizing Sensor Networks in the Energy-Latency-Density Space*, IEEE Transactions on Mobile Computing, Vol. 1, No. 1, pp. 70 – 80, 2002.

18. Kredo, K. and P. Mohapatra, *Medium access control in wireless sensor networks*, Computer Networks, Vol. 51, No. 4, pp. 961 – 994, 2007.

19. Intanagonwiwat, C., R. Govindan and D. Estrin, *Directed diffusion: A scalable and robust communication paradigm for sensor networks*, Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking, Boston, USA, 2000.

20. Lee, M. and V. W. S. Wong, *LPT for data aggregation in wireless sensor networks*, Proceedings of IEEE Global Telecommunications Conference, St. Louis, USA, 2005.

21. Jia, W., T. Wang, G. Wang and M. Guo, *Hole Avoiding in Advance Routing in Wireless Sensor Networks*, IEEE Wireless Communications and Networking Conference, Hong Kong, China, 2007.

22. Heo, N. and P. K. Varshney, *An Intelligent Deployment and Clustering Algorithm for a distributed mobile sensor network*, Proceedings of the IEEE International Conference On Systems, Man and Cybernetics, Vol. 5, pp. 4576 – 4581, 2003.

23. Howard, A., M. J. Mataric and G. S. Sukhatme, *Mobile sensor network deployment using potential fields: A distributed, scalable solution to the area coverage problem*, Distributed Autonomous Robotic Systems, Vol. 5, pp. 299 – 308, 2002.

24. Cayirci, E., H. Tezcan, Y. Dogan and V. Coskun *Wireless sensor networks for underwater surveillance systems*, Ad Hoc Networks, Vol. 4, No. 4, pp. 431 – 446, 2006.

25. Altınel, I. K., N. Aras, E. Güney and C. Ersoy, *Binary integer programming formulation and heuristics for differentiated coverage in heterogeneous sensor networks*, Computer Networks, Vol. 52, No. 12, pp. 2419 – 2431, 2008.

26. Dhillon, S.S. and K. Chakrabarty, *Sensor placement for effective coverage and surveillance in distributed sensor networks*, Defense Technical Information Center, 2003.

27. Chiang, M. and G. T. Byrd, *Neighborhood-Aware Density Control in Wireless Sensor Networks*, International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, IEEE Computer Society, Los Alamitos, CA, USA, 2008.

28. Kosar, R., E. Onur and C. Ersoy, *Redeployment Based Sensing Hole Mitigation in Wireless Sensor Networks*, IEEE Wireless Communications and Networking Conference, Budapest, Hungary, 2009.

29. Meguerdichian, S., F. Koushanfar, G. Qu and M. Potkonjak, *Exposure in wireless Ad-Hoc sensor networks*, Proceedings of the 7th annual international conference on Mobile computing and networking, pp. 139 – 150, Rome, Italy, 2001.

30. Clouqueur, T., V. Phipatanasuphorn, P. Ramanathan and K.K. Saluja, *Sensor deployment strategy for detection of targets traversing a region*, Mobile Networks and Applications, Vol. 8, No. 4, pp. 453 – 461, Springer, 2003.

31. Chin, T.L., P. Ramanathan and K.K. Saluja, *Optimal Sensor Distribution for Maximum Exposure in A Region with Obstacles*, IEEE Global Telecommunications Conference, San Francisco, CA, USA, 2006.

32. Maleki, M. and M. Pedram, *QoM and Lifetime-constrained Random Deployment of Sensor Networks for Minimum Energy Consumption*, IEEE Proceedings of information processing in sensor networks, Los Angeles, CA, USA, April, 2005.

33. Karp, B. and H. T. Kung, *GPSR: Greedy perimeter stateless routing for wireless sensor networks*, Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, Boston, MA, USA, August, 2000.

34. Ahmed, A. A. and N. Fisal, *A real-time routing protocol with load distribution in wireless sensor networks*, Computer Communications, Vol. 31, No. 14, pp. 3190 – 3203, 2008.

35. D. Arifler, Information theoretic approach to detecting systematic node destructions in wireless sensor networks, IEEE Transactions on Wireless Communications, Vol. 7, No. 11, pp. 4730 – 4738, November, 2008.

36. Zhao, Y., R. Govindan and D. Estrin, *Residual energy scans for monitoring wireless sensor networks*, Proceedings of the IEEE Wireless Communications and Networking Conference, Orlando, Florida, USA, March, 2002.

37. Zhao, J., R. Govindan and D. Estrin, *Computing aggregates for monitoring wireless sensor networks*, Proceedings of the IEEE ICC Workshop on Sensor Network Protocol and Applications, Anchorage, AK, USA, 2003.

38. Yick, J., B. Mukherjee and D. Ghosal, *Wireless sensor network survey*, Computer Networks, Vol. 51, No. 12, pp. 2292 – 2330, 2008.

39. A. Elfes, *Occupancy Grids: A Stochastic Spatial Representation for Active Robot Perception*, Autonomous Mobile Robots: Perception, Mapping, and Navigation, IEEE Computer Society Press, Los Alamitos, CA, USA, 1991.

40. Onur, E., C. Ersoy, H. Delic and L. Akarun, *Coverage in Sensor Networks When Obstacles Are Present*, Proceedings of the IEEE ICC, Istanbul, June, 2006.

41. Vincent, L. and P. Soille, *Watersheds in digital spaces: An efficient algorithm based on immersion simulations*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 13, No. 6, pp. 583598, June, 1991.

42. Clouqueur, T., P. Ramanathan, K.K. Saluja and K.C. Wang, *Value-fusion versus decision-fusion for fault-tolerance in collaborative target detection in sensor networks*, Proceedings of Fourth International Conference on Information Fusion, Montreal, Canada, 2001.

43. MATLAB R2007a *The MathWorks Inc.*, Natick, MA 01760-2098, USA, http://www.mathworks.com/products/matlab, 2009.

44. Özgövde, A., İ. Demirkol, Y. Durmuş and Y. Dönmez *S-MAC implementation for OPNET*, Bogazici University Network Research Laboratory, NETLAB, Bogazici University, Istanbul, Turkey, 2009.

45. Dong, M. J., K. G. Yung and W. J. Kaiser, *Low power signal processing architectures for network microsensors*, Proceedings of the international symposium on Low power electronics and design, Monterey, CA, USA, 1997.

46. Chipcon AS, *Datasheet*, http://www.snm.ethz.ch/pub/uploads/Projects/CC1000_datasheet.pdf, 2002.

47. A. Venkateswaran *Opnet Tricks and Tips*, http://www.cse.psu.edu/venkates/index_files/opnet_tips.html, 2009.

48. Microsoft Visual Studio 2005 *Microsoft Corporation*, http://msdn.microsoft.com/en-us/vstudio/default.aspx, 2009.

49. IBM Rational Purify *IBM Corporation*, Armonk, New York 10504-1722, USA, http://www.ibm.com/software/awdtools/purify, 2009.

50. Lazos, L., R. Poovendran and J. A. Ritcey, *Probabilistic detection of mobile targets in heterogeneous sensor networks*, Proceedings of the 6th international conference on Information processing in sensor networks, ACM Press, NY, USA, 2007.