DEPLOYMENT QUALITY MEASURES IN SURVEILLANCE WIRELESS SENSOR NETWORKS

by

Ertan Onur

B.S. in Computer Engineering, Ege University, 1997

M.S. in Computer Engineering, Boğaziçi University, 2001

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

Graduate Program in Computer Engineering

Boğaziçi University

2007

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my advisors Prof. Cem Ersoy and Prof. Hakan Deliç for their unlimited support and help during the preparation of this dissertation and for the invaluable guidance during the M.S. and Ph.D. studies of mine. Also, I am very thankful to my M.S. thesis advisor Prof. M. Ufuk Çağlayan who helped me recover from many distractions - not only academic, but also social - with his gentle presence and advices. These three names saved my life. Also, I would like to express my gratitude to Prof. Lale Akarun for her precious ideas.

I thank all of my teachers in the thesis jury, Assoc. Prof. Fatih Alagöz, Prof. Dr. M. Ufuk Çağlayan and Assoc. Prof. Sema Oktuğ for their time and valuable comments. Their remarks have improved the quality of this thesis significantly.

I have very much benefitted from the discussions with my dear friends in the Computer Networks Research Laboratory (NetLab), I thank them and all of the other friends at Boğaziçi University. I am very proud to be a Bornova Anatolian High School (BAL'93) graduate and I would like to express my gratitude to all of my teachers and friends at BAL.

Finally, I want to thank my family. My mother, Muattar Onur and father Mehmet Ali Onur encouraged me to pursue my Ph.D. degree. Many thanks to my mother especially for supporting me in every way throughout all my scholar activities and staying awake with me on the last mile of this thesis. Since my brother Erdal Onur and sister Emel Onur are doctors, I am very glad to be a son of my parents whose children are all doctors now. This thesis is dedicated to my family.

This work has been supported by the State Planning Organization of Turkey under the grant number 03K120250, and by TUBITAK under the grant number 106E082.

ABSTRACT

DEPLOYMENT QUALITY MEASURES IN SURVEILLANCE WIRELESS SENSOR NETWORKS

Surveillance wireless sensor networks are deployed at border locations to detect unauthorized intrusions. For deterministic deployment of sensors, the quality of deployment can be determined sufficiently well by analysis in advance of deployment. However, when random deployment is required, determining the deployment quality becomes challenging. To assess the quality of sensor deployment, appropriate measures must be proposed. Determining the required number of sensors to be deployed initially is a critical decision. After deployment, temporal changes in the surveillance quality as the sensors die in time must be analyzed. The network lifetime definition must consider the surveillance performance of the network.

In this thesis, to analyze the surveillance performance of the network, we propose deployment quality measures. We discuss the trade-off between the number of sensors and the deployment quality. We formulate the weakest breach path problem, and propose a method to determine the required number of sensors to be deployed. We propose the utilization of the watershed segmentation on the iso-sensing graph that reveals the equally sensed regions of the field of interest in a surveillance application. The watershed segmentation algorithm is applied on the iso-sensing graph to identify the possible breach paths. An algorithm is proposed to convert the watershed segmentation to an auxiliary graph which is then employed to determine the deployment quality. The surveillance quality is verified analytically. The temporal resilience of the surveillance quality is analyzed with a realistic discrete event simulator, and network lifetime definitions based on the deployment quality measures are proposed.

ÖZET

KABLOSUZ ALGILAYICI AĞLARDA GÖZETİM KALİTESİ ÖLÇÜLERİ

Kablosuz algılayıcı ağlar sınır bölgelerinde izinsiz sızmaları sezmek için kullanılabilir. Algılayıcıların düzenli olarak yerleştirildiği ağlarda, gözetim kalitesi önceden analiz edilebilir. Eğer algılayıcılar sınır bölgesine rasgele dağıtılıyorsa, konuşlandırma kalitesini belirlemek zordur ve uygun ölçüler kullanmak gerekir. Başlangıçta konuşlandırılacak algılayıcı sayısını belirlemek kritik bir tasarım kararıdır. Zaman içinde algılayıcılar öldükçe, konuşlandırma kalitesinin değişimini incelemek gerekir. Şebekenin ömrü gözetim kalitesine bağlı tanımlanmalıdır.

Bu tezde, kablosuz algılayıcı ağların gözetim kalitesini analiz etmek için ölçütler önerilmekte ve konuşlandırılacak algılayıcı sayısı ile arasındaki ilişki incelenmektedir. En zayıf sızma yolu problemi tanımlanarak belli bir gözetim kalitesi için gerekli algılayıcı sayısını hesaplamak için yöntemler önerilmektedir. Eş-sezme çizgesi bir bölgedeki eşit sezme olasılıklarını gösterir ve üzerine boşaltma havzası kesimleme tekniği uygulandığında ortaya çıkan çevre hatları olası sızma yollarını gösterir. Bu tezde, gözetim kalitesini hesaplamak için olası sızma yollarından oluşturulan çizgeyi kullanan bir yordam önerilmektedir. Gözetim kalitesi analitik olarak doğrulanmakta ve zaman içinde değişimi gerçekçi bir benzetim modeli ile analiz edilmektedir. Gözetim kalitesine bağlı şebeke ömrü tanımları önerilmektedir.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS iii
ABSTRACT iv
ÖZET v
LIST OF FIGURES ix
LIST OF TABLES xv
LIST OF SYMBOLS/ABBREVIATIONS xviii
1. INTRODUCTION 1
1.1. Wireless Sensor Networks 1
1.2. Surveillance Wireless Sensor Networks 2
1.3. Motivation, Addressed Problems and Contributions 4
1.4. Literature Review 7
2. WEAKEST BREACH PATH PROBLEM 16
2.1. Weakest Breach Path Problem Formulation 16
2.1.1. Field Model 16
2.1.2. Sensor Models 18
2.1.2.1. Binary Detector 18
2.1.2.2. Neyman-Pearson Detector 19
2.1.2.3. Elfes's Model 20
2.1.3. Coverage Model 21
2.1.4. Weakest Breach Path Problem 21
2.2. Analysis of the Breach Detection Probability 24
2.2.1. Sensor Parameters 24
2.2.1.1. Neyman-Pearson Detection 25
2.2.1.2. Elfes's Parameters 27
2.2.2. The Number of Sensors 28
2.2.3. Determining the Required Number of Sensors 29
2.2.4. Deterministic Deployment 32
2.3. Analysis of the Breach Probability 34
2.3.1. Determining the Required Number of Sensor Nodes 39

2.3.2. Effect of Field Shape on the Breach Probability 40
2.4. Breach Paths as Watershed Contours 43
2.4.1. Analysis of Breach Probability 45
2.5. Analysis of Vertical Breach Paths 49
2.5.1. Vertical Path Detection Probability 49
2.5.2. Evaluation of the Biased Random-Way Point Breach Paths . . 50
3. DEPLOYMENT QUALITY MEASURES 53
3.1. Iso-sensing Graph Definition 56
3.1.1. Iso-Sensing Surface Definition 57
3.1.1.1. K-Degrees of Iso-Sensing (KIS) 57
3.1.1.2. Reliable K-Degrees Iso-Sensing (KRIS) 58
3.1.1.3. Reliable Subset Iso-Sensing (RIS) 58
3.1.1.4. Most-Dominant-Sensor Iso-Sensing (MDIS) 59
3.1.2. Watershed Segmentation 61
3.2. Deployment Quality Measure 63
3.2.1. Simulation Results and Discussion 67
3.3. Area Based Quality Measures 73
3.3.1. Poorly Detected Area Measure 73
3.3.2. Redeployment Measure 75
3.3.3. Connected Sides 76
3.3.4. Breach Detection Probability 76
3.4. Analysis of Area Based Deployment Quality Measures 77
3.4.1. Propagation, Signal and False Alarm Parameters 78
3.4.2. Reliability Threshold and Deployment Density 80
3.4.3. Discrete Event Simulation 82
4. ANALYTICAL DEPLOYMENT QUALITY MEASURE 83
4.1. Random Point Detection 84
4.2. Numerical Evaluation of Random Point Detection 87
5. TEMPORAL BEHAVIOR OF THE DEPLOYMENT QUALITY 90
5.1. Lifetime Definitions 90
5.2. Application Scenarios and Simulation Setup 92
5.2.1. Simulation Setup 93

5.2.1.1. Wake-up Circuitry Model 93
5.2.1.2. Radio Model 94
5.2.1.3. Sensor Model 95
5.2.1.4. Intruder Mobility Model 95
5.3. Analysis of the Network Lifetime 96
5.3.1. Temporal Behavior of the Deployment Quality 96
5.3.2. Energy Hole Problem 98
5.3.3. Deployed Number of Sensors 100
5.3.4. Deployed Number of Sinks 102
5.3.5. Effect of Intruder Mobility 102
5.3.6. Comparative Evaluation of Sensing Range and Sensor Count . . 105
6. CONCLUSIONS 107
REFERENCES 110

LIST OF FIGURES

Figure 1.1. If the sensors are spread from an aircraft that flies over the middle of the field, then most of the sensors will fall on the trajectory, and a few will end up apart. In (a), the bottom locations are occupied by more sensors. If deterministic deployment is applicable, then sensors can be deployed uniformly such as shown in (b) 3

Figure 2.1. A sample field model constructed to find the breach path 17

Figure 2.2. Sensor models 18

Figure 2.3. Sample detection probabilities for Elfes's sensor detection model with $r = 20$ meters and $r_e = 18$ meters 20

Figure 2.4. Sample sensing coverage and breach path, where the length, width, boundary size and grid size are 260 m., 60 m., 20 m. and 1 m., respectively. Twenty Neyman-Pearson detectors are deployed with $\alpha = 0.01, \eta = 2, \gamma = 30$ dB and $L = 100$ 22

Figure 2.5. The effect of the false alarm rate α, the path loss exponent η, the signal-to-noise ratio γ and the data size L on the breach detection probability P_{BD} in NP detection 26

Figure 2.6. The effect of λ on the breach detection probability in ESDM . . . 27

Figure 2.7. The effect of the number of sensors, R, on the breach detection probability 28

Figure 2.8. A sample field where the sensors are deployed deterministically . . 33

Figure 2.9. The effect of α on the breach probability 36

Figure 2.10. The effect of η on the breach probability 36

Figure 2.11. The effect of γ on the breach probability 37

Figure 2.12. The effect of L on the breach probability 38

Figure 2.13. The effect of the number of sensor nodes on the breach probability where the sensor nodes are uniformly distributed along both the vertical and horizontal axes 38

Figure 2.14. The effect of the number of sensor nodes on the breach probability where the sensor nodes are deployed uniformly along the horizontal axis and normally distributed along the vertical axis with mean $M/2$ and a standard deviation of 10 per cent of the width of the field 39

Figure 2.15. The effect of the field shape on breach probability where the sensor nodes are uniformly distributed along both the vertical and horizontal axes 40

Figure 2.16. The effect of the field shape on breach probability where the sensor nodes are deployed uniformly along the horizontal axis and normally distributed along the vertical axis with mean $M/2$ and a standard deviation of 10 per cent of the width of the field 41

Figure 2.17. Miss probability surface and watershed segmentation shown on the detection probability surface where length=50 m, width=50 m, boundary=20 m., grid size=1 m., $R = 10, r = 15$ m., $r_e = 12$ m., $\lambda = 0.5$ and $\beta = 0.5$. 43

Figure 2.18. The effect of λ and β on breach probability for the EPS scenario where $r = 20$ m., $r_e = 18$ m 45

Figure 2.19. The effect of λ and β on the required number of sensors for a breach probability less than 0.01 46

Figure 2.20. The effect of the width of the field on breach probability for the EPS scenario where 15 sensors are utilized 47

Figure 2.21. The effect of the number of sensor nodes on the breach probability for the EPS and CBS scenarios 48

Figure 2.22. Verification of Equation 2.14 with Matlab simulations 50

Figure 2.23. The effect of sensor count on the detection ratio and time-to-detect the target when binary or Elfes's detectors are utilized 52

Figure 3.1. Voronoi segmentation fails when obstacles are present in the area of surveillance 54

Figure 3.2. A sample iso-sensing surface where the length, the width and the grid size are 160 meters, 40 meters and 1 meter, respectively. The iso-sensing surface is calculated using NPD model where the false alarm rate, SNR, path-loss exponent and the sample size are 0.01, 20 dB, two and 100, respectively 55

Figure 3.3. Two dimensional visualization of the sample iso-sensing surface shown in Figure 3.2 59

Figure 3.4. The watershed contours of the sample iso-sensing surface shown in Figure 3.3 60

Figure 3.5. Algorithm to construct auxiliary graph 64

Figure 3.6. Algorithm to label the grid points 66

Figure 3.7. Algorithm to determine the deployment quality measure 66

Figure 3.8. Trace of Algorithm in Figure 3.7. This is the auxiliary graph of the watershed contours in Figure 3.4 produced using Algorithm in Figure 3.5 68

Figure 3.9. The effect of sensor count and false alarm rate on the deployment quality measure for MDIS when NP detectors are deployed 69

Figure 3.10. The effect of sensor count and false alarm rate on the deployment quality measure for KIS when NP detectors are deployed 69

Figure 3.11. The effect of sensor count and false alarm rate on the deployment quality measure for RIS when NP detectors are deployed 70

Figure 3.12. The effect of sensor count and false alarm rate on the deployment quality measure for KRIS when NP detectors are deployed 70

Figure 3.13. The effect of sensor count and sensing coverage degree on the DQM for KIS when Elfes's detectors are utilized 71

Figure 3.14. The effect of the sensor count on the detection ratio of a when Neyman-Pearson detectors are deployed target following the watershed contours for several target speeds (g/s denotes the velocity of the target in terms of grid per second) 73

Figure 3.15. A sample iso-sensing surface and connected components where the length, the width, the boundary length and the grid size are 80 meters, 40 meters, 10 meters and one meter, respectively. The iso-sensing surface is calculated using thirteen NP detectors where the false alarm rate, SNR, path-loss exponent and the sample size are 0.01, 20 dB, two and 100, respectively 74

Figure 4.1. The effect of sensing range on the deployment quality measure is verified with simulations where $D_2 = 30$ meters, $D_1 = 100$ meters and $N = 10,\ 20,\ 30$ 87

Figure 4.2. The effect of the number of sensors on the deployment quality measure is verified with simulations where $D_2 = 30$ meters, $D_1 = 100$ meters and $d_t = 5,\ 10,\ 15$ meters 88

Figure 4.3. The effect of sensing range on the required number of sensors for different threshold detection probabilities where $D_2 = 30$ meters, $D_1 = 100$ meters 88

Figure 4.4. The effect of field shape parameter $\zeta = D_2/D_1$ on the required number of sensors for different threshold detection probabilities where total area is 3000 m^2, $d_t = 10$ meters 89

Figure 5.1. The lifetime of the individual sensors 96

Figure 5.2. The temporal changes in the deployment quality measures 97

Figure 5.3. Demonstration of the energy hole problem when sensors are uniformly deployed in the field-of-interest of 300×50 m^2 98

Figure 5.4. Demonstration of the energy hole problem when two sinks are deployed in the field-of-interest of 300×50 m^2 99

Figure 5.5. The effect of the number of sensors on the network lifetime 101

Figure 5.6. The effect of deployed number of sinks on the network lifetime . . 101

Figure 5.7. The effect of the intruder re-occurrence period (time between the occurrence of two distinct intruders) on the network lifetime . . . 103

Figure 5.8. The effect of the number of intruders on the network lifetime . . . 104

Figure 5.9. The effect of the intruder speed (meters per second) on the network lifetime 104

LIST OF TABLES

Table 2.1. Parameter values used in the simulations 25

Table 2.2. Parameter values in the simulations to determine the required number of sensors for a target breach probability level 29

Table 2.3. The required number of sensors $P_{BD} \geqslant 0.95$ for the LCFA scenario, where the sensors are distributed uniformly 30

Table 2.4. The required number of sensors $P_{BD} \geqslant 0.95$ for the LCFA scenario, where the sensors are distributed uniformly on the x-axis and normally distributed on the y-axis with a mean of half of the width and a standard deviation that is 10 per cent of the width 31

Table 2.5. The required number of sensors for $P_{BD} \geqslant 0.95$ for the HCFA scenario, where the sensors are distributed uniformly 32

Table 2.6. The required number of sensors for $P_{BD} \geqslant 0.95$ for the HCFA scenario, where the sensors are distributed uniformly on the x-axis and normally distributed on the y-axis with a mean of half of the width and a standard deviation that is 10 per cent of the width 32

Table 2.7. The required number of sensors to satisfy $P_{BD} \geqslant 0.95$ for the LCFA scenario, where the sensors are deterministically deployed 33

Table 2.8. The required number of sensors to satisfy $P_{BD} \geqslant 0.95$ for the HCFA scenario, where the sensors are deterministically deployed 34

Table 2.9. Parameter values used in the simulations for the LCFA and HCFA scenarios 35

Table 2.10. The effect of field shape on the required number of sensor nodes for a breach probability of 0.01 for the LCFA scenario 42

Table 2.11. The effect of field shape on the required number of sensor nodes for a breach probability of 0.01 for the HCFA scenario 42

Table 2.12. Surveillance field parameters 45

Table 3.1. Parameter values used in the simulations to analyze the alternative deployment quality measures 77

Table 3.2. The effect of α on the deployment quality measures 78

Table 3.3. The effect of η on the deployment quality measures 79

Table 3.4. The effect of γ on the deployment quality measures 79

Table 3.5. The effect of reliability threshold p_t on the deployment quality measures 80

Table 3.6. The effect of the sensor deployment density on the deployment quality measures 80

Table 3.7. The effect of the number of sensors on the mean of the deployment quality measures 81

Table 3.8. Verification of the breach probability through discrete event simulations 82

Table 5.1. Current consumptions of the transmission circuitry of the Chipcon CC1000 radio chip 94

Table 5.2. The effect of the number of sensors R and sensing range r on the network lifetime (hours) when Elfes's detectors are deployed where $r_e = 5$ meters, $\lambda = 0.5$ and $\beta = 0.5$ 106

LIST OF SYMBOLS/ABBREVIATIONS

$\mathfrak{B}_v$	Black and white image of the sensing coverage
$c_{v,w}$	Element of the connection matrix denoting the connection of grid points v and w
C	Connection matrix
$C(M)$	Catchment basin associated with plateau M
d	Destination point that denotes secure side
d_{vi}	Distance between grid point v and sensor i
d_v	Weight of grid point v
D_1	Field length
D_2	Field width
d_t	Sensing distance
d_c	Maximum communication distance
E	Connection matrix of the auxiliary graph
$F_D(\xi D_2)$	Cumulative distribution function of distance between two random points in a rectangle
$f_D(\xi D_2)$	Probability density function of distance between two random points in a rectangle
$\mathbf{G}_4(x, y)$	4-connected neighbor set of a grid point
$\mathbf{G}_8(x, y)$	8-connected neighbor set of a grid point
$I(p)$	Gray-scale intensity of point p
K	Coverage degree
L	Sample count
$\mathfrak{L}$	Label of watershed contour
M	Number of vertical grid lines
$M(I)$	Plateau of I around point p
N	Number of horizontal grid lines
P	Breach probability
P_{BD}	Breach detection probability
o_{vi}	Denotes if there is an obstacle between the grid point v and the sensor i

p_{vi}	Detection probability of a target on grid point v by sensor i
p^*_{vi}	Truncated detection probability of a target on grid point v by the sensor i
p_v	Detection probability of a target on grid point v
p^I_v	Uncorrelated detection probability of grid point v
p^D_v	Correlated detection probability of a target on grid point v
p^{KIS}_v	K-degrees of iso-sensing
p^{KRIS}_v	Reliable K-degrees of iso-sensing
p^{RIS}_v	Reliable subset iso-sensing
p^{MDIS}_v	Most-dominant-sensor iso-sensing
Q_{PD}	Poorly detected area measure
Q_{RD}	Redeployment measure
Q_{CS}	Connected sides measure
s	Start point that denotes insecure side
S	Set of points in a Voronoi tessellation
S_v	Set of sensors influential on grid point v
τ^{cs}	Lifetime definition in terms of the connected sides measure
τ^{dqm}	Lifetime definition in terms of deployment quality measure
τ^{first}	Lifetime definition of first dead sensor
τ^{pd}	Lifetime definition in terms of the poorly detected area measure
τ^{rd}	Lifetime definition in terms of the redeployment measure
v	Communication neighboring degree
V	Set of grid points of the weakest breach path
w	Sensing neighboring degree
W	Weight of watershed contour
x_{ij}	Denotes if the grid points i and j are on the weakest breach path and connected
z	Indicator of connected sides
α	False alarm rate
γ	Signal-to-noise ratio

η	Path-loss exponent
$\wp$	Path between point p and q
$\Phi(x)$	cumulative distribution function of the zero-mean, unit-variance Gaussian random variable at point x

AWGN	Adaptive white gaussian noise
DQM	Deployment quality measure
ESDM	Elfes's sensor detection model
FES	Frequent-event surveillance
NP	Neyman-Pearson
NPD	Neyman-Pearson detector
RES	Rare-event surveillance
SNR	Signal-to-noise ratio
QoS	Quality of sensing

1. INTRODUCTION

1.1. Wireless Sensor Networks

A wireless sensor network (WSN) is comprised of small and low-cost sensors with limited computational and communication power. The objective is sensing the environment and communicating the information to the base station. The WSN consists of autonomous nodes using sensors to monitor physical or environmental conditions, such as temperature, pressure, motion [1]. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. In addition to one or more sensors, each node is equipped with a wireless communications device and a battery. The base stations (sinks) in a WSN act as a gateway between sensor nodes and the end user and have more computational, energy and communication resources. The characteristics of a WSN are [2–5]:

- The nodes are small,
- The nodes are power-limited,
- Node failures are common,
- Network topology is dynamic,
- The scale of the deployment is large,
- Unattended operation is required.

Many areas of employment are envisaged for WSNs ranging from the monitoring of endangered animals populations to military surveillance. For example, in a vineyard in Oregon, embedded sensors monitor temperature. One minute and hourly minimum/maximum temperature readings are recorded [6]. On Great Duck Island off the coast of Maine, a sensor network monitors the light, temperature and barometric pressure of the nesting grounds of seabirds and communicates to the control center [7, 8]. With minimal human disturbance, biologists observe the seabirds and protect habitat. Furthermore, sensors tract the stresses on the Golden Gate Bridge in San Francisco and how much the bridge sways from side to side. Structural integrity weaknesses are

monitored in real time in case of natural disasters such as an earthquake [9]. Detailed reviews of various WSN applications can be found in [10–16]

1.2. Surveillance Wireless Sensor Networks

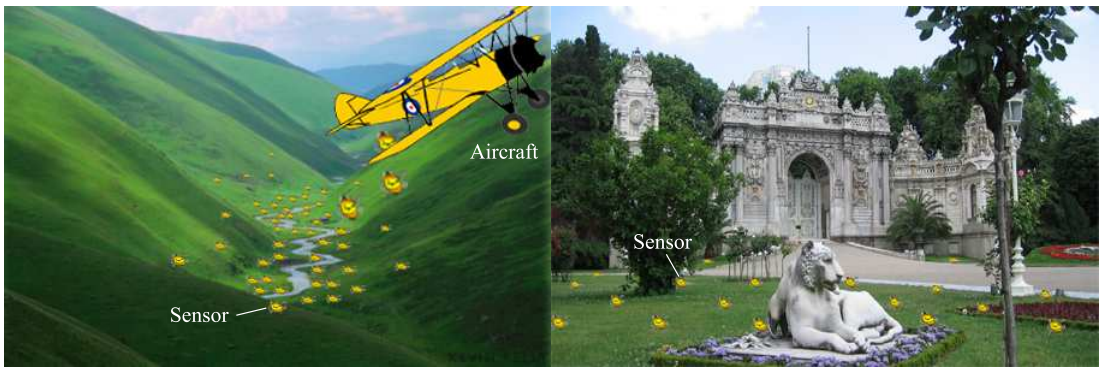
In this thesis, we concentrate on surveillance wireless sensor networks (SWSNs) whose duty is intrusion detection in applications such as border surveillance against penetration by hostile elements or perimeter protection. Sensors are deployed to a region, they wake up, organize themselves as a network, and start sensing the area for intrusion. When a sensor detects an intrusion, the event is communicated to the sink node so that an appropriate action is taken. The SWSNs are designed such that the intrusion detection probability is maximized while maintaining a long network lifetime. Such performance constraints reflect in the quality of sensor deployment and we need meaningful measures to assess the quality. It is hard to define a metric that is independent of the type and variety of the sensors, the number of sensors deployed, the deployment scheme and the characteristics of the target and the environment. For example, the detectability in a geography that is harsh and nonuniform in shape will be lower than that in a plain for fixed number of sensors.

The major differences of the wireless sensor networks from other legacy wireless networks are: Large number of sensor nodes are densely deployed providing high redundancy. Power is the bottleneck attribute of the sensors, the sensors die if their batteries drain. The sensor nodes are very prone to failures and the topology of the network changes frequently. The computational and communication capabilities of the sensors are very low and unattended operation during the network organization phase is required. The sensor nodes communicate intermittently. The WSNs are mostly data-centric and the accuracy of the readings changes during the lifetime.

Suppose that a section of a border or perimeter is to be monitored against unauthorized intrusion and the terrain is rough. Surveillance tasks may involve risks for humans in which case unmanned mission accomplishment is more desirable. Deploying a wired network infrastructure on the field is usually difficult. The WSN paradigm

offers an easy and rapid alternative for building a network. Dense deployment is preferred to ensure robustness. For example, the sensors can be dropped on some region of interest by an aircraft. Nodes organize themselves to build up a network, medium access and network layers are configured dynamically on the run, and the network becomes operational. A sleep schedule may be established adaptively to decrease the power consumption.

A SWSN may be employed in a wide range of places such as country borders, wildlife parks, embassies, factories. Example scenarios are depicted in Figure 1.1. The particular application will dictate a certain cost of a false alarm. For example, when a house or a factory is to be monitored for intrusion detection, the cost of a false alarm is relatively low. On the other hand, when the perimeter security of some mission-critical location such as an embassy or a nuclear reactor is to be ensured, a false alarm might trigger the transportation of special forces and/or personnel of related government agencies to the secured area, as well as the evacuation of residents in the surrounding neighborhoods, driving up the financial and personnel costs to confidence-shaking levels.



(a) Random deployment (b) Uniform deployment

Figure 1.1. If the sensors are spread from an aircraft that flies over the middle of the field, then most of the sensors will fall on the trajectory, and a few will end up apart.

In (a), the bottom locations are occupied by more sensors. If deterministic deployment is applicable, then sensors can be deployed uniformly such as shown in (b)

The detection of intrusions through a country's borders is a significant military application where interesting challenges related to SWSN design may exist. The border to be monitored may be a huge area where the width is smaller than the length. The area need not be a straight line either, and there may be curling regions. The altitude may vary significantly. Moreover, some natural obstacles such as a river or a lake may exist within or along the border (see Figure 1.1(a)). Depending on the sensing range, the number of sensors and deployment scheme, the sensing coverage of the SWSN may have gaps. In case of a country border which might be hundreds of kilometers long, the surveillance area may be segmented to deal with complexity before deploying the sensors to the field. Furthermore, for emergency situations, each segment may be monitored by a different control center. The segmentation can be carried out according to the geographical properties of the border such as topology and altitude.

1.3. Motivation, Addressed Problems and Contributions

Wireless sensor networks are appropriate tools to monitor an area for surveillance. The primary challenges in building a surveillance wireless sensor network pertain to the decisions to be considered while deploying the sensors. Depending on the range and the number of sensors, the sensing coverage area of the SWSN may contain breach paths. The term *quality of sensing* (QoS) signifies how well a sensor network covers a region and senses phenomena of interest such as the presence of an unauthorized intruder. The probability of detecting a target traversing the region gives precious insight about the QoS provided by the network. When analyzing the QoS, a unified approach is necessary because of the various distinct types of sensors that may be collaborating. Considering the surveillance applications, if the goal is to detect unauthorized access to a secured region, the probability of intrusion detection is a plausible performance measure for sensors of the acoustic or the sonar kind, for instance.

Once some set of sensors is deployed, how will one be sure that the deployment provides the necessary security level? To analyze if the requirement is met, one needs measures that represent the quality of the deployment, which is directly related to the sensing coverage of the network. The QoS performance of the SWSN can be further

improved by using data/decision fusion techniques. The SWSN must be able to adapt to the changing network and environment conditions. Because intrusions are usually detected by several sensors, highly-reliable intrusion information can be derived by means of cooperation among the sensor nodes.

Depending on the deployment style, the coordinates of the sensor node locations may follow a distribution such as the Gaussian. For example, if the sensor nodes are dropped from an aircraft that flies over the middle of the field, then most of the sensors will fall somewhere close to the middle, and a few will end up far away (see Figure 1.1(a)). Considering the surveillance applications, the geographical properties of the field, such as the altitude, may affect the deployment, as well. If the field is a narrow canyon, the bottom locations will be occupied by more sensor nodes. These problems require analysis of non-uniform deployment. For fields that are irregular in shape, rigorous analysis is required to reach a stronger conclusion about the effects of random and deterministic deployment strategies. When obstacles exist in the field, a line-of-sight problem arises. Some parts of the field cannot be monitored because the sensor nodes may not be able to detect the phenomenon due to the lack of a direct view. It is hard to define a metric that is independent of the type and variety of the sensors, the number of sensor nodes deployed, the deployment scheme and the characteristics of the target and the environment.

For surveillance wireless sensor networks, depending on the sensing ranges and coverage schemes of the sensors, as well as the deployment-density of the network, the sensing coverage area may contain breach paths. The probability that a target traverses the region through the breach path gives insight about the level of security provided by the SWSN. Considering SWSN, some of the design challenges may be listed as follows: How many sensors are to be deployed to provide a required security level [17]? How could the sensor detection be modelled and how is the sensing coverage determined? What are the effects of geographic properties of the field on target detection? How should the sensors be deployed in the region [18]? What is the weakest part of the coverage and how can the breach paths be discovered [19–21]? How could the false alarms be minimized and the decisions be improved about target detection

considering collaboration? What are the effects of the signal properties on the sensing coverage? What is the impact of sensor scheduling on the sensing coverage [22–24]? Non-communicating sensors are useless; what should the effective communication and sensing ranges of the sensors be [22, 25]? Should incremental deployment be considered [26]? In this thesis, we analyze some of the above challenges, and propose methods to determine the required number of sensor nodes to provide a predetermined security level that is defined with the breach detection probability of an unauthorized target passing through the field.

The network lifetime is directly related to the energy resources of the sensor nodes and can be extended by energy-aware protocols. Network failure, partial or wholly, may not only be due to the power exhaustion of the sensor nodes. A group of sensor nodes may be intentionally destroyed, leading to area failures in a SWSN which must be studied along with the failure distribution of power-deprived sensors. The effect of the sensor failures on the QoS is an open research topic. Since sensor failures are common, fault tolerance of the network should be investigated because loss of individual sensor nodes or a group of sensor nodes should not hamper the task accomplishment of the network.

After defining the challenges of the surveillance wireless sensor networks briefly, the addressed problems and the contributions in this thesis are:

- After deploying sensors to a field, the sensing coverage may bear sensing holes or breach paths. In this thesis, we define the weakest breach path problem. The least secure path that a target may follow is referred to as the weakest breach path. The solution is provided to the weakest breach defined as an optimization problem which may be represented as a linear program (Chapter 2).
- The primal functionality of the SWSN is to sense the environment to detect unauthorized traversals. Hence, analysis of the quality of the deployment is the main problem addressed in this thesis. We propose various deployment quality measures. These measures are based on probabilistic sensor models. Many factors have an impact on the deployment quality. The analyzed factors that affect the

deployment quality are: sensor decision fusion, deployment schemes, obstacles in the field, non-uniformity of the field shape (Chapter 3).

- Before deploying the sensors to a field, determining the required number of sensors is an open research topic. An analytical deployment quality measure is developed to determine the required number of sensors before deployment. Furthermore, the redundancy in terms of sensing and communication functionalities of the sensor nodes are analyzed (Chapter 4).
- Although the SWSNs are equipped with energy-efficient devices and protocols, the sensors die when their power diminishes. The lifetime of the network is mostly based on the dead sensor ratio. However, as long as the primary functionality is carried out, the SWSN can be considered operational. The effect of the disposed sensors on the deployment quality is analyzed during the lifetime of the network. And the network lifetime is defined based on the deployment quality measures. Deploying only the required number of sensors without redundancy to provide the initial deployment quality threshold is the best strategy in terms of the network lifetime (Chapter 5).

1.4. Literature Review

Since sensors may be spread in an arbitrary manner, one of the fundamental issues in a wireless sensor network is the coverage problem. In general, this reflects how well an area is monitored or tracked by sensors. Due to the large variety of sensors and applications, coverage is subject to a wide range of interpretations. In general, coverage can be considered as the measure of quality of sensing of a sensor network.

The coverage problem in wireless sensor network is defined as to place sensor devices in the field-of-interest so that the entire area is covered in [27] and reduced to two sub-problems: floor-plan and placement. The floor-plan problem is to partition the service area into well-defined geometric cells, where the placement problem is to assign the sensor devices into a set of cells. The proposed model transforms the search space from a continuous into discrete and reduces the complexity of the coverage problem.

In [28], the authors formulate the coverage problem as a decision problem, whose goal is to determine whether every point in the field-of-interest of the sensor network is covered by at least K sensors, where K is a given parameter. The sensing ranges of sensors can be unit disks or non-unit disks. The authors present polynomial-time algorithms, in terms of the number of sensors, to analyze the sensing coverage. With the proposed techniques, insufficiently covered areas in a sensor network can be determined, fault-tolerant capability in hostile regions can be enhanced, and energies of redundant sensors in a randomly deployed network can be conserved.

In a SWSN, the region to be monitored may be a large perimeter that might be several kilometers. Before deploying sensors in the field, the perimeter may be segmented to deal with the complexity. Segmentation can be done according to the environmental properties of the perimeter such as altitude and topography. Segmentation is beyond the scope of this thesis, and we deal with a single segment. Obstacles in the field have a significant impact on the sensing performance. In [29], a field model that includes obstacles is proposed, where the deployed sensors have various randomly distributed sensing ranges and are mobile to recover from the individual node failures. Sensing coverage is generally calculated by using a grid-based field model [19,20]. The positions of the sensors influence the sensing coverage [21]. In general, dense and highly redundant sensor deployment is preferred to ensure robustness. A probabilistic approach is presented for determining the number of sensors necessary to operate at a desired probability of detection with and without considering the sensor correlations in [17] and [30], respectively.

Most of the time, the area under investigation is irregular in shape. The field to be monitored is usually narrow and long in perimeter security applications. Thus, non-uniform deployment may be necessary. He *et al.* provide the lessons-learned from a running energy-efficient surveillance wireless sensor network [31]. One of the most significant conclusions of that work is that the sensor nodes generate false alarms at a non-negligible rate. They categorize the false alarms into transient and persistent ones. It is concluded that an exponentially weighted moving average on the sensor node is sufficient to eliminate transient alarms. To overcome the individual persistent false

alarms, in-network aggregation is proposed. In the worst case, the spatial-temporal correlations of the alarm reports at the sink should be analyzed. This conclusion suggests the SWSN performance evaluation must take into account the false alarms.

In [32], Megerian *et al.* define the worst and the best case coverage of a WSN when homogeneous sensors are deployed. The intruder (or target) wants to avoid the sensors. Thus, passing far from the sensor is beneficial from his/her viewpoint. The worst case coverage (maximal breach path) is defined with the quality of sensing measure defined as the closest distance to the sensors while the intruder passes the field. A similar problem derived from the worst case coverage definition is to find a quality of sensing measure defined as the farthest distance to the sensors when the agent wants to stay as close as possible to the sensors. This problem is referred to as the *best case coverage* (maximal support path) problem. Traditionally, Voronoi segmentation is utilized to solve these problems. Voronoi tessellation of a discrete set of sensors distributed in the Euclidean space determines the sets of points closest to each of the sensors. In [33], Megerian *et al.* introduce the exposure concept as the ability to observe a target moving in a sensor field. By expressing the sensibility of a sensor in a generic form, the field intensity is defined as the sum of the active sensor sensibilities. The exposure is then defined as the integral of the intensities (involving all sensors or just the closest one) on the points in a path in the sensor field. Next, they develop a method to calculate the minimum exposure path between any two points in a sensor field. However, some important questions are left unanswered. It is not clear what the threshold value of the minimum exposure has to be for determining the required number of sensor nodes. Determining the threshold becomes too complex when different types of sensors are utilized.

The effect of sensor deployment on the performance of target detection is considered in [19, 20], where the authors propose a measure of goodness of deployment, namely the path exposure which is the likelihood of detecting a target that traverses the region using a given path. The unauthorized traversal problem is defined, and an incremental sensor deployment strategy is proposed. Zou and Chakrabarty propose a virtual force algorithm to increase the coverage after an initial random deployment of

sensors [21]. The problem is stated as maximizing the coverage area within a cluster subject to a given number of sensors. In both papers, the area to be monitored is a rectangular field. However, most of the time, the area under surveillance is irregular in shape. Considering the perimeter security applications, the field to be monitored is usually narrow and long. Therefore, non-uniform deployment must also be considered. An incremental sensor deployment strategy is proposed in [26], where there are no prior models of the static environment, and all of the sensors are identical and are able to communicate with a remote base station. The proposed algorithm runs to maximize the coverage area while maintaining full line-of-sight connectivity, and it is shown to produce similar coverage results as the model-based algorithms. The authors analyze the trade-offs in sensor network infrastructure in [18], where continuous update and phenomenon-driven application level scenarios are analyzed by considering accuracy, latency, energy efficiency, good-put (ratio of total packet count received by observer to the total packet count sent by all sensors) and scalability as the performance measures. It turns out that there is no appreciable difference between grid-type deployment and random deployment; yet, biasing density to target movement pattern increases accuracy.

The quality of detection achieved by a SWSN can be quantified by evaluating the probability of detecting a mobile target crossing a field of interest. The detection probability of mobile targets when a set of sensors are randomly deployed to monitor a field of interest is analyzed analytically in [34]. The authors map the target detection problem to a line-set intersection problem and show that the detection probability depends on the length of the perimeters of the sensing areas of the sensors and not their shape.

Another approach to the unauthorized traversal problem is finding the path which is as far as possible from the sensor nodes [35]. In this research, maximum breach path and maximum support path problems are formulated. In the maximum breach path formulation the objective is to find a path from the initial point to the destination point where the smallest distance from the set of sensor nodes is maximized. In the former problem, the longest distance between any point and the set of sensor nodes

is minimized. To solve these problems, Kruskal's algorithm is modified to find the maximal spanning tree, and the definition of a breach number tree is introduced as a binary tree whose leaves are the vertices of the Voronoi graph.

The weakest breach path is also referred to as the best coverage problem in [36]. The energy considerations are modeled, a graph is created and the distributed Bellman-Ford algorithm is used to find the shortest path. Several extensions to the solutions are provided such as finding the best path with the minimum energy consumption and finding the path where the length is bounded. The main difference of this study and [37] is that the latter is a centralized algorithm.

Chvatal's art gallery problem [38] is to determine the minimum number of guards required to cover all points in a gallery. The similarity between the art gallery and sensor placement problems is established in [39], where the algorithms are proposed to find effective locations for the sensor nodes. One algorithm tries to maximize the average coverage of the grids and the other tries to maximize the coverage of the least effectively covered grid. The goal is to determine the required number of sensor nodes and their places to provide a coverage threshold that defines the confidence level of the deployment. These algorithms outperform the random and uniform deployment schemes. Given the sensor and target characteristics, an exposure-based model to find the required number of sensor nodes is presented in [40]. Specifically, a scheme is developed to determine the density of sensors for complete coverage. The model incorporates a mobile target that moves on a straight line.

In [22], a coverage configuration protocol is presented that provides varying degrees of coverage depending on the application. Defining the coverage as the monitoring quality of a region, an analysis of the sensing coverage and communication connectivity is provided in a unified framework rather than an isolated one. A binary detection model is used in this work, where a sensor node detects a target if the Euclidean distance between the target and the node is less than a sensing range. By defining the sensing domination as the contribution to the sensing coverage of a wireless sensor network, a scheduling algorithm is proposed in [41]. In this scheme the sensor

nodes calculate their sensing dominations and schedule themselves probabilistically. It is stated that with the same energy consumed, better coverage can be provided. In order to calculate the sensing domination, the authors propose the sensing accuracy model which is a function of distance and depends on the sensor characteristics. For any point, the detection probability is calculated as one minus the product of miss probabilities which is calculated using the sensing accuracy model. Then, the sensing coverage of the field is defined to be the sum of these probabilities.

In another work, given the initial placements of sensor nodes, an algorithm is proposed to find the placement and roles to maximize the lifetime of the network [42]. The roles could be to sense or to relay. In [43], the limit of the sensor network lifetime that all scheduling algorithms can possibly achieve is explored. Assuming that the sensor nodes fail only because of power depletion and the positions of the sensor nodes are drawn from a Poisson point process, the authors provide an upper bound derivation based on the theory of the coverage process. The wireless sensor network is assumed to live as long as a predetermined portion of the field is covered by at least one sensor node. Based on the simulations, the authors conclude that the proposed upper bound applies not only to large scale sensor networks but also to small scale ones.

During the deployment phase of a WSN, the crucial parameters are the sensing and communication ranges of the sensors, which are assumed equal in [25]. It is stated in [25] that maintaining the full coverage of the area requires finding the area dominating set, which is the smallest subset of sensor nodes that are active to cover the area. In this work, they modify the dominating node set protocol to find the area coverage and state their future work as to study sensor networks where communication and sensing ranges are different because the authors believe that it is advantageous when the sensor nodes have a communication range larger than the sensing range. If the least number of sensor nodes that cover a region is K, then the coverage is of K degrees. In [22], it is shown that for a set of sensor nodes that provide at least one degree of coverage on a convex region, the communication graph is connected if the communication range of sensor nodes is greater than or equal to twice the sensing range [44].

In [45], the authors analyze the usage of various sensors with different sensing ranges and its effect on the power consumption. During the lifetime of the WSN, not only the wireless communication consumes power, but also the sensing activity drains the power away. Although, the power consumed to sense can be accepted as negligible in comparison to the consumed level during communication, the sensor may require more samples per decision. Taking more samples, increases the reliability of the sensor and the power consumption.

Although sensing is the main functionality of a SWSN, it is useless without the ability to communicate data [46, 47]. The sensing and communication coverage problems are addressed separately [48]. Optimization of the sensing coverage and analysis of the deployment quality measure should be carried out in conjunction with the communication requirements. Because SWSNs suffer from the malfunctioning of sensors, the sensing and communication capabilities are dynamic. The deployment quality measures may change within the lifetime of the network as a result of sensor failures. Cross-layer design of the communication protocols that considers the sensing functionality is inevitable. It is claimed that if binary detection is assumed, the communication range of a sensor must be at least twice the sensing range [48]. This argument must be rigorously tested for propagation environments with topographies and obstacles that affect the communication and the sensing functionality at the same time. Sensing and communication coverage of the nodes should be modeled for three-dimensional space that contains topographical and man-made obstacles, which block the line-of-sight [49].

Energy saving is one critical issue for sensor networks since most sensors are equipped with non-rechargeable batteries that have limited lifetime. To extend the lifetime of a sensor network, one common approach is to dynamically schedule sensors' duty cycles. In general, these energy-efficient scheduling mechanisms (also called topology configuration mechanisms) need to satisfy certain application requirements while saving energy. In [50], Wang and Xiao provide a survey on energy-efficient scheduling mechanisms in sensor networks that have different design requirements than those in traditional wireless networks. The mechanisms are classified based on their design assumptions and design objectives. Different mechanisms may make different assump-

tions about their sensors including detection model, sensing area, transmission range, failure model, time synchronization, and the ability to obtain location and distance information. They may also have different assumptions about network structure and sensor deployment strategy. Furthermore, while all the mechanisms have a common design objective to maximize the network lifetime, they may also have different objectives determined by their target applications [22–24]. Coordinated operation with a well-designed sleep scheduling reduces the energy consumption. For surveillance applications sleeping sensors may produce insecure regions in the field. The primary concern in designing a sleep scheduling for surveillance wireless sensor networks is maintaining the coverage area. For example, Lui *et al.* proposes a scheduling algorithm without accurate location information subject to sensing coverage and connectivity requirements [51]. For a given coverage degree, they propose a lower bound on the required number of sensors to provide a coverage intensity level. Coverage intensity is defined as the ratio of active time to the total time where the points in the field is covered with at least one active sensor. Other scheduling works considering sensing coverage are proposed by Ren *et al.* in [52] and by Hsin and Liu in [53].

Wang *et al.* consider the coverage problem for target detection applications in wireless sensor networks in [54]. Unlike conventional coverage problems which assume sensing regions are disks around sensors, the authors define the sensing region according to detection constraints in terms of false alarm probability and missing probability and show that exploiting cooperation between sensors can extend the overall sensing region while maintain the same constraints on false alarm probability and missing probability. They propose an energy efficient cooperative detection scheme and study the tradeoffs on energy consumption between cooperative and non-cooperative schemes and put forward that cooperation reduces the number of sensors to cover the area by 30 per cent and increase the network lifetime by nearly 70 per cent.

Since sensors have significant power constraints, energy efficient protocol development for wireless sensor networks is a well studied topic [55]. Medium access protocols (MAC) influences the communication mechanisms through the radio module which consumes most of the energy. In [56] and [57], a discussion of medium access con-

trol in wireless sensor networks is provided. The network layer protocols are surveyed in [58, 59]. Sensors are prone to failures and the topology of the network changes in time. Chen *et al.* propose a highly accurate faulty sensor identification algorithm for WSNs [60].

2. WEAKEST BREACH PATH PROBLEM

In this chapter, we describe the weakest breach path problem and formulate it as an optimization problem. Using different sensor detection models, we present how to find the sensing coverage.

2.1. Weakest Breach Path Problem Formulation

The security level of a SWSN can be described by the breach detection probability, which is defined as the maximum detection probability of an unauthorized target passing through the field via the weakest breach path. We define the weakest breach path problem as finding the breach detection probability of the weakest path in a SWSN. To calculate the breach detection probability, one needs to determine the sensing coverage of the field in terms of the detection probabilities.

In this section, we present how the weakest breach path problem is formulated. The sensors are placed in the field using several deployment schemes. Then, assuming that the sensor positions are known, the sensing coverage graph is constructed. Using these models, we formulate the weakest breach path problem as an optimization problem that can be converted to a linear program by using a transformation function. As a solution to this problem, we apply Dijkstra's shortest path algorithm.

2.1.1. Field Model

In order to simplify the formulations, we model the field as a cross-connected grid. A sample field model is presented in Figure 2.1. The field model consists of the grid points and two auxiliary nodes which are the starting and the destination points. The aim of the target is to breach through the field from the starting point that represents the insecure side to the destination point that represents the secure side. The horizontal axis is divided into $N-1$ and the vertical axis is divided into $M-1$ equal parts. Thus, there are NM grid points plus the starting and destination

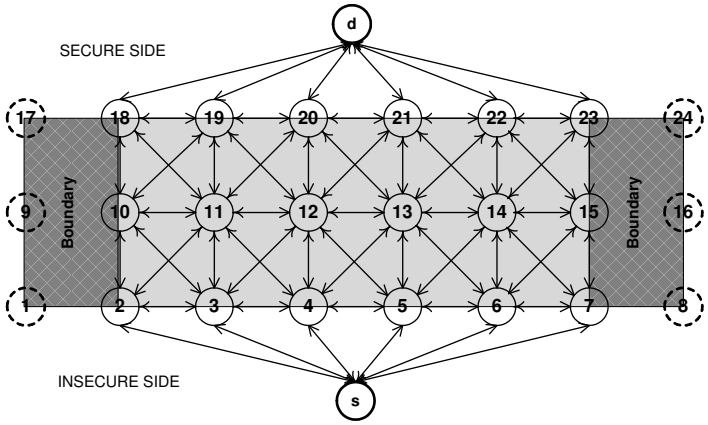


Figure 2.1. A sample field model constructed to find the breach path

points. In order to simplify the notation, instead of using two dimensional grid point indices (x_v, y_v) where $x_v = 0, 1, \ldots, N-1$ and $y_v = 0, 1, \ldots, M-1$, we utilize a one dimensional grid point index v which is calculated as $v = y_v N + x_v + 1$. For the starting point, $v = 0$, and for the destination point, $v = NM + 1$. In order to represent the connections of the grid points which a target uses to proceed through the field, the connection matrix $c_{v,w} \in \mathbf{C}_{(NM+2)\times(NM+2)}$ is defined as

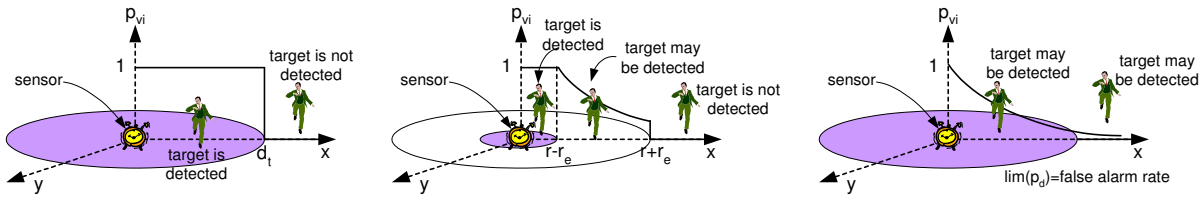
$$c_{v,w} = \begin{cases} 1 & \text{if } 0 < v, w < NM+1 \text{ and } (x_v - x_w, y_v - y_w) \in D, \\ 1 & \text{if } v = 0 \text{ and } y_w = 0, \\ 1 & \text{if } w = N \times M + 1 \text{ and } y_v = M - 1, \\ 0 & \text{otherwise,} \end{cases} \tag{2.1}$$

where $D = \{\{-1, 0, 1\} \times \{-1, 0, 1\}\} - \{(0, 0)\}$ which is the set of possible difference-tuples of the two-dimensional grid point indices excluding $v = w$. The first condition of the partial function of connection matrix $\mathbf{C}$ states that each grid point (excluding the starting and destination points) is connected to the grid points which are either one-hop away or cross-diagonal. The second condition states that the starting point is connected to all of the initial horizontal grid points of the field. The third condition states that all of the final horizontal grid points are connected to the destination point. Otherwise, the two grid points are not connected.

Using this field model, the detection probabilities are to be computed for each grid point to find the breach detection probability. In order to determine the detection probabilities, the sensor models must be first defined.

2.1.2. Sensor Models

In this thesis, we consider the Neyman-Pearson (NP) detector and Elfes's sensor detection model. NP detector is optimal in the sense that it maximizes the detection probability subject to a preset false alarm rate. The accompanying hypothesis testing model is attractive because it accommodates signal propagation and noise characteristics, as well as false alarms. For those sensor types where the NP formulation is hard to evaluate, impractical, or inappropriate, we resort to Elfes's sensor detection model [21, 61].



(a) Binary detector (b) Elfes's model (c) Neyman-Pearson detector

Figure 2.2. Sensor models

2.1.2.1. Binary Detector. Binary detector is the most common model in WSN research. The sensing coverage of a sensor is modeled as an isotropic disc with radius d_t. As shown in Figure 2.2(a), if the trajectory of target intersects with any disc, it is assumed to be detected. As experimented by Cao *et al.* in [62], the sensing capability of the passive infrared sensors (PIR) is not isotropic and the sensing ranges for any direction can be modeled with normal distribution. But, for PIR sensors if the sensor-to-target distance exceeds the sensing range around 3 - 7 per cent, the detection performance decreases sharply. The latter result shows that PIR sensors can be approximated with the binary detection model. Many works are based on isotropic

binary detection assumption because of its analytical simplicity. Such a simplification may be acceptable for indoor deployment, especially when line-of-sight is ensured.

2.1.2.2. Neyman-Pearson Detector. The optimal decision rule that maximizes the detection probability subject to a maximum allowable false alarm rate α is given by the Neyman-Pearson lemma [63]. Two hypotheses that represent the presence and absence of a target are set up. The Neyman-Pearson detector (NPD) computes the likelihood ratio of the respective probability density functions, and compares it against a threshold which is designed such that the false alarm constraint is satisfied. Suppose that passive signal reception takes place in the presence of additive white Gaussian noise (AWGN) with zero mean and variance σ_n^2, as well as path-loss with path loss exponent η. Each breach decision is based on the processing of L data samples, which are collected fast enough so that the sensor-to-target distance remains about constant throughout the observation epoch. Let d_{vi} be the Euclidean distance between the grid point v and the sensor node i. Then, as depicted in Figure 2.2(c), given the NP formulation with false alarm rate α, the detection probability of a target at grid point v by sensor i is

$$p_{vi} = 1 - \Phi\Big(\Phi^{-1}(1-\alpha) - \sqrt{\gamma L d_{vi}^{-\eta}}\Big) \tag{2.2}$$

where $\Phi(x)$ is the cumulative distribution function of the zero-mean, unit-variance Gaussian random variable at point x [17]. The distance d_{vi} is doubled in case of active sensing. In Equation 2.2, $\gamma = \frac{A\psi}{\sigma_n^2}$ controls the per-datum signal-to-noise power ratio (SNR) where the sensor node transmits with power ψ, and A is a constant that accounts for antenna gains, propagation losses, etc.

For outdoor environments such a sensor like the micro-power impulse radar (MIR) can be used. MIR is a low-power system that uses ultra-wideband pulses [64]. MIR sensors can be used for intrusion sensing, and perimeter security. It is possible to integrate this radar with a transceiver and a processor to build a wireless sensor node [65]. Commercial MIR devices are available that detect motion up to 18 meters. MIR sensors can be modeled with the Neyman-Pearson detector as in Equation 2.2.

2.1.2.3. Elfes's Model. This sensor detection model was first proposed by Elfes in [61]. The detection probability is defined such that different sensor types are represented by generic parameters. Specifically, the probability that sensor i detects a target on grid point v is

$$p_{vi} = \begin{cases} 1 & \text{if } r - r_e \geq d_{vi}, \\ e^{-\lambda a^{\beta}} & \text{if } r_e > |r - d_{vi}|, \\ 0 & \text{if } d_{vi} \geq r + r_e, \end{cases} \tag{2.3}$$

where r_e ($r_e < r$) is a measure of uncertainty in sensor detection, λ and β are parameters that model different sensor characteristics, d_{vi} is the sensor-to-target distance and $a = d_{vi} - r + r_e$ (see Figure 2.2(b).). The parameters r, r_e, λ and β are adjusted according to the physical properties of the sensor. In particular, r and r_e affect the threshold distances of target detection. When the sensor-to-target distance is smaller than $r - r_e$, the target is absolutely detected. When the sensor-to-target distance is larger than $r + r_e$, the target cannot be detected. This model is hereafter referred to as Elfes's sensor detection model (ESDM). Sample sensor detection probabilities are depicted in Figure 2.3.

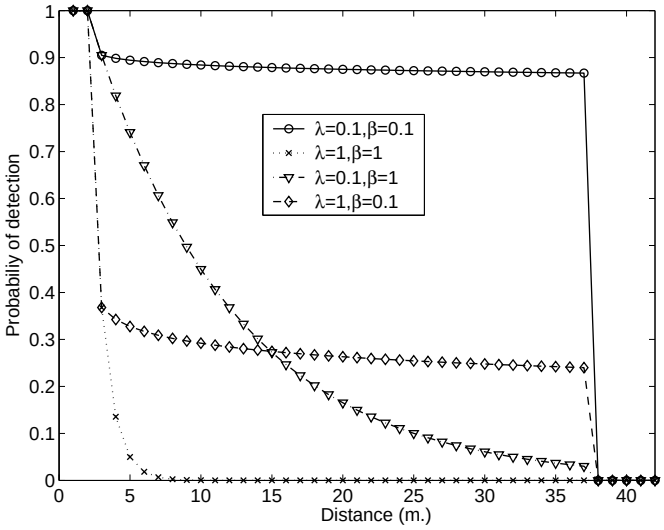


Figure 2.3. Sample detection probabilities for Elfes's sensor detection model with $r = 20$ meters and $r_e = 18$ meters

2.1.3. Coverage Model

When a decision about the presence/absence of a target is to be made, the individual decisions of a subset of sensors may be highly correlated, particularly if the deployment is dense. That is, if a sensor detects a target, it is very probable that another sensor which is at about the same distance will also detect the same target assuming homogeneous SNR and propagation conditions. From a network viewpoint, what matters is the performance of the sensor with the best detection capability. Consequently, we define the detection probability of a target on grid point v as

$$p_v = \max_{1 \leq i \leq R} p_{vi} \tag{2.4}$$

for such a correlated coverage where R is the number of sensor nodes deployed in the field. Using the two-dimensional field model and adding the detection probability as the third axis, we obtain hills and valleys of detection probabilities. With the field, sensors and the coverage model defined, we can now formulate the weakest breach path problem.

2.1.4. Weakest Breach Path Problem

The weakest breach path problem can be defined as finding the permutation of a subset of grid points $V = [v_0, v_1, \ldots, v_k]$ with which a target traverses from the starting point to the destination point with the least probability of being detected where $v_0 = 0$ is the starting point and $v_k = NM + 1$ is the destination point. The nodes v_{j-1} and $v_j,\ j = 0, 1, \ldots, k$, are connected to each other where $c_{v_{j-1}, v_j} = 1$. Here, we can define the breach probability P of the weakest breach path V as

$$P = \prod_{\forall v_j \in V} (1 - p_{v_j}) \tag{2.5}$$

where p_{v_j} is the detection probability associated with the grid point $v_j \in V$. A sample sensing coverage graph and breach path is shown in Figure 2.4.

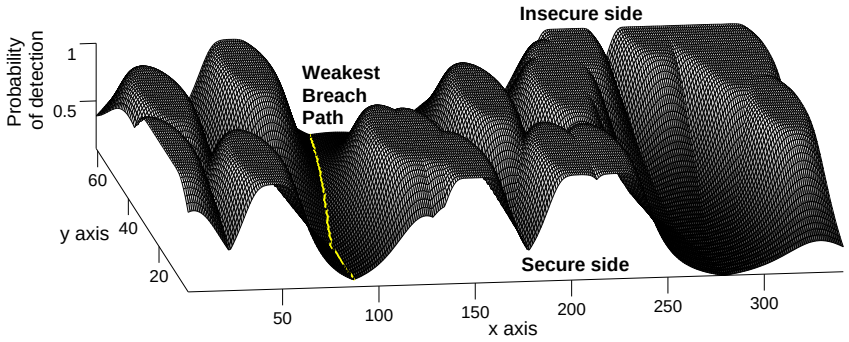


Figure 2.4. Sample sensing coverage and breach path, where the length, width, boundary size and grid size are 260 m., 60 m., 20 m. and 1 m., respectively. Twenty Neyman-Pearson detectors are deployed with $\alpha = 0.01, \eta = 2, \gamma = 30$ dB and $L = 100$

On this sensing coverage graph, one can find the weakest breach path by solving the following optimization problem: Find

$$\max \prod_{(i,j)\in\mathbf{C}} (1 - p_i) x_{ij} \tag{2.6}$$

subject to

$$\sum_{(s,j)\in\mathbf{C}} x_{sj} = 1,$$

$$\sum_{(i,d)\in\mathbf{C}} x_{id} = 1,$$

$$\sum_{(i,j)\in\mathbf{C}} x_{ij} - \sum_{(k,i)\in\mathbf{C}} x_{ki} = 0, \forall i, j, k = 1, 2, \ldots, NM,$$

$$x_{ij} = \begin{cases} 1 & \text{if } i\text{th and } j\text{th nodes are on the path and } c_{i,j} = 1, \\ 0 & \text{otherwise,} \end{cases}$$

where x_{ij} denotes the edge which originates from the ith node and terminates in the jth node, s is the starting node and d is the destination node and $\mathbf{C}$ is as defined in Equation 2.1. Thus, in this formulation, the objective is to maximize the breach probability P defined in Equation 2.5. By utilizing the logarithm, the optimization problem defined in Equation 2.6 can be converted to a linear program, where the objective is to find

$$\min \sum_{(i,j)\in\mathbf{C}} -\log(1-p_i)x_{ij} \tag{2.7}$$

subject to the constraints listed for Equation 2.6.

In order to solve the weakest breach path problem defined in Equation 2.7, linear programming algorithms such as simplex can be utilized [66]. However, since we construct a graph to model the field, Dijkstra's shortest path algorithm can be employed [67]. (See [33, 68, 69] for other applications of Dijkstra's algorithm in sensor networks.) The weight of the grid point v is [17]

$$d_v = -\log(1-p_v). \tag{2.8}$$

Using Dijkstra's algorithm, the breach probability can be defined as the reverse transformation of the weight d_{NM+1} of the destination point, which is

$$P = 10^{-d_{NM+1}}. \tag{2.9}$$

The found path, V can be used to calculate the miss probability of the weakest breach path as in Equation 2.5 that is equal to the breach probability value defined in Equation 2.9 or to the optimal value of the linear program defined in Equation 2.7. To determine the required number of sensor nodes for an acceptable security level pro-

vided with the sensing coverage, the breach detection probability

$$P_{BD} = \max_{\forall v_j \in V} p_{v_j} \tag{2.10}$$

is used as the measure. Analogously, the maximum detection probability in Equation 2.10 shows the highest altitude reached in the sensing coverage surface while the target follows the weakest breach path. Thus, this measure depicts the detection probability of the single most powerful sensor on the path. All other parameters being equal, it shows the closest sensor to the weakest breach path, since the breach path follows the most distant grid points to all of the sensors. In this way, it gives insight about the spread of the sensors in the field.

In the next section, the breach detection probability is analyzed as a function of signal, noise and propagation characteristics, as well as the field shape. Moreover, different deployment schemes and their impact on the performance are studied.

2.2. Analysis of the Breach Detection Probability

In this section, the breach detection probability is analyzed. The effect of the sensor parameters, sensor count and deployment scheme on the breach detection probability are presented.

2.2.1. Sensor Parameters

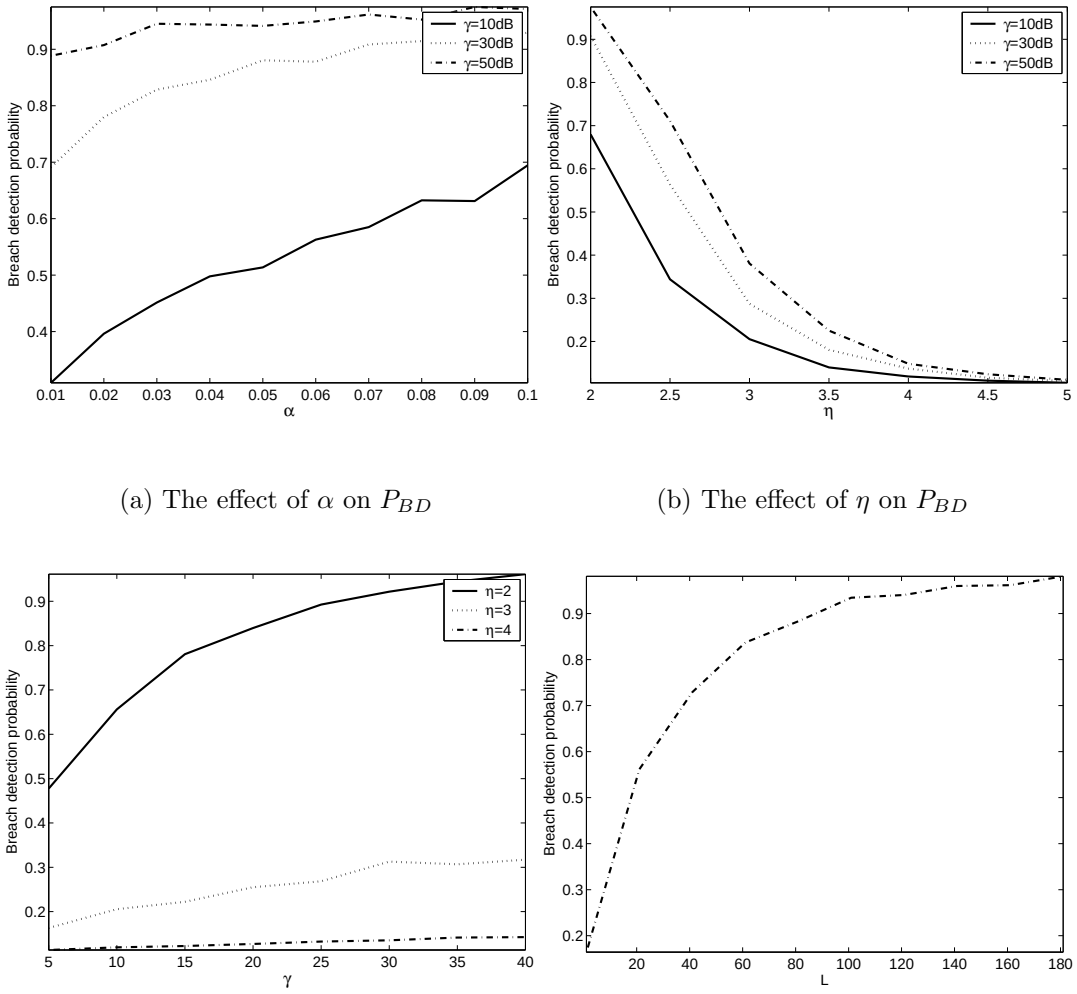
In this section, the effects of the sensor parameters on the breach detection probability are analyzed. The sensor deployment is random with uniform distribution. When the parameters are fixed, they are as in Table 2.1. When NP detection is employed, the results depict how the environmental properties and the tolerance to the false alarms change the sensing coverage and how the breach path is affected. For Elfes's model, changing the parameters models different types of sensors. The figures that are presented in the following subsections are the averages of 100 runs.

Table 2.1. Parameter values used in the simulations

Field Model	
Length	180 m.
Width	40 m.
Boundary size	10 m.
Grid size	1 m.
NPD	
α	0.1
η	2
γ	30 dB
L	100
ESDM	
r	30 m.
r_e	17 m.
λ	0.2
β	0.6

2.2.1.1. Neyman-Pearson Detection. In a field where the parameters are as in Table 2.1, 13 sensors are deployed. The effect of the false alarm rate, α, on the breach detection probability P_{BD} is shown in Figure 2.5(a), which essentially represents the network operating characteristics. With greater tolerance to false alarms, the P_{BD} performance improves, and hence the sensing range becomes larger. Sufficiently high SNR is necessary for an acceptable P_{BD} level, which is also relatively insensitive to the false alarm rate.

For environments where the signal attenuates more rapidly with distance, the breach detection probability becomes lower as shown in Figure 2.5(b). As η increases, more sensors are needed to cover the field and meet the performance requirements.



(a) The effect of α on P_{BD}

(b) The effect of η on P_{BD}

(c) The effect of γ on P_{BD}

(d) The effect of L on P_{BD}

Figure 2.5. The effect of the false alarm rate α, the path loss exponent η, the signal-to-noise ratio γ and the data size L on the breach detection probability P_{BD} in NP detection

Also note that P_{BD} level off independently of the SNR for $\eta \geq 5$, which corresponds to e.g. indoor office environment with obstructions.

As the SNR increases, the sensor detection performance improves, the miss probability of a target traversing the weakest breach path decreases, and P_{BD} increases as seen in Figure 2.5(c). Greater performance enhancement is obtained through higher transmit power, which comes at the expense of battery life, when the path loss expo-

nent is small. The curves in Figure 2.5(c) stress the impact of a cluttered propagation environment on the sensing performance, and the importance of sensor placement. The more the number of data samples, the better the precision of the sensor detection. As a result, P_{BD} increases steadily with growing data size, as shown in Figure 2.5(d). This outcome is also observed in Equation 2.2.

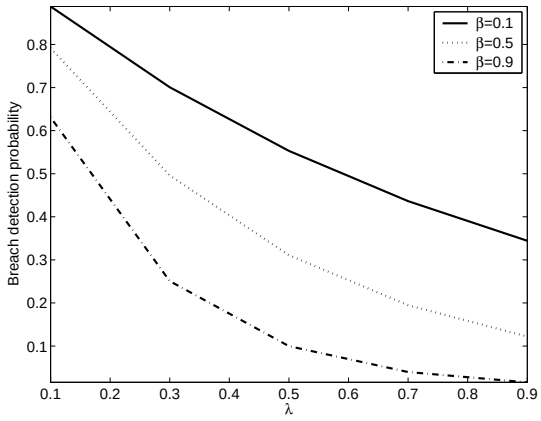


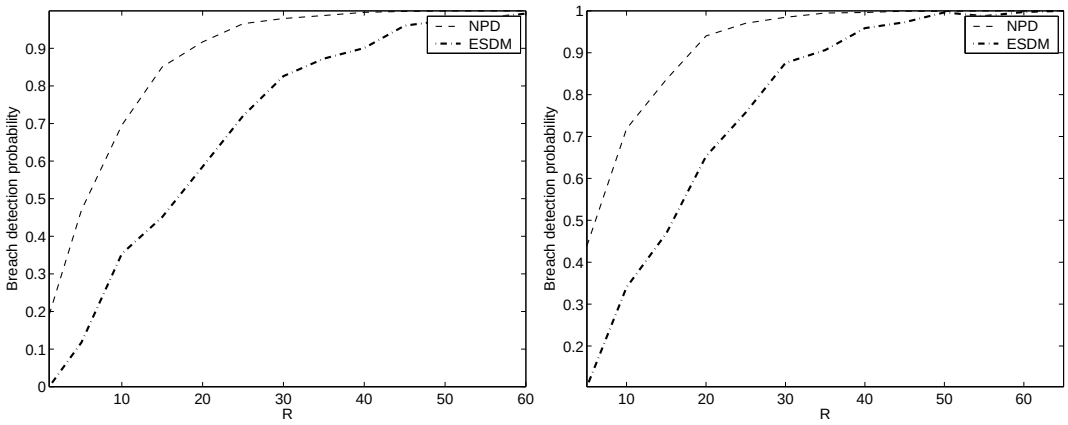
Figure 2.6. The effect of λ on the breach detection probability in ESDM

2.2.1.2. Elfes's Parameters. Elfes's sensor detection model imitates different sensor types through the parameters β and λ. The other two parameters r and r_e change the sensing ranges. ESDM is a truncated model where the detection probability is one if the target-to-sensor distance is below $r - r_e$ or zero if the target-to-sensor distance is larger than $r + r_e$. For distances in between $r - r_e$ and $r + r_e$, the slope of the sensor detection probability curve is determined by λ and β (see Figure 2.3).

For different values of β, the effect of λ on breach detection probability is shown in Figure 2.6. The field parameters and the ranges of the sensors are listed in Table 2.1. In these experiments, 43 sensors are deployed in the field to obtain a maximum detection probability around 0.95. Experiments indicate that P_{BD} is more sensitive to λ than β.

2.2.2. The Number of Sensors

Two deployment schemes are considered in this subsection: (1) uniform random deployment; and (2) uniform random x-axis and normally distributed y-axis with a mean of half the width and a standard deviation that is 10 per cent of the width. The effect of the number of deployed sensors are shown in Figures 2.7(a) and 2.7(b), respectively for the two deployment strategies described above. For the uniform random deployment, as the number of sensors grows, the density of the wireless sensor network increases. Thus, the weakest breach path is forced to pass closer to the sensors. Moreover, the grid points become more secure in terms of the detection probability, and P_{BD} approaches one in the limit of R.



(a) Uniform on both axes (b) Uniform x-axis and gaussian y-axis

Figure 2.7. The effect of the number of sensors, R, on the breach detection probability

When Figure 2.7(a) is analyzed, the maximum detection probability on the breach path is around 0.95 if 30 NP sensors are deployed as opposed to the 50 sensors required by Elfes's model. For the second deployment scheme (Figure 2.7(b)), the sensors create a barrier along the x-axis in the field, and therefore fewer sensors are required to provide the required security level.

Table 2.2. Parameter values in the simulations to determine the required number of sensors for a target breach probability level

	Parameter	LCFA	HCFA
NPD	α	0.1	0.01
	η	5	3
	γ	30 dB	30 dB
	L	100	100
ESDM	r	30	35
	r_e	17	23
	λ	0.2	0.2
	β	0.6	0.6

2.2.3. Determining the Required Number of Sensors

In this chapter, two SWSN scenarios are focused on to determine the required number of sensors for an acceptable breach avoidance performance, which is represented by P_{BD}.

Low-Cost False Alarm (LCFA) For example, a house or a factory is to be monitored for intrusion detection. In this scenario, the cost of false alarms is relatively low, e.g. police officers patrolling nearby are called in.

High-Cost False Alarm (HCFA) False alarms may involve significant personnel and finance costs, and are to be minimized. For instance, the perimeter security of some mission-critical place such as an embassy or a nuclear reactor is to be provided by a SWSN against unauthorized access. A false alarm might then trigger the transportation of special forces, or the evacuation of a residential area.

The parameter values that correspond to LCFA and HCFA are listed in Table 2.2, which can be considered as the building blocks that may be used to cover larger fields.

Considering different field sizes, the required number of sensor nodes for $P_{BD} \geqslant 0.95$ are listed in Tables 2.3 - 2.6. The boundary regions are not utilized in the simulations. The sensors are either distributed uniformly on both axes, or uniformly on the x-axis and normally distributed on the y-axis with a mean of half of the width and a standard deviation of 10 per cent of the width. The deterministic deployment is analyzed as a sub-case. Keeping the total area the same (9000 m^2), the width and the length are changed. The results listed in the following tables are the averages of 50 runs.

For the LCFA scenario, the required number of sensors to obtain $P_{BD} \geqslant 0.95$ for the uniform random deployment and the normally-distributed y-axis schemes are shown in Tables 2.3 and 2.4, respectively. To obtain a high level of breach resistance, the target, and hence the breach path must always be in close enough proximity of a sensor. Keeping the total area constant, and increasing the width produces smaller target-to-sensor distances along the x-axis. As the length decreases, fewer sensors are required as seen in the tables. In conclusion, the closest sensor along the x-axis plays a critical role because traversing the region horizontally increases the total number of grid points, and the breach detection probability increases. Since Dijkstra's algorithm tries to minimize the number of visited grid points, the breach path does not curl much in the field. Thus, the sensors that create a barrier along the x-axis play a more critical

Table 2.3. The required number of sensors $P_{BD} \geqslant 0.95$ for the LCFA scenario, where the sensors are distributed uniformly

Length	**Width**	**NPD**	**ESDM**
250	36	403	51
225	40	376	40
200	45	364	39
180	50	328	36
150	60	321	30
125	72	284	27

role. The requirement for the NPD is larger compared to ESDM because the sensing range given by NPD is smaller. However, a direct comparison of NPD and ESDM will be severely misleading. Tables 2.3 and 2.4 indicate that when the sensors are deployed following the normally distributed y-axis scheme, fewer sensors are required, because the sensors create a stronger barrier along the x-axis since they are deployed more densely in the field. The sensors which are not deployed within the field do not contribute to the breach detection task.

Tables 2.5 and 2.6 depicts the results for the HCFA scenario. Again, fewer sensors supply the required P_{BD} with ESDM compared to NPD. Although the SNR is the same as that of the LCFA scenario, the path loss exponent is smaller, signal attenuates less, and the detection probability increases. As a consequence, P_{BD} is larger with the same number of sensors for the HCFA scenario despite the higher false alarm rate allowed for LCFA. For the normally distributed y-axis deployment scheme, the standard deviation of the normal distribution is set to be the 10 per cent of the width of the field. Thus, as the width increases, the dispersion increases and the requirement changes along with the dispersion. Similar to the LCFA results, for HCFA, the normally distributed y-axis deployment scheme yields fewer sensors compared to the uniform random deployment.

Table 2.4. The required number of sensors $P_{BD} \geqslant 0.95$ for the LCFA scenario, where the sensors are distributed uniformly on the x-axis and normally distributed on the y-axis with a mean of half of the width and a standard deviation that is 10 per cent of the width

Length	**Width**	**NPD**	**ESDM**
250	36	227	34
225	40	208	33
200	45	201	32
180	50	154	24
150	60	152	26
125	72	146	17

Table 2.5. The required number of sensors for $P_{BD} \geqslant 0.95$ for the HCFA scenario, where the sensors are distributed uniformly

Length	**Width**	**NPD**	**ESDM**
250	36	121	53
225	40	117	51
200	45	113	42
180	50	110	40
150	60	101	35
125	72	93	29

2.2.4. Deterministic Deployment

Depending on the type of the application, sometimes it is possible to deploy the sensors manually. In this subsection, we present the results for grid-based uniform deterministic deployment. The number of placed sensors along the x-axis and the y-axis are proportional to the length and the width of the field, respectively. A sample

Table 2.6. The required number of sensors for $P_{BD} \geqslant 0.95$ for the HCFA scenario, where the sensors are distributed uniformly on the x-axis and normally distributed on the y-axis with a mean of half of the width and a standard deviation that is 10 per cent of the width

Length	**Width**	**NPD**	**ESDM**
250	36	104	42
225	40	107	35
200	45	114	47
180	50	94	32
150	60	70	29
125	72	54	17

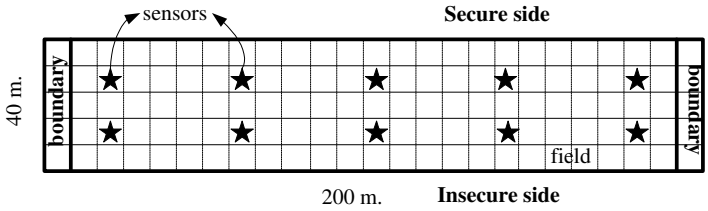


Figure 2.8. A sample field where the sensors are deployed deterministically

deterministic deployment is depicted in Figure 2.8 where the length, width, boundary and the grid sizes are 184, 40, eight and eight meters, respectively. A total of 10 sensors are employed in this sample, where two rows with five sensors each are utilized to be proportional to the length and width of the field.

When the sensors are deployed deterministically following a uniform grid topology, the required quantity is smaller than that in random deployment schemes. The main reason is that the sensing barrier is stronger with deterministic deployment, and fewer nodes satisfy the required measure.

Table 2.7. The required number of sensors to satisfy $P_{BD} \geqslant 0.95$ for the LCFA scenario, where the sensors are deterministically deployed

Length	**Width**	**NPD**	**ESDM**
250	36	195	10
225	40	175	9
200	45	192	8
180	50	196	7
150	60	192	6
125	72	200	5

Table 2.8. The required number of sensors to satisfy $P_{BD} \geqslant 0.95$ for the HCFA scenario, where the sensors are deterministically deployed

Length	**Width**	**NPD**	**ESDM**
250	36	44	11
225	40	60	10
200	45	54	9
180	50	48	8
150	60	56	14
125	72	55	6

2.3. Analysis of the Breach Probability

In this section, the impact of various parameters on the breach probability, P defined in Equation 2.5 is investigated. The sensor detections are assumed to be uncorrelated in this section. The effect of the field shape on the breach probability is also analyzed, and a method for computing the required number of sensor nodes is provided. The false alarm rate is set to 0.01 and 0.1 for HCFA and LCFA, respectively. The other parameter values are listed in Table 2.9 The grid size is taken as one meter to be able to assume that the detection probabilities of targets on adjacent grid points are independent. The results are the averages of 50 runs.

Because the NP detector ensures that

$$\lim_{d_{vi} \to \infty} p_{vi} = \alpha,$$

instead of using p_{vi}, we introduce the measure

$$p_{vi}^{*} = \begin{cases} p_{vi} & \text{if } p_{vi} \geq p_t, \\ 0 & \text{otherwise,} \end{cases} \tag{2.11}$$

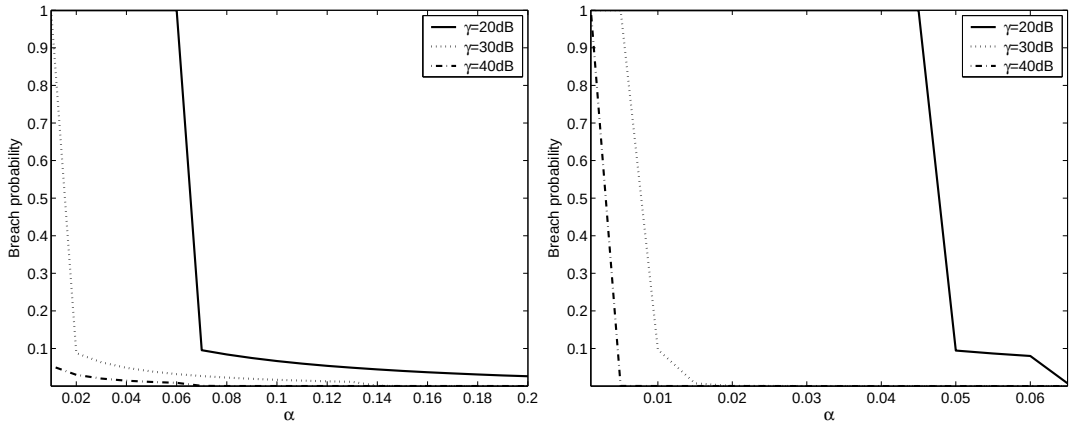
Table 2.9. Parameter values used in the simulations for the LCFA and HCFA scenarios

Parameter	**LCFA**	**HCFA**
Length	20 m.	100 m.
Width	5 m.	10 m.
Boundary	10 m.	10 m.
Grid size	1 m.	1 m.
N	41	121
M	6	11
α	0.1	0.01
η	5	3
γ	30 dB	30 dB
L	100	100
p_t	0.9	0.9
R	17	31

where $p_t \in (0.5, 1)$ is the threshold probability that represents the confidence level of the sensor. That is, the sensor decisions are deemed sufficiently reliable only at those d_{vi} distances where $p_{vi} > p_t$. Depending on the application and the false alarm requirement, typically $p_t \geq 0.9$. Note that p^*_{vi} is not a probability measure, but we shall nevertheless treat it as one in the ensuing calculations. Assuming that the sensor detections are statistically uncorrelated, the detection probability p_v at any grid point v is defined in Equation 2.4 becomes

$$p_v^I = 1 - \prod_{i=1}^{R} (1 - p^*_{vi}) \tag{2.12}$$

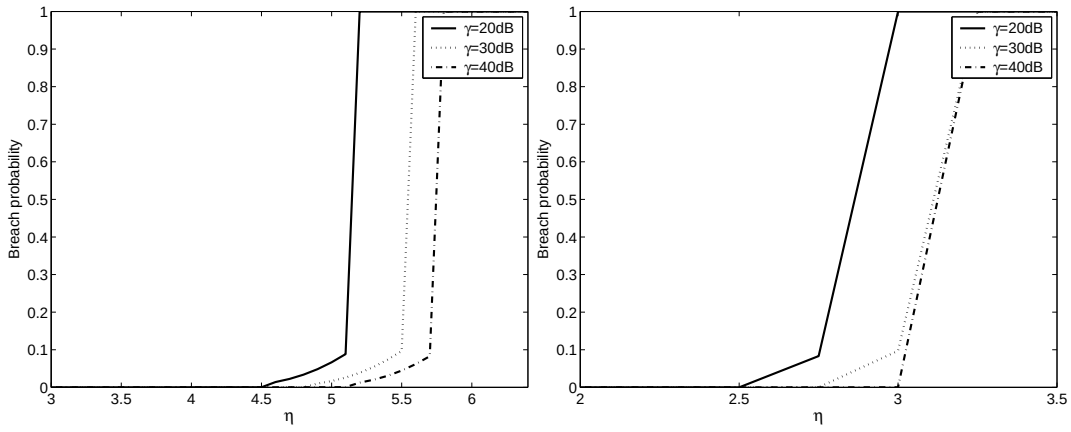
where R is the number of sensor nodes deployed in the field. The miss probabilities of the starting and destination points are one, that is $p_0 = 0$ and $p_{NM+1} = 0$. These points are not monitored because they are not in the sensing coverage area.



(a) LCFA (b) HCFA

Figure 2.9. The effect of α on the breach probability

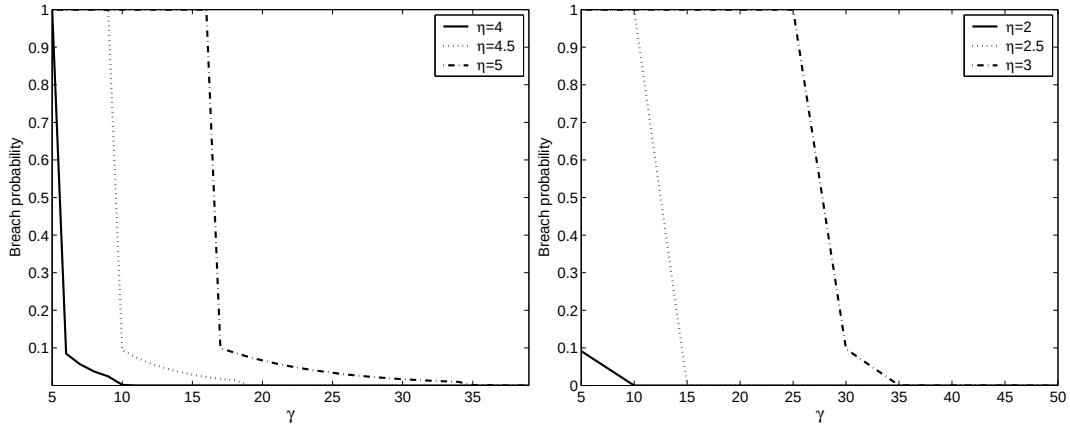
The breach probability P is quite sensitive to the false alarm rate α. As shown in Figure 2.9(a) for the LCFA scenario and in Figure 2.9(b) for the HCFA scenario, as α increases, the SWSN allows more false alarms. Because α reflects the tolerance level to false alarm errors, the NP detection probability and the detection probability p_v of the targets at grid point v both increase in α. Consequently, the breach probability decreases.



(a) LCFA (b) HCFA

Figure 2.10. The effect of η on the breach probability

For a given α and γ pair, there is an upper bound on the path-loss exponent for which a breach probability requirement can be met. When the false alarm rate is high as in LCFA, cluttered and obstructed environments are still successfully monitored by the network. For instance, Figure 2.10(a) suggests that $\gamma = 20$ dB is sufficient for $\eta = 4.5$. On the other hand, with tight control of the false alarms, the sensors must be carefully positioned to have line-of-sight (see Figure 2.10(b)).

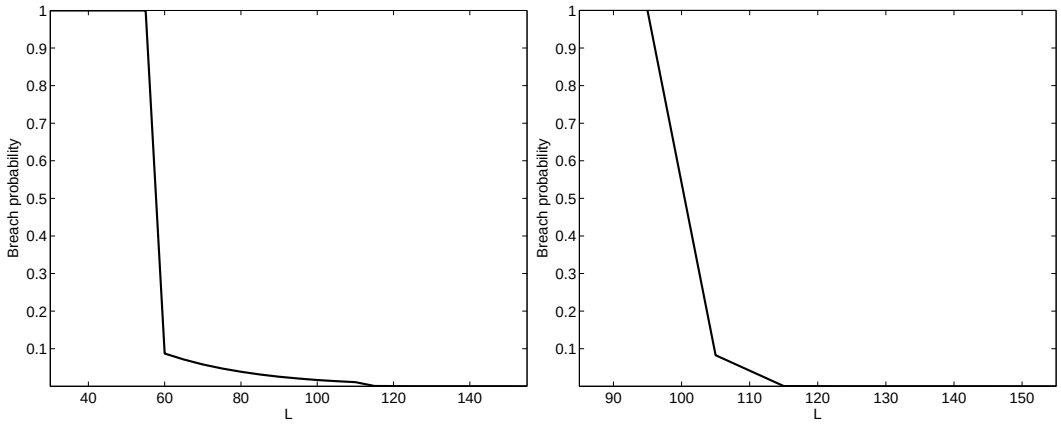


(a) LCFA (b) HCFA

Figure 2.11. The effect of γ on the breach probability

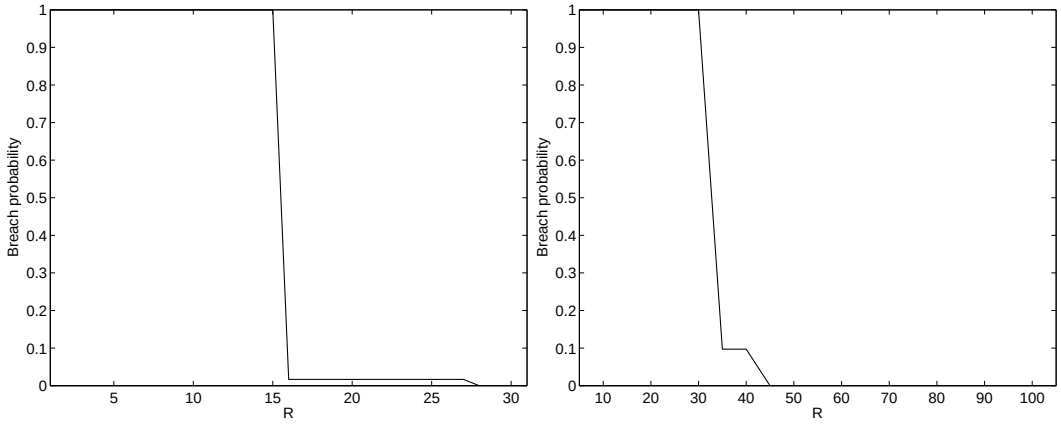
As the signal-to-noise ratio γ increases, the detection performance improves (see Figure 2.11), and the breach probability decreases. Depending on the path-loss exponent, $\gamma = 10$ dB yields minimal breach probability for both LCFA and HCFA. Note that η and γ display a duality in that if one is fixed, the performance breaks down when the other parameter is below or above some value. For example, for $\gamma = 30$ dB, $P \to 1$ as soon as η exceeds 5.5 in LCFA (Figure 2.10(a)). Similarly, for the same scenario, breach detection becomes impossible once $\gamma < 6$ dB if $\eta = 4$ (Figure 2.11(a)). The deterioration is somewhat more graceful for HCFA.

Figure 2.12(b) depicts that a data record of 60 and 115 samples per breach decision is sufficient for LCFA and HCFA, respectively, if $P \approx 0.1$ is good enough. In general, more data samples per breach decision are required if a low false alarm rate is desired. However, note that L grows asymptotically to the same quantity for both



(a) LCFA (b) HCFA

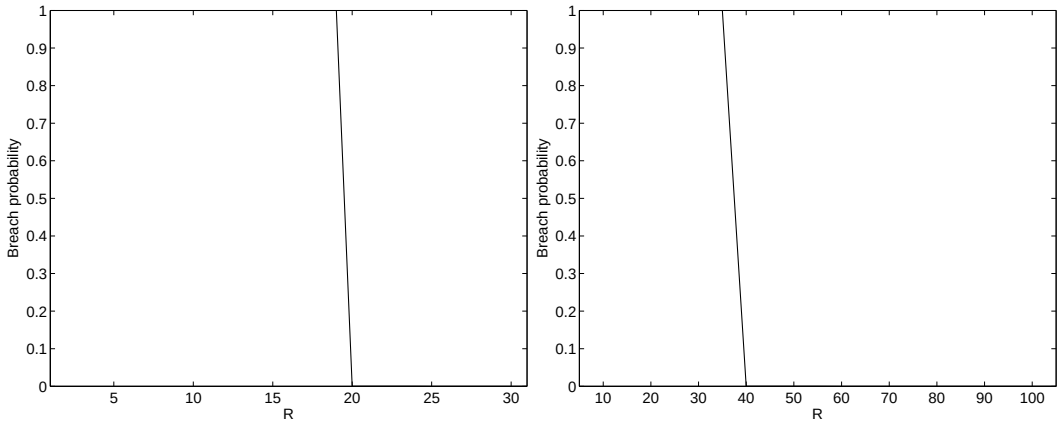
Figure 2.12. The effect of L on the breach probability



(a) LCFA (b) HCFA

Figure 2.13. The effect of the number of sensor nodes on the breach probability where the sensor nodes are uniformly distributed along both the vertical and horizontal axes

LCFA and HCFA as $P \rightarrow 0$. For active sensors, restrictions on energy consumption may prohibit collecting too many samples.



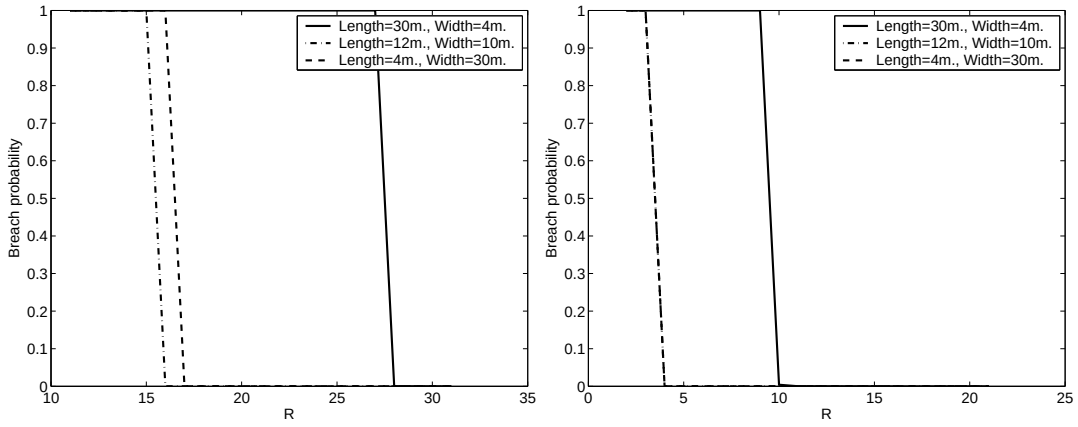
(a) LCFA. (b) HCFA.

Figure 2.14. The effect of the number of sensor nodes on the breach probability where the sensor nodes are deployed uniformly along the horizontal axis and normally distributed along the vertical axis with mean $M/2$ and a standard deviation of 10 per cent of the width of the field

2.3.1. Determining the Required Number of Sensor Nodes

While analyzing the required number of sensor nodes for a given breach probability, we consider two cases of random deployment. In the first case, we assume that the sensor nodes are uniformly distributed along both the vertical and horizontal axes. In the second case, the sensor nodes are deployed uniformly along the horizontal axis and normally distributed along the vertical axis with mean $M/2$ and a standard deviation of 10 per cent of the width of the field. In the simulations, the sensor nodes that are deployed outside the field are not included in the computations of the detection probabilities.

Considering uniformly distributed y-axis scheme, the required number of sensor nodes for a given breach probability is plotted in Figure 2.13. A breach probability of 0.01 can be achieved by utilizing 16 sensor nodes for LCFA, and 45 for HCFA. Exchanging the false alarm rates to $\alpha = 0.01$ for LCFA and $\alpha = 0.1$ for HCFA, the requirement becomes 28 and 30 sensor nodes, respectively. The rapid decrease in the



(a) LCFA. (b) HCFA.

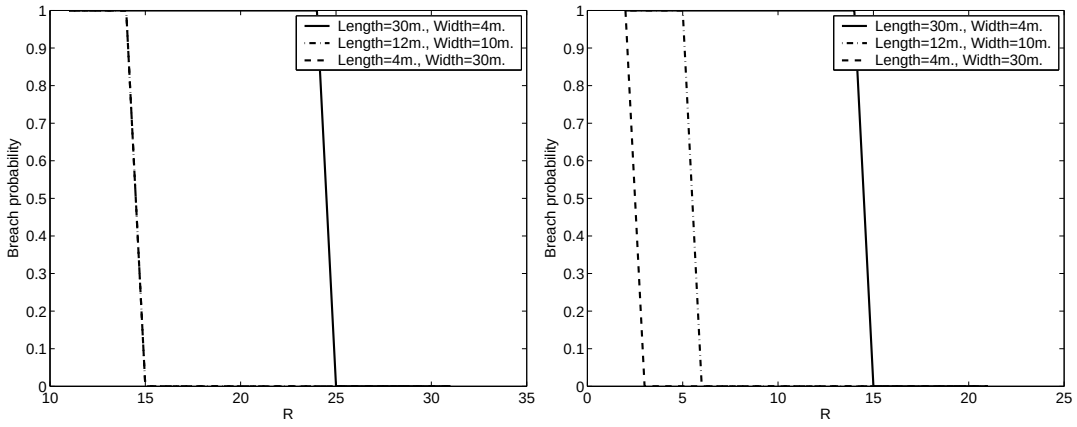
Figure 2.15. The effect of the field shape on breach probability where the sensor nodes are uniformly distributed along both the vertical and horizontal axes

breach probability at $R = 16$ in Figure 2.13(a) can be justified by the fact that most of the grid points are covered with high detection probabilities (saturated) for $R = 15$, and adding one more sensor node decreases the breach probability drastically. Once the saturation is reached, placing more sensors in the field has marginal effect.

Analyzing Figure 2.14, the above-mentioned saturation is seen more clearly for the normal-distributed y-axis scheme. For this kind of deployment, since the sensor node may fall outside the field, the breach probability decreases slower compared to the uniformly distributed y-axis scheme.

2.3.2. Effect of Field Shape on the Breach Probability

Depending on the application, the field shape of the grid model may vary. In Figures 2.15 and 2.16, the effect of the field shape on the breach probability is depicted considering uniformly and normally distributed y-axis schemes, respectively. For a given number of sensor nodes, the breach probability is larger for narrow and long fields compared to the thick and short fields. For example, when uniform random deployment on both axes are considered, with 20 sensor nodes, it is possible to provide



(a) LCFA. (b) HCFA.

Figure 2.16. The effect of the field shape on breach probability where the sensor nodes are deployed uniformly along the horizontal axis and normally distributed along the vertical axis with mean $M/2$ and a standard deviation of 10 per cent of the width of the field

a breach probability below 0.01 for a field where the length is four meters and the width is 30 meters. However, with the same number of sensor nodes the breach probability turns out to be around one for the field where the length is 30 meters and width is four meters.

In Tables 2.10 and 2.11, different grid sizes are simulated for LCFA and HCFA, respectively, and the required number of sensor nodes are tabulated for $P \leq 0.01$. As the size of the grid becomes shorter and thicker, the required number of sensor nodes decreases. For the LCFA scenario, as the field is shortened and widened, the difference between the required number of sensor nodes for the uniformly and normally distributed y_v schemes decreases. However, the largest difference is obtained for the fields where the width is the smallest. The normal-distributed y_v scheme is more determining of the required number of sensor nodes, because it produces a deployment where many sensor nodes are placed around the center line of the field along the horizontal axis. This deployment scheme produces a well-secured barrier in the middle of the field.

Table 2.10. The effect of field shape on the required number of sensor nodes for a breach probability of 0.01 for the LCFA scenario

Length (m.)	**Width** (m.)	$y_v \sim \text{Uniform}(0, M-1)$	$y_v \sim \text{Normal}(M/2, N/10)$
40	3	16	20
30	4	11	15
24	5	11	13
20	6	7	13
15	8	4	3
12	10	4	3
10	12	3	3
8	15	3	2

Table 2.11. The effect of field shape on the required number of sensor nodes for a breach probability of 0.01 for the HCFA scenario

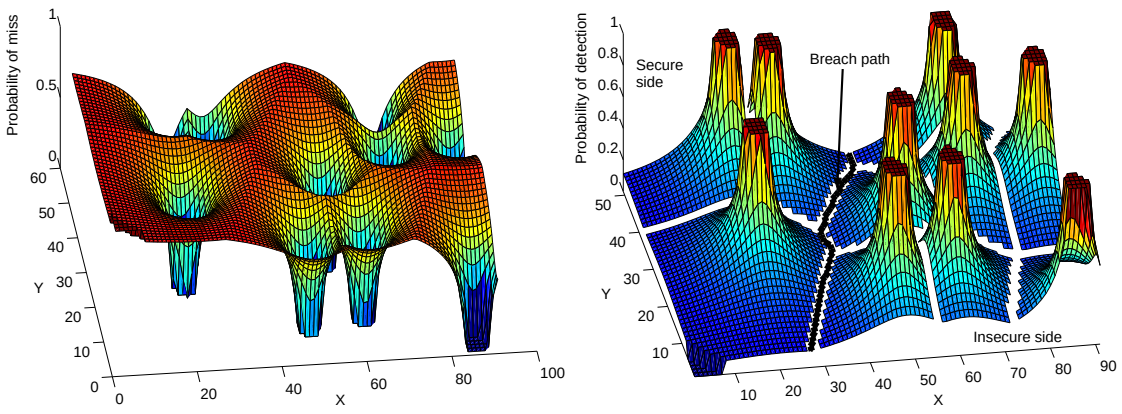
Length (m.)	**Width** (m.)	$y_v \sim \text{Uniform}(0, M-1)$	$y_v \sim \text{Normal}(M/2, N/10)$
40	3	10	13
30	4	4	3
24	5	4	3
20	6	4	3
15	8	3	2
12	10	2	2
10	12	2	2
8	15	2	2

2.4. Breach Paths as Watershed Contours

If it is assumed that the measurements of individual sensors are statistically independent, then the detection probability of a target on grid point v is

$$p_v^I = 1 - \prod_{i=1}^{R} (1 - p_{vi}) \tag{2.13}$$

where R is the total number of sensors deployed in the region. Thus, Equation (2.13) represents the so-called uncorrelated coverage model. When a decision whether a target exists is to be made, the individual decisions of a subset of sensors may be highly correlated. Then, $p_v^D = p_v$ as defined in Equation 2.4 and referred to as "correlated coverage model". The two probabilities p^I and p^D act as upper and lower bounds on the detection probability, respectively.



(a) Miss probability surface.

(b) Detection probability surface.

Figure 2.17. Miss probability surface and watershed segmentation shown on the detection probability surface where length=50 m, width=50 m, boundary=20 m., grid size=1 m., $R = 10, r = 15$ m., $r_e = 12$ m., $\lambda = 0.5$ and $\beta = 0.5$.

Using the two-dimensional field model and adding the detection probability as the third axis, we obtain hills and valleys of detection probabilities (see Figure 2.17(b)). The weakest breach path problem can be informally defined as finding the path which

follows the valleys and through which the target does not have to climb hills so much. Because, the valleys denote the lowest detection probabilities. Furthermore, regarding the two-dimensional field model as an image, where the detection probabilities of the grid points can be mapped to the gray levels of the pixels, suggests that image processing techniques can be employed.

One of the well-known image segmentation algorithms is the watershed algorithm [70]. The watershed algorithm is best-understood with an analogy to water flooding from the minimal points of a three dimensional topographic surface where the third dimension is the altitude. As the water increases, dams are built where the floods would merge. After the completion of immersion, only the dams emerge and separate the valleys. This algorithm can be easily applied to the coverage area of wireless sensor networks in order to find the possible breach paths. After deploying the sensors to the field and calculating the coverage area of the sensor network, utilizing the miss probabilities on the grid points produces hills and valleys where the altitude is mapped to the miss probability as shown in Figure 2.17(a). The minimal points of this surface is the sensor node positions. Thus, analogously, it can be considered that the water starts flooding from the sensor nodes. After applying the watershed algorithm, the contour points (dams) correspond to possible breach paths as shown in Figure 2.17(b).

Among these breach paths we still need to find the weakest one. Watershed segmentation reduces the solution space of the Dijkstra's shortest path algorithm. For this reason, a graph is constructed using only the contour points and Dijkstra's shortest path algorithm is applied. A similar approach to the one explained in [17] is used. To identify the insecure side of the region the starting node is added which is connected to all of the points on the closest line of the grid on x-axis. Similarly, the secure side is identified with the destination node and all of the contour points of the farthest line of the grid are connected to the destination point. The aim of the target is to traverse the region from the starting node till the destination node by proceeding on the contour points where the detection probabilities are the smallest among all. The boundary regions are not taken into consideration while constructing this graph, because we want the breach path pass through the field, not through the boundaries.

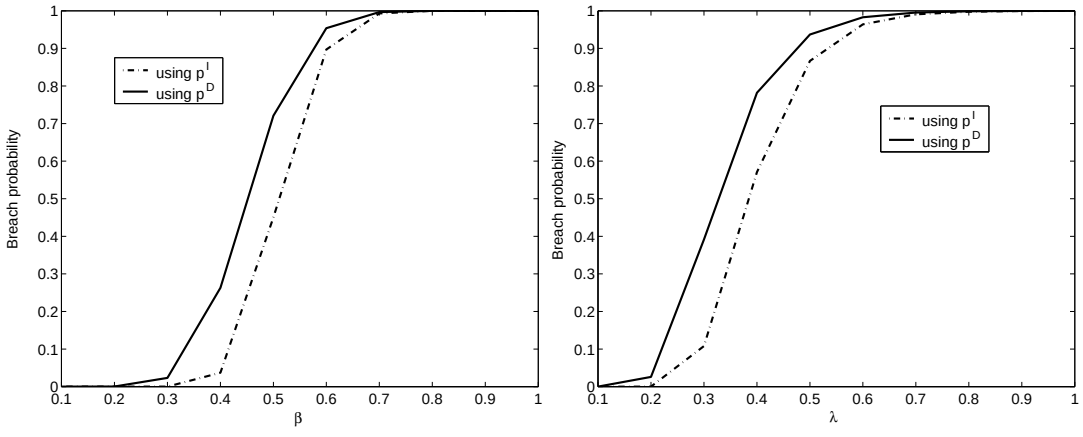
Table 2.12. Surveillance field parameters

Parameter	Length	Width	Grid size	Boundary
EPS	200 m.	50 m.	1 m.	20 m.
CBS	1000 m.	100 m.	1 m.	50 m.

2.4.1. Analysis of Breach Probability

The ESDM parameters are $r = 20$ meters, $r_e = 18$ meters, $\lambda = 0.3$ and $\beta = 0.8$. In order to analyze the watershed algorithm to find the breach paths, we use two scenarios where the fields differ in dimension defined in the previous section. These are the *Embassy Perimeter Security* (EPS) scenario, and the *Country Border Surveillance* (CBS) scenario. For these two scenarios, the field parameters are shown in Table 2.12. The grid size is taken to be one meter in the simulations.

Upon analyzing the effect of β on the breach probability for the EPS scenario, it is



(a) The effect of β ($\lambda = 0.3$). (b) The effect of λ ($\beta = 0.8$).

Figure 2.18. The effect of λ and β on breach probability for the EPS scenario where $r = 20$ m., $r_e = 18$ m

seen that selecting a sensor with a larger value for β will increase the breach probability. Holding λ constant and increasing β decreases the detection probability. Thus, the breach probability shown in Figure 2.18(a) increases in β. The same conclusion can be drawn for λ on interpreting Figure 2.18(b). The increase in the breach probability is delayed in terms of parameter increase when the sensing coverage is calculated using Equation 2.13. Furthermore, when compared to β, increasing λ causes a quicker rise in the breach probability.

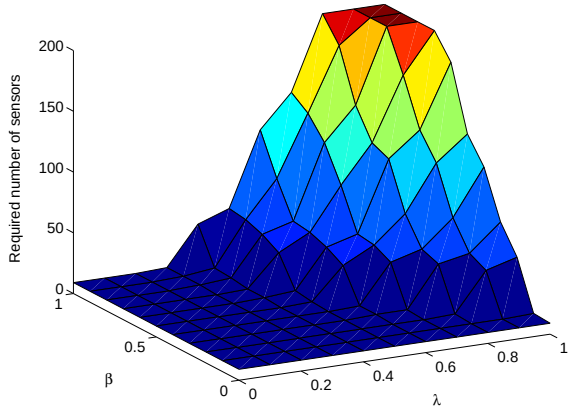
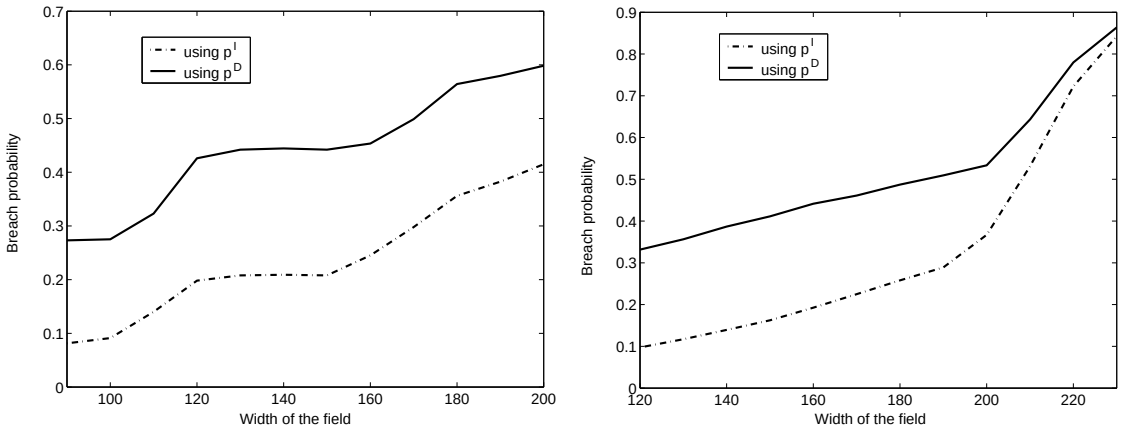


Figure 2.19. The effect of λ and β on the required number of sensors for a breach probability less than 0.01

In Figure 2.19, the required number of sensors for a breach probability less than 0.01 is shown for different sensor characteristic parameters λ and β. Extreme values of λ and β provide special detection models. For example, when $\lambda = 1, \beta = 1$ or $\lambda = 0, \beta = 0$ the sensor detection model turns out to act as a binary detection model, where the threshold value becomes $r - r_e$ and $r + r_e$, respectively. Considering this, when Figure 2.19 is analyzed, it can be concluded that the sensing range is very critical in determining the required number of sensors. Thus, while designing a SWSN, selection of sensors significantly affects the breach probability. The required number of sensors is 9 when $\lambda = 0, \beta = 0$. However, when λ and β are set to one, the requirement becomes 200. As λ and/or β increase, the breach probability grows exponentially.

Holding the required number of sensors constant, when a large field in width is analyzed, larger breach probabilities are observed (see Figure 2.20). Widening the field

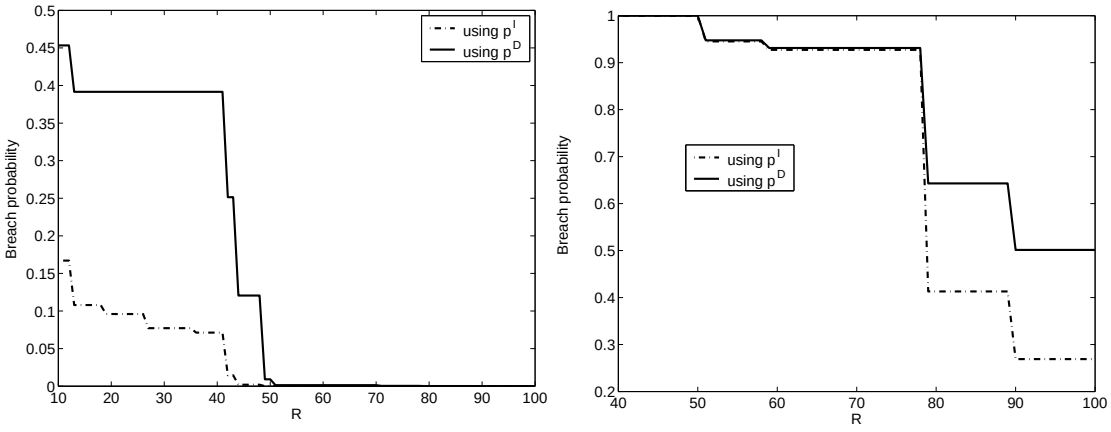


(a) EPS Scenario (15 sensors). (b) CBS Scenario (120 sensors).

Figure 2.20. The effect of the width of the field on breach probability for the EPS scenario where 15 sensors are utilized

allows a target more space with smaller detection probabilities to traverse. When the EPS scenario is compared to the CBS scenario, the increase in breach probabilities for the two sensing coverage calculation schemes is larger in CBS. Similar trends are observed for the two sensing coverage calculations in EPS, whereas for the CBS, the two breach probability curves tend to converge to one. This is because, when the width is increased in the CBS scenario, the target is able to find a path which is distant enough from most of the sensor nodes such that the minimum distance between the sensors and the path is $r + r_e$. Therefore, when the width is greater than $r + r_e$, the breach probability increases more.

To determine the required number of sensor nodes for a given breach probability level, it is crucial to analyze the effect of the number of sensors on the breach probability. Since a truncated sensor detection model is used, the breach probability remains at a constant level as long as the deployed number of sensors are not sufficient to cover the region fully. Thus, for the EPS scenario, on analyzing Figure 2.21(a), at about 15 to 40 sensors the breach probability is around 0.4. When 40 sensors are deployed to the field, the saturation or, in other words, full-coverage is achieved. Thus, at first a sharp decrease is observed when more than 40 sensors are deployed. Afterwards, the breach



(a) EPS Scenario. (b) CBS Scenario.

Figure 2.21. The effect of the number of sensor nodes on the breach probability for the EPS and CBS scenarios

probability does not seem to be affected with additional sensor deployment. The reason behind the lack of further improvement is the value chosen for the field width. Since the field width is less in the EPS scenario compared to the CBS scenario, most of the time the path does not curl in the region and flow along the x-axis. However, in the CBS scenario when Figure 2.21(b) is analyzed, considering that the same type of sensors are deployed (the detection probability is truncated to zero at a distance of $r + r_e = 38$ m.), the width of the field is twice the width of the EPS scenario. In this scenario, the path may curl and flow along the x-axis depending on the fact that smaller detection probabilities may exist. Consequently, there exist more steps in the curve of the breach probabilities in Figure 2.21(b). More clearly, the additionally deployed sensor does not have an impact on the path, because the sensor-to-path distance is larger than $r + r_e$. The steps of the curves are more straight for p^D compared to p^I. This is due to the fact that the additional sensor deployment has no effect on the detection probability of the target-on-the-path if it is not closer than the closest sensor when the sensing coverage is calculated with p^D. However, when the sensing coverage is calculated with p^I, if the distance between the additionally deployed sensor and the path is less than $r + r_e$, the deployment affects the detection probability of the target-on-the-path.

2.5. Analysis of Vertical Breach Paths

In this section, the vertical breach paths are analyzed. An analytical model for vertical path detection is presented and the biased random-way point mobility model of an intruder is analyzed.

2.5.1. Vertical Path Detection Probability

Assume a target model where the objective is to pass from insecure side of the field to the secure side following a vertical straight line. The target is positioned on a random point at the insecure side and walks on the vertical line that starts from that random point. Denote the number of randomly deployed binary detectors with R in a rectangular field where the length and the width are D_1 and D_2 meters, respectively. While the target is moving on the vertical path, if the path intersects any disk with radius equal to sensing range d_t and center as the sensor position, the target is assumed to be detected.

Calculating the path detection probability in this two-dimensional model can be reduced to a one-dimensional random line packing problem [71]. The projection of a sensor location on a line covers an interval of length $2d_t$ which is independent of the orientation of the line. Hence, using the x-axis values of the sensor positions is the projection of positions onto the horizontal line. Then, the probability of covering a line with R sensors is considered as the vertical path detection probability. Formally, consider a set of R binary detectors with range d_t meters located randomly on a line of length $D1$ meters where $2Rd_t \geq D_1$. If $2Rd_t < D_1$ then there exists an absolute uncovered gap on the line. The path detection probability is the probability that R sensors with $2d_t$ meters of intervals covers the whole line is

$$p = 1 - \sum_{i=1}^{h} (-1)^i \begin{pmatrix} n+1 \\ i \end{pmatrix} \left(1 - \frac{2id_t}{D_1 + 2d_t}\right)^R \tag{2.14}$$

where h is the largest integer such that $2hd_t \leq D_1 + 2d_t$ [71].

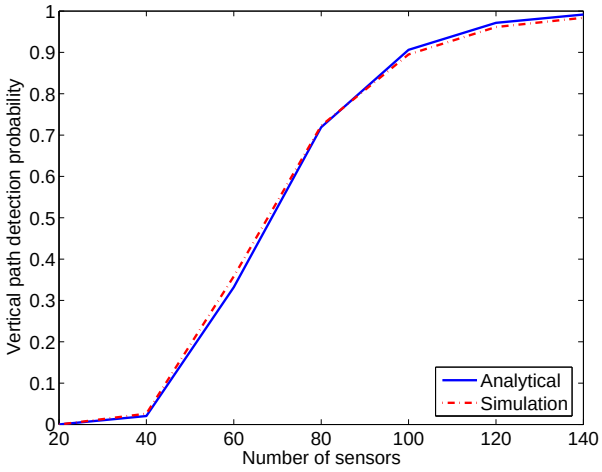


Figure 2.22. Verification of Equation 2.14 with Matlab simulations

In Figure 2.22, the analytical path detection probability is verified with simulations. R sensors are positioned on a line of 500 meters length. The detection range of the binary sensors is 18 meters. Hence, a single sensor's coverage on the line is 36 meters. For each sensor count, the results are the averages of 20000 deployments. If any deployment has a gap larger than 36 meters than the result is labeled as failure, otherwise as success. The simulation results are the ratio of success' to 20000. The results closely match the analytical results.

2.5.2. Evaluation of the Biased Random-Way Point Breach Paths

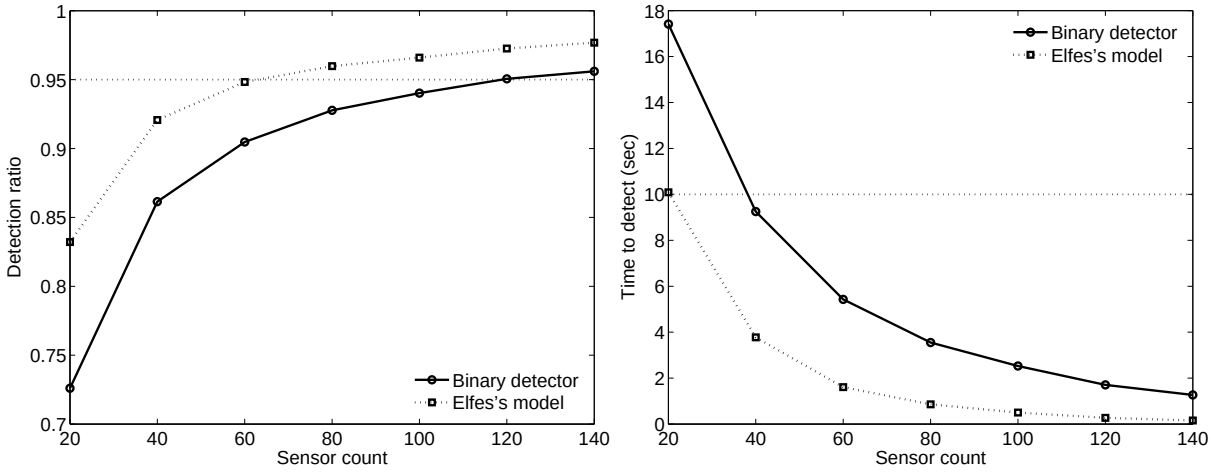
There are several discrete event simulators that can be used to model SWSNs. In this section, we present results produced with OMNeT++, which is a public-source discrete event simulation environment [72]. New modules can easily be developed and incorporated into the architecture. Wireless sensor nodes can be modeled as a component defined by a high level description language, which is in turn compiled to produce the C++ code.

A simulation of a simple border surveillance scenario is developed. The objective of the target is to pass from the insecure side to the secure side. The physical layer sensing operation is modeled in accordance with the binary or Elfes's detector. The

sensor locations are uniformly distributed in a 500×200 m^2-field, and the sensors have sensing range of 18 meters. The target passes the field at a speed of two meters per second starting at a randomly selected point in the field. The step interval of the target is 25 ms. A biased random way-point mobility model for the target is employed. Specifically, defining the residual field as the area between the current position of the target and the secure side, the target chooses randomly a point in the residual field and moves there next. The movement process is repeated until either the target reaches the secure side, or it is detected by a sensor. The results are the averages of 100 different deployments, and for each deployment the target traverses the region for 100 times. The data collection rate of the sensor, the velocity of the target, the number of sensors deployed and the field dimensions are the parameters that are controlled in the simulations.

The effect of the sensor count on the detection ratio and the time-to-detect are shown in Figure 2.23. Because binary detectors are distributed uniformly, more sensors means larger sensing coverage and improved detection performance. In many cases, detecting the intruder quickly enough is just as crucial as detecting it at all. The time-to-detect parameter in this scenario is directly related to the coverage obtained by the deployment of sensors close to the insecure side. As Figure 2.23(b) demonstrates, by increasing the number of sensors, the density of the sensors near the insecure side grows, as well. Hence, the time required for the target to pass through the coverage area of a sensor becomes shorter.

Figure 2.23 shows the impact of the sensor count on the detection ratio and time-to-detect under Elfes's model, which can represent any sensor type. The parameters are set as $r = 36$ meters, $r_e = 20$ meters, $\lambda = 0.2$ and $\beta = 0.6$. For comparison with the binary detector, here probability of detection is 0.5 when target-to-sensor distance is 18 meters, which is the maximum binary detection range. When Elfes's model is employed, the detection performance is better and the time-to-detect the intruder is lower because there is still some small probability of detection even at larger distances compared to the binary detector.



(a) The effect of sensor count on detection ratio

(b) The effect of sensor count on time-to-detect the target

Figure 2.23. The effect of sensor count on the detection ratio and time-to-detect the target when binary or Elfes's detectors are utilized

A surveillance application referred to as *A Line in the Sand* is presented in [73]. The objective there is to detect breaches through a perimeter or in a field. The user requirements are defined with three parameters: a correct detection probability of 0.95 or higher; a false alarm probability that is less than 0.10; and a latency between target presence and its detection that is shorter than 10 seconds. Figure 2.23 suggests that for this scenario, if the field size is 500×200 m^2, then 120 binary detectors are needed to ensure a detection ratio that is slightly greater than 0.95 and an average target detection duration under 1.71 seconds so that the goals of [73] are met. As seen in Figure 2.22, these results comply with the requirement calculated using Equation 2.14 for a vertical path detection probability of 0.95. Figure 2.23 depicts that 60 Elfes detectors are adequate to provide the required levels of the same metrics. The doubling of the required number of nodes when binary detection is adopted stresses the importance of having proper sensor models for WSN deployment.

3. DEPLOYMENT QUALITY MEASURES

Suppose a rough terrain is to be monitored to detect unauthorized intrusions. This task can be risky for humans. Due to the self-organizing nature, deploying a wireless sensor network is an easy alternative to deploying a wired one. Sensors can be dropped by an aircraft, and they can configure themselves to start sensing and communicating [31, 74].

From the functional point of view of a SWSN, sensing coverage and breach prevention are more crucial compared to the communication problems. Measures must be defined to analyze the sensing coverage. The sensing quality depends on the type and variety of the sensors, the number of sensors deployed, the deployment scheme and the characteristics of the target and the environment. The variety of sensor technologies makes the coverage analysis difficult because the underlying signal processing and the detector structure depend on the physics of the sensing device. If the target detection probability is well-defined, a quality of sensing measure can be established.

To prevent intrusions through the surveillance field, the breach paths in the sensing coverage must be determined. This problem is referred to as the weakest breach path problem in the previous chapter [30, 32, 36]. Traditionally, Voronoi segmentation is utilized to reveal breach paths based on exposure definitions [22, 32, 33, 75]. Voronoi tessellation of a discrete set of sensors distributed in the Euclidean space determines the sets of points closest to each of the sensors. Given a set S of discrete number of points (sensors) in the Euclidean space (surveillance field), for any point (x, y) in this space, there is one point from S, say s_i, to which (x, y) is closer than any other point in S except the equally distant ones. Hence, the set of closest points to point s_i in S produces a convex polytope referred to as the Voronoi cell. The set of Voronoi cells produces the Voronoi tessellation that corresponds to S of the Euclidean space [76].

When obstacles are incorporated in the field model, a line-of-sight problem arises. That is, some parts of the field cannot be monitored because the sensors may not be

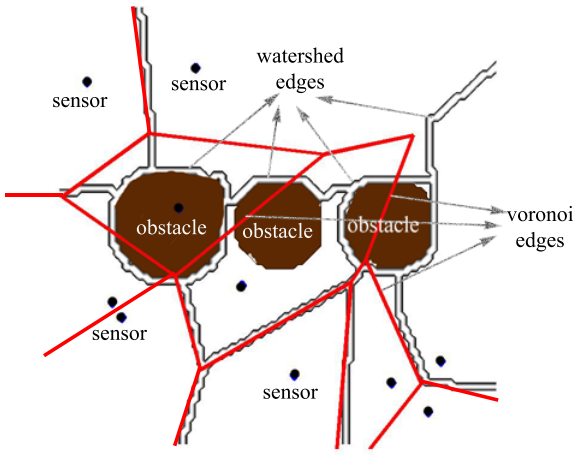


Figure 3.1. Voronoi segmentation fails when obstacles are present in the area of surveillance

able to detect the phenomenon due to the lack of a direct view. Similar obstruction models are analyzed in [29,77]. Voronoi segmentation considers just the positions of the sensors, and therefore falls short of finding the weakest breach path. A simple scenario is depicted in Figure 3.1, where the breach path found through Voronoi segmentation passes over the obstruction, which may be impossible geographically. Therefore, another method which takes into account the sensing capability at each point or subregion in the field must be utilized.

As one of the major contributions of this thesis, we employ watershed segmentation to determine the breach paths in the presence of geographic or man-made obstacles. When the surveillance field is modeled as a grid and we know the positions of all sensors, the detection probabilities (or exposure levels) for each grid point can be calculated. Restricting the field to a two-dimensional space and adding the detection probability as the third dimension, a three-dimensional surface which we refer to as an iso-sensing graph is obtained. In this chapter, we propose a method to determine the quality of deployment in a SWSN in an environment that contains obstacles. The minimum of the maximum detection probabilities of the potential breach paths is used as the deployment quality measure. The watershed segmentation algorithm is applied

on the graph formed by the iso-sensing curves to identify the possible breach paths. An algorithm is proposed to convert the watershed segmentation to an auxiliary graph which is then employed to determine the deployment quality measure.

The iso-sensing graph that we define in this chapter resembles the contours that denote the equal heights in a topographic map. Correspondingly, the contours in the iso-sensing graph represent the equally-sensed areas. A sample iso-sensing graph is shown in Figure 3.2 where the sensors are deployed randomly. To model the real world, obstacles that disable sensing and physical traversals are incorporated. By looking at Figure 3.2, the weakest breach path problem can be defined as finding the path through which an intruder may pass from the insecure side of the the field to the secure side with the lowest probability of detection, while simultaneously avoiding the obstacles.

Most research on coverage assume that sensor locations are known as we assume in this work [22, 33, 37]. If the field of interest is known a priori, and deterministic deployment is possible, the designer may utilize the near optimal sensor placement algorithm proposed by Lin and Chiu in [78] to provide a complete sensing coverage. For random deployment, it is concluded that the optimal sensor placement problem is NP-complete [78].

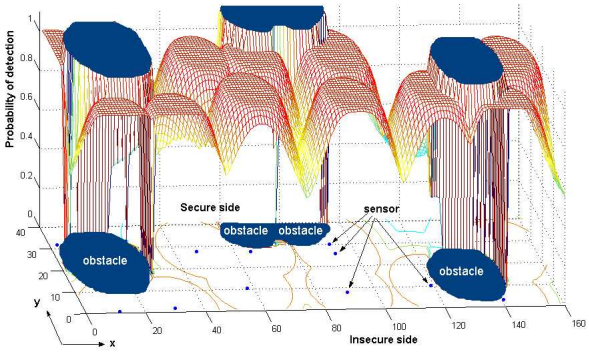


Figure 3.2. A sample iso-sensing surface where the length, the width and the grid size are 160 meters, 40 meters and 1 meter, respectively. The iso-sensing surface is calculated using NPD model where the false alarm rate, SNR, path-loss exponent and the sample size are 0.01, 20 dB, two and 100, respectively

3.1. Iso-sensing Graph Definition

In this section, we define how the iso-sensing graph is produced, and present how the watershed algorithm is used to determine the breach paths. We model the field as an $N \times M$ grid as seen in Figure 3.2. For a grid point (x, y), the *4-connected neighborhood* is defined as the set of grid points $\mathbf{G}_4(x, y) = \{(x+1, y), (x-1, y), (x, y+1), (x, y-1)\}$ and the *8-connected neighborhood* is the set of grid points $\mathbf{G}_8(x, y) = \mathbf{G}_4(x, y) \bigcup \{(x+1, y+1), (x-1, y-1), (x-1, y+1), (x+1, y-1)\}$. We use the 8-connected neighborhood definition in the field model. The two grid points (x_1, y_1) and (x_2, y_2) are assumed to be connected if $(x_2, y_2) \in \mathbf{G}_8(x_1, y_1)$.

Any probabilistic sensor model can be used to produce the iso-sensing graph. In this thesis, instead of the common binary detection with static [22, 79–81] and adjustable sensing ranges [82, 83], we use the NPD and ESDM. The latter models present a particularly suitable formulation for radar sensing, which is pivotal in the surveillance of very large areas.

To model the real outdoor environments obstacles must be considered. The probability of detecting a target on each grid point can be calculated if there is line-of-sight between the target and the sensor (e.g. no obstacles exist in between). To incorporate the obstacles in the model, we define $o_{vi} = 1$ if there is line-of-sight between the target at grid point v and the sensor i, and $o_{vi} = 0$ otherwise. If obstacles are not modeled, then $o_{vi} = 1$. Depending on the type of the sensor, obstacles may not disable sensing functionality completely. For such situations, the designer may assume $0 \leq o_{vi} \leq 1$ as a sensing degradation factor. In this chapter, we consider the Boolean approach as Kansal *et al.* presented in [77] where they analyze the effect of obstacles on the sensing coverage. A similar obstruction approach is presented in [29]. In the following section, we define different approaches to produce the iso-sensing graph.

3.1.1. Iso-Sensing Surface Definition

The iso-sensing definition that is presented in this section is an off-line process. That is, operationally, all nodes are in sensing mode unless any sleep scheduling is implemented. However, in the following iso-sensing graph definitions, the decisions of a subset of sensors are fused to produce the breach decision which is not the case in an active network. For grid point v, define the set of sensors in decreasing order of detection probabilities as $S_v = \{s_1, s_2, \ldots, s_\ell, \ldots, s_R\}$ with $p_{vs_1} \geq p_{vs_2} \geq \ldots p_{vs_\ell} \geq \ldots \geq p_{vs_R}$ where p_{vs_ℓ} is the detection probability of a target at grid point v by sensor s_ℓ, $\ell = 1, \ldots, R$, is the identity of the sensor and R is the total number of sensors deployed in the field. Any probabilistic sensor model can be used to calculate p_{vs_ℓ} such as ESDM or NPD. Throughout the lifetime of the wireless sensor network, the sensor nodes do not communicate to sort out their detection probabilities for any grid point; they just function to sense and communicate the sensed phenomenon.

3.1.1.1. K-Degrees of Iso-Sensing (KIS). In this type of iso-sensing graph definition, $K \leq R$ of the closest sensors (first K sensors in S_v) act on the decision for a grid point. Then, the detection probability of a target on grid point v is

$$p_v^{KIS} = 1 - \prod_{\ell=1}^{K} (1 - p_{vs_\ell} o_{vs_\ell}). \tag{3.1}$$

This type of iso-sensing surface definition can be used where the sensor nodes sleep from time to time. Since redundant number of sensor nodes are deployed, sleep scheduling of sensors for both communication and sensing reduces the total energy consumption, which provides a more efficient network. Designing a sleep scheduling algorithm according to the sensing performance is beyond the scope of this thesis. For example, Lui *et al.* proposes a scheduling algorithm without accurate location information subject to sensing coverage and connectivity requirements [51]. For a given coverage degree, they propose a lower bound on the required number of sensors to provide a coverage intensity level. Coverage intensity is defined as the ratio of active time to the total time where the points in the field is covered with at least one active sensor. Another

scheduling work considering sensing coverage is proposed by Ren *et al.* in [52] and by Hsin and Liu in [53].

Other application level coverage degree measures can be based on accuracy or fault tolerance. For applications such as battlefield surveillance, increasing the degree of sensing coverage improves the overall sensing accuracy. In other words, failure of an individual sensors must not hamper the network operation. Hence, fault tolerance can be ensured with higher coverage degrees. Another motivation is that when the position of the target is to be estimated, measurements from more than one sensor are required. For triangular positioning algorithms, the degree of coverage may be adjusted accordingly.

3.1.1.2. Reliable K-Degrees Iso-Sensing (KRIS). In KIS, large values of K increase the variance of sensor decisions. For a more reliable design, S_v can be bounded with a reliability factor $r_{vs_\ell} = 1$ if $p_{vs_\ell} > p_t$, and $r_{vs_\ell} = 0$ otherwise. The threshold probability $p_t \in (0.5, 1)$ represents the confidence level of the sensor. That is, sensor decisions are deemed sufficiently reliable only at those d_{vs_ℓ} distances where $p_{vs_\ell} > p_t$. Depending on the application and the false alarm requirement, typically $p_t \geq 0.9$. The sensors are incorporated in the calculations if they can sense with $p_{vs_\ell} > p_t$. Hence, this model is referred to as Reliable K Degrees Iso-Sensing (KRIS) and the detection probability becomes

$$p_v^{KRIS} = 1 - \prod_{\ell=1}^{K} (1 - p_{vs_\ell} o_{vs_\ell} r_{vs_\ell}). \tag{3.2}$$

Ideally, $p_t < p_{vs_K}$; otherwise, the degree of the coverage is smaller than K. Moreover, in an active network the sensor does not decide if it is reliable or not; it just decides if there is target or not according to its functional design.

3.1.1.3. Reliable Subset Iso-Sensing (RIS). Since those sensor decisions that are sufficiently reliable are incorporated in KRIS, to reduce the complexity about deciding on the appropriate value of K, the designer may prefer to take K as the number of

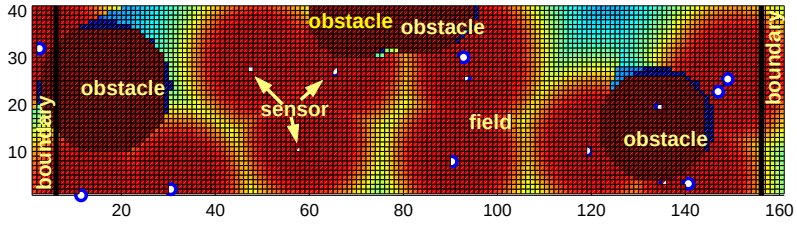


Figure 3.3. Two dimensional visualization of the sample iso-sensing surface shown in Figure 3.2

sensors $K = R$, then,

$$p_v^{RIS} = 1 - \prod_{k=1}^{R} (1 - p_{vk} o_{vk} r_{vk}), \tag{3.3}$$

and this model is referred to as the Reliable Subset Iso-Sensing (RIS) and assumes uncorrelated sensor decisions. However, if a sensor detects a target, it is highly probable that another sensor also detects the same target depending on the position of the sensor and the environmental situation (e.g. obstacles). With RIS, the total effect of the sensor correlations is bounded because low probability values are truncated. Hence, the variance is not affected.

3.1.1.4. Most-Dominant-Sensor Iso-Sensing (MDIS). The individual detections of a subset of sensors may be highly correlated, particularly if the deployment is dense. If a sensor detects a target, it is very probable that another sensor which is at about the same distance will also detect the same target assuming same environmental conditions. A similar approach is considered in [33] where observability by the closest sensor is dominating. The designer may merely assume that the sensor with the largest detection probability dominates the grid point, in which case

$$p_v^{MDIS} = \max_{1 \le k \le R} \{p_{vk} o_{vk}\}. \tag{3.4}$$

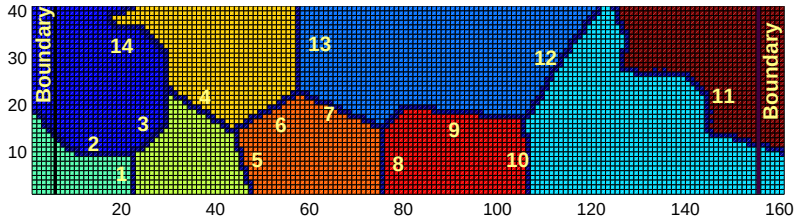


Figure 3.4. The watershed contours of the sample iso-sensing surface shown in Figure 3.3

This model is equivalent to KIS with $K = 1$. By definition, $p_v^{MDIS} = p_v$ defined in Equation 2.4 if no obstacles are modelled. A more strict approach would be to assume that detection probability is zero if the detection probability of the closest sensor is less than the threshold probability.

Obviously, KIS and RIS definitions necessitate redundant sensor deployment. To increase the coverage degree, more sensors must be deployed, which increases the density of the network and decreases the possible target-to-sensor distances. Hence, more sensors provide detection probabilities that are greater than the reliability threshold. Thus, RIS and KIS work in a similar way in terms of detection performance. Consequently, designing a network according to KIS, KRIS or RIS is more costly compared to one designed following the MDIS formulation. However, former provide higher reliability. Sorted in terms of decreasing reliability level, the measures follow the KRIS, RIS, KIS and MDIS order.

Calculating the detection probabilities for each grid point produces the iso-sensing graph. After calculating the iso-sensing graph (see Figure 3.2) and producing the gray-scale 2-D image (see Figure 3.3), the watershed algorithm can be applied to determine the paths through the valleys. In image processing, the watershed algorithm is applied to a gradient image to find edges in the original image, or the highest peaks in the gradient image [70]. Therefore, our iso-sensing graph may be interpreted as an inverted

gradient image. In the following section, we point to an analogy between an iso-sensing graph and a topographical relief and present how the breach paths can be revealed through the watershed algorithm.

3.1.2. Watershed Segmentation

In image processing, the gradient images which correspond to the topographic reliefs are often denoted with gray-scale pictures. The gray tones in the image depict the elevations in the region. Image segmentation is a process to discriminate the objects in an image from the background. A common approach is to find disjoint regions that are homogeneous with respect to some property. Watershed segmentation is a region based approach and the idea behind this algorithm comes from nature. The watershed transform is a region-based segmentation approach.

Watershed segmentation is best-understood with an analogy to water flooding from the minimal plateaus of a three dimensional topographic surface, where the third dimension is the altitude. Minimal plateau is a set of points with an altitude from which it is impossible to reach a lower altitude without having to climb. As the water rises in the catchment basins, dams are built where the floods will merge. The catchment basin associated with a minimal plateau is the set of points such that a water drop that falls on one of these points flows until it reaches the minimal plateau. After the completion of immersion, water reaches the maximum level, and only the dams that separate the valleys emerge. Consequently, the topographic surface is partitioned into regions that are separated by the dams referred to as *watersheds* or the dividing lines that separate the catchment basins. The labeling process of the revealed regions is referred to as the *watershed transform* [84]. This approach is generally referred to as immersion analogy. The watershed segmentation algorithm by simulated immersion is presented by Vincent and Soille in [70].

When simulating the immersion process, there are two approaches: in the first approach, the basins are found, then watersheds are formed by taking a set complement. In the second approach, the image is completely partitioned into basins; then, by

boundary detection, the watersheds are discovered. There are several sequential and parallel algorithms for watershed transformation [84]. They can be divided into two classes: those based on the recursive algorithm by Vincent and Soille [70], and others based on distance functions by Meyer [85]. In this thesis, we use the Vincent-Soille algorithm. There are two main steps of the algorithm: the sorting and flooding steps. After sorting the gradient values of each pixel, the algorithm starts working with the pixels with the lowest gradient values and assigns a unique label to each minimum and its corresponding basin using a breadth-first technique. If a pixel is adjacent to more than one basin it is marked as a watershed edge. The time complexity of the algorithm is linear proportional to the number of pixels.

For a grid, the intensity of grid point p is denoted by $I(p)$ that takes discrete values in $[0, N]$. The path $\wp$ between grid point p and q is described with an l-tuple, $(p, x_1, x_2, \ldots, x_{l-2}, q)$. The length of the path $\wp$ is l. Denote the neighbors of grid point p with $N(p)$. A minimal plateau of I around point p denoted with $M(I)$ is defined with a set of points $\forall q \notin M(I)$ such that $I(q) \geqslant I(p)$ and $\forall \wp = (p, x_1, \ldots, x_{l-2}, q)$ such that $I(x_i) \geqslant I(p)$ where $i = 1, 2, \ldots, l-2$. Then, the catchment basin $C(M)$ associated with the minimal plateau M is the set of points around p with higher intensities that corresponds to the altitude to where a falling water drop flows until it reaches the M. The dividing lines that separate the catchment basins are the watershed contours [70].

The iso-sensing graph can be considered as a 2-D image where the miss probabilities are quantized to gray-scale color values. The watershed algorithm can be applied to the iso-sensing graph to find the possible breach paths. After deploying the sensors to the field and calculating the iso-sensing graph of the sensor network, utilizing the miss probabilities on the grid points produces hills and valleys where the altitude is mapped to the miss probability. The minima of this surface are the sensor node positions. Analogously, it can be considered that the water starts flooding from the sensor nodes. After applying the watershed algorithm, the contour points (dams) correspond to possible breach paths. The watershed segmentation of the sample iso-sensing graph is depicted in Figure 3.4. The right and left sides have been marked as boundary regions that are not included in the analysis since they are not completely covered.

3.2. Deployment Quality Measure

The most secure path for a target follows the grid points that are the most distant from the sensors in the field. From the WSN's point of view, this path is the weakest breach path. Thus, the maximum detection probability on the weakest breach path provides a measure to analyze the quality of the deployment [30]. Watershed segmentation produces several contours, in which the weakest breach path resides. If all sensors are identical and the iso-sensing surface is monotonous, then watershed segmentation is equivalent to the Voronoi segmentation. However, the presence of obstacles produces more complex surfaces and Voronoi segmentation does not work. The obstacles not only block the line-of-sight of sensors, but also the breach paths.

Notice that, the watershed contours are the points in the iso-sensing graph with the least detection probabilities which is in favor of the target. Many combinations of watershed contours exist that connect the insecure side to the secure side. Among these alternative paths, the path with the least maximum detection probability denotes the quality of deployment. To determine the deployment quality measure, an auxiliary graph is constructed using the labeled watershed edges. The objective of the labeling process it to assign a weight which shows the level of breach security. The watershed contours are denoted with nodes in the auxiliary graph and the nodes are assigned weights as the detection probability of the grid point with the maximum detection probability among others on the same watershed contour.

Watershed segmentation algorithm produces a labeled image where all the watershed contours have the same label. To discriminate the individual watershed contours and to label them, algorithms shown in Figure 3.5 and Figure 3.6 can be applied. Suppose that each grid point v is marked with $n_v = 1$ if grid point v belongs to a watershed edge, $n_v = 0$ otherwise. Then, the degree of grid point v can be defined as $d_v = \sum_{\forall w \in G_8(v)} n_w$. The grid points which connect two or more watershed edges are referred to as the connection points and for a connection point v, $n_v = 1$ and $d_v > 2$. With a minor modification of the watershed algorithm, the connection points can be obtained easily. Denoting the state of all of the grid points s_v = `unknown`, for each

```
ConstructAuxiliaryGraph()
 1: ∀v, s_v = unknown /* state of v */
 2: c = 0 /* labels and the nodes of the auxiliary graph */
 3: for all v where n_v = 1 and d_v > 2 do
 4:    Disconnect v from adjacent nodes
 5:    for all ω ∈ G_8(v) do
 6:       if n_ω = 1 then
 7:          if s_ω = unknown then
 8:             c = c + 1 /* generate new edge label */
 9:             t = LabelGridPoint(c, ω)
10:          else
11:             t = 𝔏_ω
12:          end if
13:          E_ct = E_tc = connected
14:       end if
15:    end for
16: end for
```

Figure 3.5. Algorithm to construct auxiliary graph

connection point v if the state of an adjacent node $s_\omega =$ `unknown` and $n_\omega = 1$, mark the adjacent node ω with an unique label and set $s_\omega =$ `known` and record the maximum detection probability for this labeled edge and continue to apply the same algorithm to adjacent grid points of ω until it is another connection point or field borders are crossed.

Each labeled edge (watershed contour) is represented as a node. The nodes are connected in the auxiliary graph if the respective edges originate from the same connection point. A sample auxiliary graph for the iso-sensing surface in Figure 3.2 is shown in Figure 3.8(a). The connection matrix of the auxiliary graph is represented with $\mathbf{E}$, and the vector W denotes the weights of the nodes that is the maximum detection probability of the respective edge in the iso-sensing graph. The labels of each

grid point are denoted with the vector $\mathfrak{L}$. The start node s and the destination node d denote the insecure and secure sides, respectively. If any edge crosses the boundary regions on either side of the field, remove the nodes from the auxiliary graph. If any edge touches the secure side, connect the representing node to the destination node, and if the edge touches the insecure side, connect the representing node to the start node. This algorithm constructs the auxiliary graph. Algorithms shown in Figure 3.5 and Figure 3.6 have linear time complexities proportional to the number of points on the watershed contours.

In Figure 3.8(a), nodes 2 and 11 are disconnected from the graph since their corresponding edges cross the boundary regions. Nodes 1, 5, 8 and 10 are connected to the start node s since they cross through the border of the insecure side and nodes 12, 13 and 14 are connected to the destination node since they cross the border of the secure side. The auxiliary graph shows the possible breach paths which a target may prefer. For example, among others, $(s, 1, 3, 14, d)$, $(s, 1, 3, 4, 14, d)$ or $(s, 8, 7, 6, 13, d)$ are some breach paths. The path with a set of nodes which has the minimum weights is the best from the view point of the target.

On the auxiliary graph, instead of determining the weakest breach path, a simpler approach, described in Figure 3.7 can be employed to determine the bottleneck edge through which the weakest breach path may pass. In this algorithm, the weights of the nodes are sorted, and the node with the largest weight is removed from the graph. If the start and destination nodes are disconnected, the weakest breach path must pass through this edge if there are no other edges with the same weight. If the graph is not disconnected, the same algorithm is applied on the residual graph until a disconnected residual graph is obtained. The weight of the final node that is removed produces the deployment quality measure (DQM). The weakest breach path cannot be determined with this approach because it may follow another edge with the same weight, whose removal does not disconnect the start and destination nodes. Denote the number of nodes in auxiliary graph with ϖ and the number of connections with e, then the algorithm shown in Figure 3.7 has $O(\varpi e \log \varpi)$ complexity.

LabelGridPoint(c, v)

1: $s_v = known$
2: $\mathfrak{L}_v = c$ /* store the label of the grid point */
3: **if** $W_c > p_v$ **then**
4: $W_c = p_v$ /* store the weight of the node */
5: **end if**
6: **if** v touches to insecure side **then**
7: $\mathbf{E}_{cs} = \mathbf{E}_{sc} = connected$; /* connect to s */
8: **end if**
9: **if** v touches to secure side **then**
10: $\mathbf{E}_{cd} = \mathbf{E}_{dc} = connected$; /* connect to d */
11: **end if**
12: **if** $n_\omega = 1$ and $s_\omega = unknown$ where $\omega \in G_8(v)$ **then**
13: LabelGridPoint(c, ω) /* There is only one such grid point. */
14: **end if**

Return c

Figure 3.6. Algorithm to label the grid points

DeploymentQualityMeasure()

1: buildHeap H using W_c
2: **while** not $H.empty()$ **do**
3: $h = H.extractMax()$
4: Remove node $h.c$ from auxiliary graph
5: **if** s and d are disconnected **then**
6: **Return** $h.W_c$ /* Depth first search can be used */
7: **end if**
8: **end while**

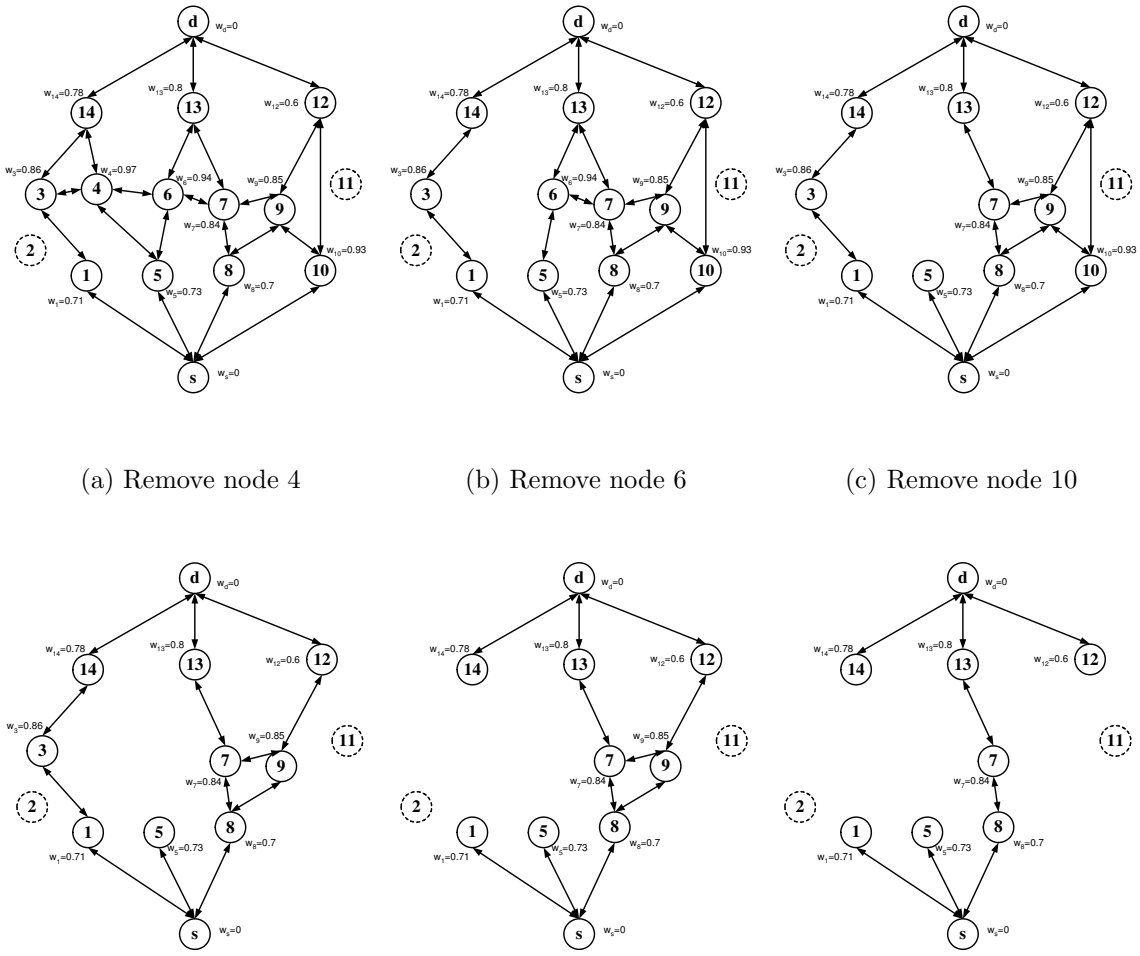
Figure 3.7. Algorithm to determine the deployment quality measure

In Figure 3.8, the trace of the algorithm shown in Figure 3.7 for the sample auxiliary graph shown in Figure 3.8(a) is shown. The DQM algorithm removes the nodes with the largest weight from the auxiliary graph to obtain a residual graph where the start and destination nodes are disconnected. Hence, the algorithm builds a heap using the weights of the nodes, extracts the index of the node with the largest weight and remove the node as well as the incoming and outgoing edges and runs the depth first search algorithm to determine if the residual graph is disconnected. At the first step (Figure 3.8(a)), the node with the largest weight is Node 4 and it is removed and the residual graph shown in Figure 3.8(b) that is not disconnected is obtained. So, the algorithm continues. At the second step, Node 6 is removed because it has the residual largest weight and the connected residual graph in Figure 3.8(c) is obtained. Continuing like this, at the sixth step Node 7 is with the residual largest weight so it is removed and the residual graph is disconnected now. Consequently, the algorithm stops and declares that the DQM is 0.84 because it is the weight of the last removed node.

3.2.1. Simulation Results and Discussion

To analyze the watershed segmentation, we developed a simulator coded in C++ integrated with Matlab. In the simulations, a 300×60 m^2 surveillance field is modeled as a grid, where the grid size is taken to be one meter and the boundary is 10 meters. The NPD sensors are deployed uniformly random. 13 obstacles are modeled as discs where the centers are uniformly distributed and the radii are uniform random variables between 10 and 20 meters. The obstacles not only block the line-of-sight of the sensors, but also the traversal of the intruder. The sensors are modeled as Neyman-Pearson detectors [63], where the signal-to-noise ratio is $\gamma = 20$ dB and the signal attenuates with path-loss exponent $\eta = 2$ because of the line-of-sight requirement. The sensor decisions are based on $L = 100$ samples where the reliability threshold probability is chosen as 0.9. For KIS and KRIS, the required degrees of coverage K is three.

The effect of false alarm rate and sensor count for the Most-Dominating Sensor Iso-Sensing (MDIS), K-Degrees of Iso-Sensing (KIS), Reliable Iso-Sensing (RIS) and



(a) Remove node 4 (b) Remove node 6 (c) Remove node 10

(d) Remove node 3 (e) Remove node 9 (f) Remove node 7

Figure 3.8. Trace of Algorithm in Figure 3.7. This is the auxiliary graph of the watershed contours in Figure 3.4 produced using Algorithm in Figure 3.5

Reliable K-Degrees Iso-Sensing (KRIS) definitions are depicted in Figures 3.9, 3.10, 3.11 and 3.12, respectively. The results are the averages of 100 runs and the variance in the results is acceptably low. The figures indicate that as the false alarm rate and the sensor count increase, the deployment quality measure increases. Increasing the signal-to-noise ratio improves the detection probability of the sensor, and hence the DQM. The chosen α values of 0.01, 0.05 and 0.1 can be considered as low, moderate and high false alarm rate scenarios, respectively. The sensor count parameter is arranged accordingly to depict sparse, moderate and dense deployment.

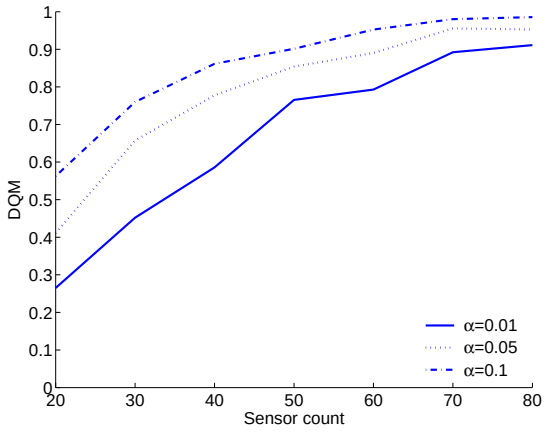


Figure 3.9. The effect of sensor count and false alarm rate on the deployment quality measure for MDIS when NP detectors are deployed

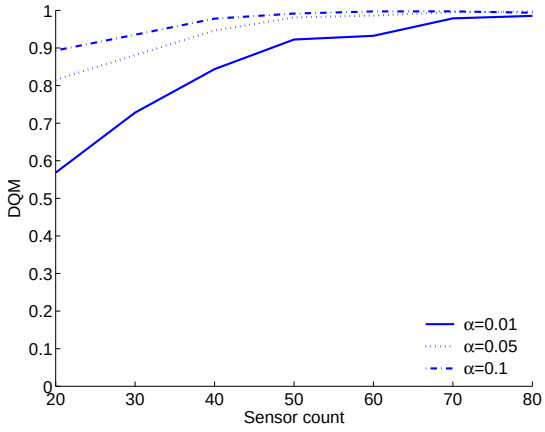


Figure 3.10. The effect of sensor count and false alarm rate on the deployment quality measure for KIS when NP detectors are deployed

For large false alarm rate scenarios, it is clear that sparse deployment satisfies the required DQM. When the false alarm rate is lowered, the number of deployed sensors is to be increased. The sensor count is more influential when the false alarm rate is allowed to be low. For sparse deployments, KIS produces a larger DQM value compared to MDIS (KIS where $K = 1$) because the detection probabilities of K sensors are combined to obtain a better decision. However, for dense deployments, increasing the value of K does not make a significant difference in the results. When KIS is bounded with a reliability threshold probability p_t, sparse deployment produces apparent breach paths.

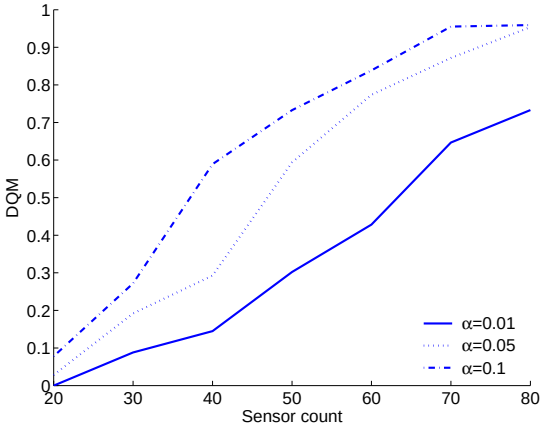


Figure 3.11. The effect of sensor count and false alarm rate on the deployment quality measure for RIS when NP detectors are deployed

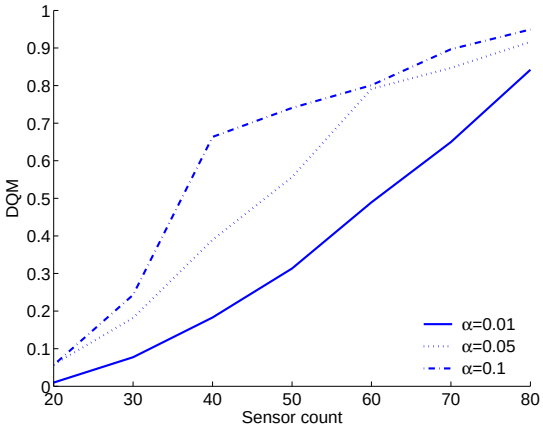


Figure 3.12. The effect of sensor count and false alarm rate on the deployment quality measure for KRIS when NP detectors are deployed

That is, for some paths in the surveillance field, no sensors detect the phenomenon with a probability larger than p_t. For example, when KIS with $K = 3$ is used, for a false alarm rate of 0.05, 30 sensors are sufficient to produce a DQM of 0.9. However, for the same false alarm rate scenario, more than 70 sensors are required for RIS when $p_t = 0.9$.

The effect of the reliability threshold is seen in Figure 3.11, when fewer than 80 sensors are deployed for $\alpha = 0.05$, some parts of the field is not monitored reliably.

Hence, when fewer than 20 sensors are deployed some parts of the field is assumed to be monitored with zero probability since the detection probabilities associated with those points are lower than the reliability threshold. Consequently, as seen in Figure 3.11, the DQM is zero for $\alpha = 0.05$ where fewer than 20 sensors are deployed.

When RIS is bounded with the coverage degree parameter K, the results do not change significantly. Because, to increase the detection probability at each grid point, dense deployment is required. Considering the spatial distribution of the sensors, to attain at least the threshold probability level, the required number of sensors provide a coverage degree larger than three. In other words, deploying more sensors to increase the detection probability at each grid point automatically increases the coverage degree and vice versa. Furthermore, for RIS and KRIS when the required DQM value is achieved, it means that the deployment is saturated, and additionally deployed sensors do not improve performance. Thus, for RIS and KRIS, it is more appropriate to consider saturated and unsaturated deployment scenarios instead of sparse, moderate and dense deployments.

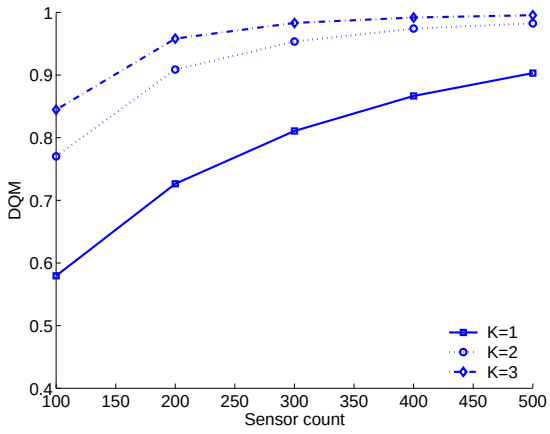


Figure 3.13. The effect of sensor count and sensing coverage degree on the DQM for KIS when Elfes's detectors are utilized

For some applications such as battlefield surveillance, higher accuracy may be required. For those applications KIS with $K > 1$ can be employed. The effect of coverage degree on the deployment quality measure is analyzed in Figure 3.13 where ESDM (see Equation 2.3) are utilized. The sensing range and the decay of the detectors

are arranged according to parameters $r_e = 18$ meters, $r = 20$ meters, $\lambda = 0.1$ and $\beta = 0.9$. To provide the same DQM level for larger coverage degree requirement, denser deployment is necessary. For example, to provide a DQM of 0.9 for KIS with $K = 1$, $K = 2$ and $K = 3$, required number of sensors are 150, 200 and 500, respectively.

The iso-sensing graph definition is extended to model obstacles, which block the line-of-sight of sensors and the traversal of intruders so that the detection probability of the grid points on which the obstacles are located can be set to one. Hence, the watershed segmentation algorithm takes the obstacles into account, and the contours do not overlap with the obstacles. From the target's standpoint, following the watershed contours is beneficial. However, the period of time the target spends in the field influences the detectability, as well. A discrete event simulation (DES) is coded in C++ using Matlab to verify this argument next. After applying the watershed segmentation algorithm, the potential breach paths are revealed. A target with a constant velocity traverses the region through the watershed contours starting at a random grid point on the contour where it touches the bottom line along the x-axis. The aim is to pass the field to reach the other side along the x-axis (see Figure 2).

The 600×100 m^2 field is modelled as a grid, where the grid size is one meter. The iso-sensing graph is calculated according to MDIS after deploying varying number of NP-detectors in this field uniformly randomly. The signal-to-noise ratio is $\gamma = 30$ dB, the signal attenuates with path-loss exponent $\eta = 2.5$, the false-alarm rate $\alpha = 0.01$ and the sensor decisions are based on $L = 100$ samples. The simulation is repeated 2000 times per deployment and the results are the averages of 100 distinct deployments. Three circular obstacles are placed where the radii are uniformly randomly chosen between eight and 15 meters.

The detection ratio of targets with several constant velocities (denoted in grids per second, g/s) for varying sensor counts is depicted in Figure 3.14. If the target remains in the field for a longer time period, then its detection probability will be larger. For example, when nine sensors are deployed, for a target with a velocity of five g/s the detection ratio is around 0.68, whereas for a velocity of one g/s, the same

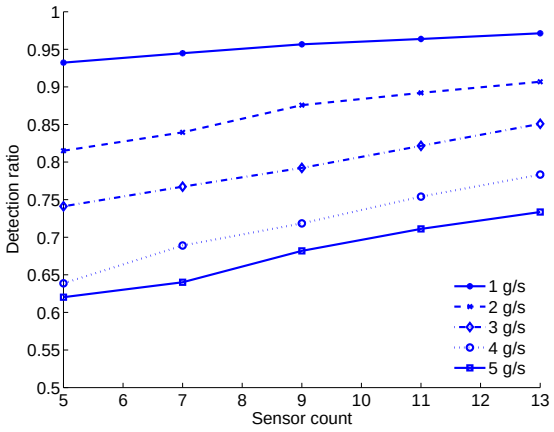


Figure 3.14. The effect of the sensor count on the detection ratio of a when Neyman-Pearson detectors are deployed target following the watershed contours for several target speeds (g/s denotes the velocity of the target in terms of grid per second)

ratio rises to approximately 0.95. Consequently, the target should not only just pass far from the sensors, but also spend little time in the field.

3.3. Area Based Quality Measures

The deployment quality measure defined in the previous section describes the worst-case scenario assuming that the target will choose the most-distant path to all sensors. Instead of the worst case scenario, if it is assumed that the target has no information about sensor positions, measures that depicts the overall performance of the sensing coverage can be defined. In this section, we study some alternative deployment quality measures for surveillance wireless sensor networks.

3.3.1. Poorly Detected Area Measure

The ratio of the poorly detected area to the total area of the field, denoted by Q_{PD}, gives insight as to whether the deployed number of sensors are adequate or not. A point in the area is said to be poorly sensed or weakly covered if the number of sensors to monitor that point is less than a predefined value, or if the calculated

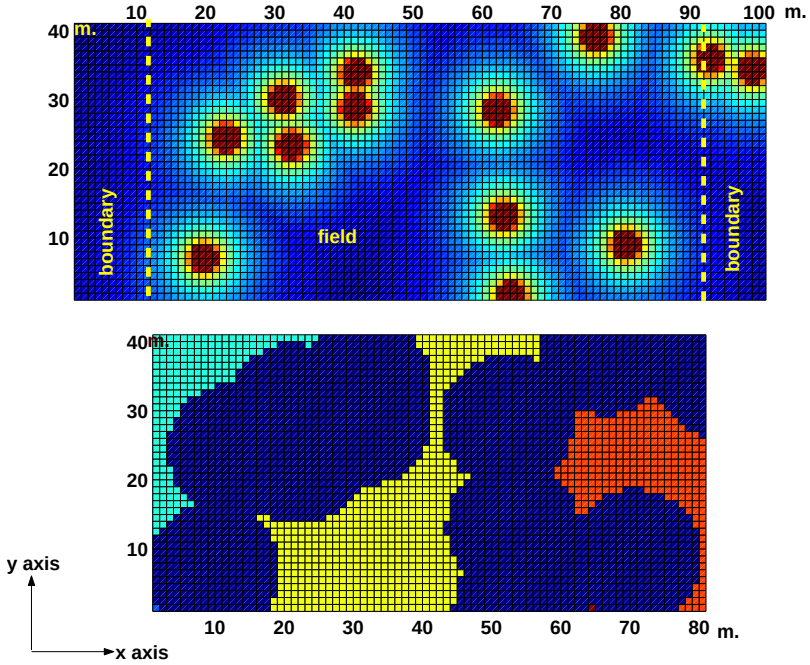


Figure 3.15. A sample iso-sensing surface and connected components where the length, the width, the boundary length and the grid size are 80 meters, 40 meters, 10 meters and one meter, respectively. The iso-sensing surface is calculated using thirteen NP detectors where the false alarm rate, SNR, path-loss exponent and the sample size are 0.01, 20 dB, two and 100, respectively

detection probability for that point is less than some threshold. Suppose that the SWSN detection performance on point v is sufficiently reliable only at those distances for which $p_v > p_t$, where p_t is the minimum acceptable detection probability. Depending on the application, it is usually expected that $p_t \geq 0.9$. Let the grid points v of the field that resembles a pixel in an image, be represented by the indicator $\mathfrak{B}_v$,

$$\mathfrak{B}_v = \begin{cases} 1 & \text{if } p_v < p_t, \\ 0 & \text{otherwise,} \end{cases} \tag{3.5}$$

which represents inadequately monitored grid points with unity value. With this approach, the iso-sensing graph is converted to a black and white, binary image. The black regions of the image denote the poorly sensed area and the white regions denote

reliably sensed area. Then, the deployment quality measure Q_{PD} is defined as,

$$Q_{PD} = \frac{\sum_v \mathfrak{B}_v}{NM}, \tag{3.6}$$

where the numerator counts the poorly detected grids and NM is the total number of grid points in the field. That is, Q_{PD} is the ratio of the sum of black pixels to the total number of pixels. For applications where security is critical, the Q_{PD} value is required to be close to zero. Large values of this measure depicts that the coverage of the network is low. The threshold value for the detection probability is to be fine-tuned depending on the security requirements.

3.3.2. Redeployment Measure

Depending on the non-uniformity of the region, random deployment schemes may yield large poorly sensed areas, in which case redeployment may be necessary. The ratio of the largest connected, poorly sensed area to the area of the field hints whether redeployment is required or not. After representing the field according to Equation 3.5, we obtain a binary image on which image processing techniques such as connected component labeling can be applied.

We use the 8-connected neighborhood definition in the field model. The two grid points v and ω are assumed to be connected if $\omega \in \mathbf{G}_8(v)$. Furthermore, v and u are assumed to be connected if there is a path of grid points from v to u where each grid point is connected to the next one. A connected component is the set of grid points which are all connected to each other. The algorithms to find the connected components are referred to as connected component labeling. Connected component labeling works by scanning an image, pixel by pixel in order to identify connected pixel regions. A sample iso-sensing graph and connected components are shown in Figure 3.15. Further information about the connected component labeling can be found in [86].

After applying the connected component labeling to the binary image $\mathfrak{B}_v$ defined in Equation 3.6, suppose that we have the grid labels $\ell_v \in \mathbb{Z}$, where $\ell_v = 0$ denotes the

background of the image and $\ell_v > 0$ are the label values. Denote the component that has the maximum number of connected pixels (grid points) with the label L. Then, the redeployment measure Q_{RD} can be defined as

$$Q_{RD} = \frac{\sum_{v:\ell_v=L} \mathfrak{B}_v}{NM}. \tag{3.7}$$

This measure depicts the possible sub-fields where redeployment can be considered. For large Q_{RD} values, if Q_{RD} is close to the Q_{PD} value, then it can be concluded that there is a single big gap in the coverage, where redeployment of sensors is a must.

3.3.3. Connected Sides

Even if the field is poorly detected, the sensors can be deployed such that there exists a barrier in the field. Considering our field model, suppose that the largest poorly detected area is small; however, there exists a path from the start node to the destination node through this poorly detected area, which means that there is no barrier. To evaluate this kind of situation, let z be the indicator function showing if there is a path from the start node to the destination node through the poorly detected areas. In order to determine if there is such a path, the previously defined connected component labels, ℓ_v can be used. If any two of the components that have the same label are connected to the start and destination nodes, respectively, then $z = 1$, and otherwise, $z = 0$. The tables reflect the percentage of the experiments that result in $z = 1$, which is denoted by Q_{CS}.

3.3.4. Breach Detection Probability

The weakest breach path defined in the previous chapter can be defined as the permutation of a subset of grid points which targets traverse from the start node s to the destination node d with the least probability of being detected. The consecutive nodes are connected to each other. The deployment quality measure called the breach detection probability on the weakest breach path, P_{BD}, is defined as $P_{BD} = \max_{\forall v \in V} p_v$ in Equation 2.10 where V is the set of grid points the target traverses. The P_{BD}

Table 3.1. Parameter values used in the simulations to analyze the alternative deployment quality measures

Parameter	**Value**
Length	400 m.
Width	50 m.
Boundary	20 m.
Grid size	1 m.
N	441
M	51
α	0.05
η	3
γ	30 dB
L	100
R	300
p_t	0.9

measure depicts the detection probability of just one sensor on the path. In other words, it shows the closest sensor to the weakest breach path since the breach path follows the most distant grid points to all of the sensors, assuming identical sensor characteristics. Therefore, it gives insight about the spread of the sensors in the field.

The effects of the sensor model parameters, the number of sensors, and the density of the deployment on the quality measures are analyzed in the next section.

3.4. Analysis of Area Based Deployment Quality Measures

In this section, the SWSN scenario described by the parameter values listed in Table 3.1 is investigated. NPD is utilized as the sensor model. The simulation results shown in the following tables are the averages of 100 distinct deployment runs. These

Table 3.2. The effect of α on the deployment quality measures

α	Q_{RD} (%)	Q_{PD} (%)	Q_{CS} (%)	P_{BD}
0.01	4.38	22.51	72	0.82
0.02	3.32	19.23	47	0.89
0.03	3.03	17.34	35	0.92
0.04	2.91	15.91	34	0.91
0.05	2.48	14.49	29	0.94
0.06	2.43	13.48	23	0.93
0.07	2.21	12.27	16	0.95
0.08	2.16	11.70	15	0.96
0.09	2.02	10.89	15	0.96
0.10	2.04	10.38	15	0.96

models can be considered as the building blocks that may be used to cover larger fields.

3.4.1. Propagation, Signal and False Alarm Parameters

As the false alarm rate α increases, not only the detection performance of the sensor improves (see Table 3.2), but also smaller components are produced since the detection probabilities are above the p_t level. Consequently, the Q_{RD} and Q_{PD} values become smaller. Furthermore, as the components get smaller, the likelihood of the existence of a component touching both the secure and insecure sides becomes less, and Q_{CS} decreases. The greater allowance for false alarms translates to more aggressive pursuit of targets by the Neyman-Pearson detector. Hence, the miss probability of a target passing through the weakest breach path decreases while P_{BD} increases.

An increase in the propagation exponent η corresponds to faster decay in signal power with distance. Indeed, a small change in η triggers large deviations in the deployment quality measures as depicted by Table 3.3. The number of grid points

Table 3.3. The effect of η on the deployment quality measures

η	Q_{RD} (%)	Q_{PD} (%)	Q_{CS} (%)	P_{BD}
2.00	0.00	0.00	0	1.00
2.50	0.74	2.16	2	1.00
3.00	2.40	14.21	28	0.93
3.50	8.81	32.09	97	0.69
4.00	29.82	46.76	100	0.42
4.50	53.31	57.47	100	0.23
5.00	64.59	65.06	100	0.15

having $p_v < p_t$ increases; thus, the largest component, as well as the total component areas increase yielding a larger percentage. Consequently, for fields where the signal attenuates rapidly, more sensors have to be deployed to meet performance requirements. For example, for $\eta > 4$, it is highly probable that a component exists through which the target may pass from the insecure side to the secure one. The sharp decrease in P_{BD} implies that line-of-sight contact with the target must be ensured by the WSN at all times.

High signal-to-noise ratio (SNR) γ produces better P_{BD} and smaller component

Table 3.4. The effect of γ on the deployment quality measures

γ	Q_{RD} (%)	Q_{PD} (%)	Q_{CS} (%)	P_{BD}
10	14.50	38.26	100	0.63
20	4.34	22.24	65	0.87
30	2.40	14.40	26	0.93
40	1.86	9.96	13	0.97
50	1.44	7.15	5	0.99

Table 3.5. The effect of reliability threshold p_t on the deployment quality measures

p_t	Q_{RD} (%)	Q_{PD} (%)	Q_{CS} (%)
0.75	1.40	7.65	2.00
0.80	1.73	9.50	6.00
0.85	2.22	11.84	13.00
0.90	2.74	14.49	25.00
0.95	3.30	18.93	50.00

areas. However, γ does not impact the deployment quality measures as much as η does (see Table 3.4).

3.4.2. Reliability Threshold and Deployment Density

In Table 3.5, the effect of the threshold probability p_t is displayed. As p_t increases, the area of the components increase as expected. Moreover, for large p_t, the largest component size grows. In other words, the components start to merge to occupy a larger portion, and Q_{CS} increases, as well. When higher reliability is required, more sensors are to be deployed to provide the same deployment quality level.

Table 3.6. The effect of the sensor deployment density on the deployment quality measures

Density (sensors/m^2)	Q_{RD} (%)	Q_{PD} (%)	Q_{CS} (%)	P_{BD}
0.068	0.09	0.12	1	1.00
0.034	0.58	1.83	4	0.99
0.023	1.21	5.42	7	0.98
0.017	1.72	9.60	14	0.96
0.013	2.40	14.40	26	0.93

Table 3.7. The effect of the number of sensors on the mean of the deployment quality measures

R	Q_{RD} (%)	Q_{PD} (%)	Q_{CS} (%)	P_{BD}
200	7.17	26.99	97	0.76
210	6.37	25.54	90	0.77
220	5.65	24.05	86	0.79
230	5.14	22.47	86	0.81
240	4.40	21.12	68	0.84
250	3.92	19.89	58	0.86
260	3.42	18.44	50	0.88
270	3.45	17.55	49	0.91
280	2.96	16.30	42	0.91
290	2.86	15.47	34	0.93
300	2.55	14.36	26	0.92

Keeping the number of sensors and the length of the field constant, if the width of the field is enlarged, the density of the deployment decreases and the number of grid points having $p_v < p_t$ increases (see Table 3.6). Thus, the number of the components increase while their areas grow, and the Q_{RD}, Q_{PD} and Q_{CS} values increase. The P_{BD} values decrease since the target-to-sensor distances become larger. The detection probabilities associated with the grid points depend on the closest sensor. Deploying more sensors results in higher p_v probabilities. Thus, the quality of deployment improves as seen in Table 3.7. Because the sensors are randomly deployed in the field, each grid point has a greater chance to be close to any one of the sensors. Consequently, the detection probabilities increase and the deployment quality measures other than P_{BD} take smaller values. Obstacles are not modelled in the simulations, and the deployed sensors are identical. Therefore, the increase in the number of sensors produces a smoother change in the deployment quality measures.

Table 3.8. Verification of the breach probability through discrete event simulations

R	P	r_m
20	0.45	0.45
40	0.25	0.25
60	0.22	0.23
80	0.02	0.02

When more sensors are deployed, since p_v increases, fewer grid points have $p_v < p_t$, and the Q_{RD} and Q_{PD} values decrease. For 260 sensors, the probability that there exists a component touching both the secure and insecure sides is about 0.5. However, for 200 sensors the same probability is close to one.

3.4.3. Discrete Event Simulation

In order to validate the breach probability of a target passing through the weakest breach path, a discrete event simulation environment is created. In the simulations, the trajectory of the target is the weakest breach path found through the application of Dijkstra's algorithm. The target moves from one grid point to the other by following the sequence of the grid points on the weakest breach path. Velocity of the target is not included in the traversal process. For each grid point, the detection process is simulated. If the target is not detected at any grid point, the result is assumed to be zero, and it is one otherwise. The simulations for each instance are repeated 10000 times and the ratio of the number of detections to ten thousand represent the miss rate, r_m.

The parameter values in the simulations are as in Table 3.1. For different number of sensors, the breach probability P associated with the weakest breach path defined in Equation 2.5 is compared with the simulation results in Table 3.8. The discrete event simulations are in agreement with earlier results.

4. ANALYTICAL DEPLOYMENT QUALITY MEASURE

Assume that a set of sensors are deployed randomly to a region to detect unauthorized traversals. What is the quality of the deployment? Is the deployed number of sensors adequate to provide the required quality in terms of breach detection? In this and previous chapters, we proposed experimental methods based on different deployment quality measures. In this section, we propose an analytical method to determine the required number of sensors based on only the sensing coverage. The probability of detecting a randomly positioned target by a set of binary sensors is formulated. Using this formulation, it is possible to determine the required number of sensors to provide a required detection probability. Also, the expected number of sensors that cover any randomly chosen point in the field can be determined.

We define three problems which are related to each other. All of the problems are based on the following assumptions: The field is rectangular and $D_1 \times D_2$ m^2. The positions of the sensors are uniformly random. The x and y coordinates are independent. R identical sensors are deployed. Binary detectors with sensing range d_t are utilized. The communication range d_c of the sensors are at least twice the sensing range, $d_c \geqslant 2d_t$ [87].

The sensing-neighboring degree, w is defined as the number of sensors within sensing range d_t of each other. Given d_{ij}, the distance between sensors i and j, then define adjacency as $a_{ij} = 1$, if $d_{ij} \leqslant d_t$ and $a_{ij} = 0$, otherwise. Then, the sensing-neighboring degree of i^{th} sensor is $w_i = \sum_{i \neq j} a_{ij}$. The communication-neighboring degree, v is defined as the number of sensors within communication range d_c of each other. Define adjacency $a_{ij} = 1$ if $d_{ij} \leqslant d_c$ and $a_{ij} = 0$, otherwise and the communication-neighboring degree of i^{th} sensor is $v_i = \sum_{i \neq j} a_{ij}$. Now, the problems can be stated as: (1) What is the probability of detecting a randomly located target by at least one sensor given that R sensors are deployed? The solution to this problem can be considered as a deployment quality measure (DQM). (2) What is required number of sensors to provide the required deployment quality measure p_t? (3) What are the average sensing-

and communication-neighboring degrees given that the communication range is at least twice the sensing range $d_c \geqslant 2d_t$.

4.1. Random Point Detection

Assume that the positions of a set of sensors be uniform randomly distributed in a rectangular field where the length and the width are D_1 and D_2, respectively, where $D_2 \leqslant D_1$. The distance between two random points d in a rectangular field is defined as the random variable $\mathbf{D}$. Then the probability density function and the cumulative distribution functions are defined in Equations 4.1 and 4.2 [88], respectively.

$$f_D(\xi D_2) = \frac{1}{D_2} \begin{cases} 2\zeta^2\xi^3 + 2\zeta\xi\pi - 4\zeta\xi^2(1+\zeta), & 0 \leqslant \xi < 1, \\ 4\zeta\xi\sqrt{\xi^2-1} - 2\zeta\xi(2\xi+\zeta) & \\ \qquad +4\zeta\xi\sin^{-1}(1/\xi), & 1 \leqslant \xi < \zeta^{-1}, \\ 4\zeta\xi\sqrt{\xi^2-1} + 4\zeta^2\xi\sqrt{\xi^2-\zeta^{-2}} & \\ -2\xi(\zeta^2\xi^2+1+\zeta^2) + 4\zeta\xi\sin^{-1}(1/\xi) & \\ \qquad -4\zeta\xi\cos^{-1}(1/(\zeta\xi)), & \zeta^{-1} \leqslant \xi < \sqrt{1+\zeta^{-2}}, \\ 0, & \text{otherwise.} \end{cases} \tag{4.1}$$

$$F_D(\xi D_2) = \begin{cases} 0, & \xi < 0 \\ \zeta\xi^2(\frac{1}{2}\zeta\xi^2 - \frac{4}{3}\xi(1+\zeta) + \pi, & 0 \leqslant \xi < 1, \\ \frac{2}{3}\zeta\sqrt{\xi^2-1}(2\xi^2+1) & \\ -\frac{1}{6}\zeta(8\xi^3+6\zeta\xi^2-\zeta) & \\ +2\zeta\xi^2\sin^{-1}(1/\xi), & 1 \leqslant \xi < \zeta^{-1} \\ \frac{2}{3}\zeta\sqrt{\xi^2-1}(2\xi^2+1) & \\ -\frac{1}{2}\zeta^2(\xi^4+2\xi^2-\frac{1}{3}) & \\ +\frac{2}{3}\sqrt{\xi^2-\zeta^{-2}}(2\zeta^2\xi^3+1) & \\ +\frac{1}{6}\zeta^{-2} - \xi^2 & \\ +2\zeta\xi^2\sin^{-1}1/\xi & \\ -2\zeta\xi^2\cos^{-1}1/\zeta\xi & \zeta^{-1} \leqslant \xi < \sqrt{1+\zeta^{-2}} \\ 1, & \sqrt{1+\zeta^{-2}} \leqslant \xi \end{cases} \tag{4.2}$$

where $\zeta = D_2/D_1 \leqslant 1$ is the shape parameter and $\xi = d/D_2$. Binary detector can be formulated as

$$g_D(x) = \begin{cases} 1, & x \leqslant d_t \\ 0, & x > d_t \end{cases} \tag{4.3}$$

where $x \geqslant 0$ is the sensor-to-target distance, d_t is the sensing range and $g(x)$ is the detection probability function defined with the random variable $x \in \mathbf{D}$. Assume that a target and a binary detector are positioned randomly in a rectangle region, then the expected value of target detection probability is

$$E\{g_D(\mathbf{x})\} = \int_0^{\infty} g_D(\mathbf{x}) f_D(x) dx = \int_0^{d_t} f_D(x) dx \tag{4.4}$$

By definition, this is the value of cumulative distribution function for d_t defined in Equation 4.2. That is, $E\{g_D(\mathbf{x})\} = F_D(d_t)$. We can define a Bernoulli trial as: Chose two random positions in the rectangle, assume that the target is located on one of the points and there is a sensor on the other point. If the distance between these two random points is smaller than d_t, the target is detected successfully and the trial fails otherwise. The expected value of this Bernoulli trial is defined in Equation 4.4. By definition, the expected value of a Bernoulli trial is equal to the success probability. Hence, the detection probability is $p = F_D(d_t)$. Repeating Bernoulli trials R times produces binomial distribution. If R sensors are deployed, then the probability that a randomly positioned target is detected by k of the sensors follows this binomial distribution. Hence,

$$p(R,k) = \binom{R}{k} p^k (1-p)^{R-k} = \binom{R}{k} F_D(d_t)^k (1 - F_D(d_t))^{R-k}. \tag{4.5}$$

Equation 4.5 cannot be approximated by a Poisson distribution because

$$\lim_{R \to \infty} R F_D(d_t) \to \infty.$$

However, since $RF_D(d_t)$ is large enough, Equation 4.5 can be approximated by normal distribution $\mathbb{R}(\mu, \sigma)$ where $\mu = RF_D(d_t)$ and $\sigma = RF_D(d_t)(1 - F_D(d_t)$. The probability that the target is detected by at least one sensor is

$$p_d = 1 - p(R, 0) = 1 - (1 - F_D(d_t))^R. \tag{4.6}$$

where p_d is the solution of question "What is the probability of detecting a randomly located target by at least one sensor given that R sensors are deployed?". Equation 4.6 can be expressed as the complement of the probability that none of the sensors detect the target. Using Equation 4.6, one can derive R for a predetermined target detection probability value p_t, then the required number of sensors for a given DQM level p_t is

$$R = \left\lceil \frac{\log(1 - p_t)}{\log(1 - F_D(d_t))} \right\rceil. \tag{4.7}$$

Concentrating on any randomly deployed sensor, we can define a Bernoulli trial as whether any other randomly deployed sensor is in the sensing range. If R sensors are deployed, then the sensing-neighboring degree of a sensor is the expected value of the binomial distribution obtained by $R - 1$ Bernoulli trials. Consequently, the sensing-neighboring degree is

$$w = E\{p(R - 1, k)\} = (R - 1)F_D(d_t) \tag{4.8}$$

Since the communication range d_c is at least $2d_t$, then we can define the trial according to the communication range, hence the communication-neighboring degree is

$$v \geqslant (R - 1)F_D(2d_t). \tag{4.9}$$

Since $F_D(2d_t) > F_D(d_t)$, if the network is designed according to the communication range, breach holes will exist in the sensing coverage. In the next section, we present numerical evaluation of the proposed analytical deployment quality measure.

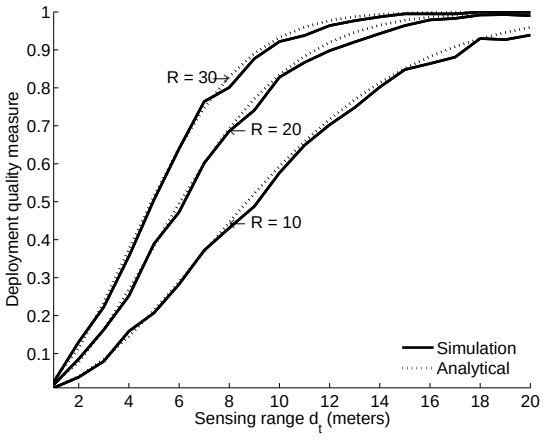


Figure 4.1. The effect of sensing range on the deployment quality measure is verified with simulations where $D_2 = 30$ meters, $D_1 = 100$ meters and $N = 10,\ 20,\ 30$

4.2. Numerical Evaluation of Random Point Detection

The simulations are performed with Matlab. A set of sensor positions are determined randomly in a rectangle. For each run, a target is assumed to be located on a random position. If the distance between the target and any sensor is smaller than the sensing range, then the run is assumed to be a success, otherwise it is a failure. The results are averages of 1000 runs for each deployed sensor set. The effect of the number of sensors and the detector range on the DQM are shown in Figure 4.1 and Figure 4.2, respectively. The variances in the simulations are in the acceptable range and verify the correctness of the analytical model.

Cumulative distribution functions are monotonic increasing functions. As the sensing range increase, $F_D(d_t)$ increases and the probability of target detection p_d decreases (see Equation 4.6). This is depicted in Figure 4.1; for $R = 10,\ 20,\ 30$, the deployment quality measure is plotted as the sensing range increases. As the number of deployed sensors increase, the provided DQM level increases (Figure 4.2). For denser deployments, the required DQM is provided with sensors whose ranges are smaller. When the sensing range is equal to the width of the field, the DQM is one and only a couple of randomly deployed sensors are enough to cover the field as seen in Figure 4.3.

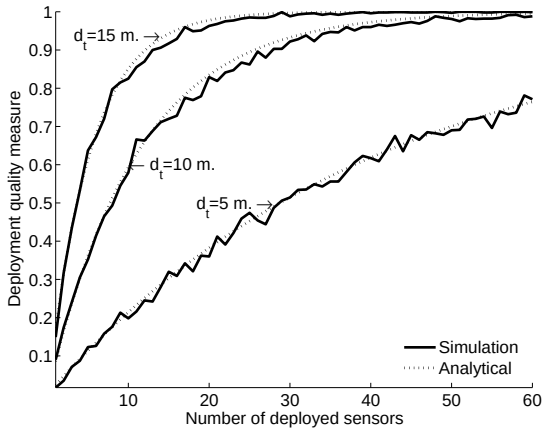


Figure 4.2. The effect of the number of sensors on the deployment quality measure is verified with simulations where $D_2 = 30$ meters, $D_1 = 100$ meters and $d_t = 5,\ 10,\ 15$ meters

Keeping the field area constant as 3000 m^2, the shape of the field is influential on the required number of sensors as seen in Figure 4.4, where the sensing range is 10 m. As the field becomes square in shape, fewer sensors are enough to provide the required DQM. When the shape parameter is small, more sensors are required. As the required deployment quality increases, more sensors are required. For example, when $\zeta = D_2/D_1 = 0.0083$, 58 sensors are required to provide a deployment quality of 0.85

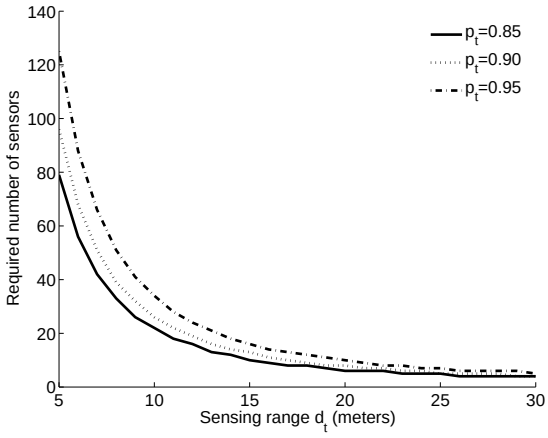


Figure 4.3. The effect of sensing range on the required number of sensors for different threshold detection probabilities where $D_2 = 30$ meters, $D_1 = 100$ meters

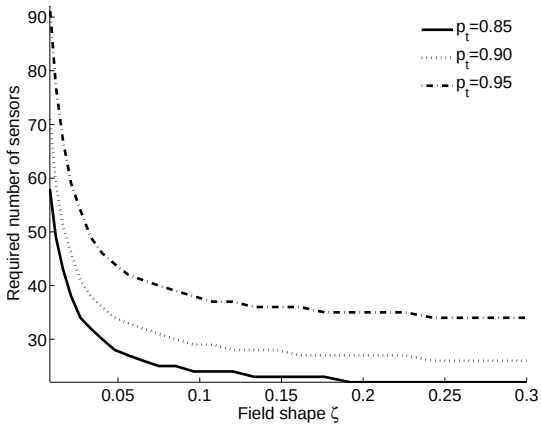


Figure 4.4. The effect of field shape parameter $\zeta = D_2/D_1$ on the required number of sensors for different threshold detection probabilities where total area is 3000 m^2, $d_t = 10$ meters

target detection probability. However, if $\zeta = 0.30$, deploying 22 sensors is adequate. The effect of the field shape is more influential when the shape parameter is quite small. That is, when the field is a rather narrow and long region, more sensors are required. When ζ is larger than 0.1, shape does not affect the required number of sensors much.

The average sensing- and communication-neighboring degrees increase as the sensing range increases. For example, when 10 sensors with seven meters of sensing range is utilized, the average sensing neighboring degree is 1.02. The average communication degree is 3.15 if the communication range of the sensor is 14 m. When the network is planned according to the sensing-coverage, it can be considered as over-engineered in terms of the communication degree. Hence, high redundancy for communication is provided if the network is planned according to the sensing that is the main functionality of the network.

5. TEMPORAL BEHAVIOR OF THE DEPLOYMENT QUALITY

Suppose that a perimeter is to be monitored and unauthorized intruders traversing the field-of-interest are to be detected by the SWSN. The quality of surveillance provisioned after the initial deployment is presented in the previous chapter without considering its temporal resilience. Failures of the sensors influence the sensing coverage, and the provisioned sensing quality diminishes. For surveillance applications, definition of the network lifetime in terms of the sensing quality is a must. Taking the sensor failures as the root cause, the objective of recent literature such as [89] is to increase the network lifetime with energy-aware protocols. Along with energy awareness, the effect of failures on the sensing capability needs a rigorous analysis. This view point opens up a new research perspective: temporal resilience of the surveillance quality and definition of the lifetime of the SWSN in terms of the deployment quality measures.

5.1. Lifetime Definitions

The principle stated in [90] is that the network lifetime definition must consider the capability of the network towards satisfying the design purpose. The simplistic network lifetime definition depends on the assumption that the network dies when the first sensor runs out of battery. An extensive survey about the network lifetime can be found in [91]. Considering just the ratio of alive sensors is acceptable for applications of wireless sensor networks where periodic messaging with a balanced routing strategy is implemented. However, event generations in surveillance applications are not deterministic, and death of several sensors may not cause significant degradation of the deployment quality. The network is considered operational as long as it provides the required surveillance quality.

The presence of an intruder may be decided by more than one neighboring sensors in a short period of time. Hence, there are spatial and temporal correlations among

the detections of intruders in a SWSN. Also, the trajectory of the breach is influential on the event generations and causes spatial locality of sensor decisions. The detections causes power consumption not only by sensing units but also by the radio unit of the sensor because the presence decision of an intruder must be communicated to the sink.

In this work, we define the following network lifetime definitions based on the deployment quality measures defined in the previous chapter:

Deployment quality lifetime (τ^{dqm}) After the deployment of the sensors, the deployment quality is calculated as formulated in Section 3.2. The deployment quality measure is calculated after each sensor dies and if the value of this measure is less than a threshold (e.g. 0.95) the network is regarded as dead.

Poorly detected area lifetime (τ^{pd}) If the ratio of poorly detected area to the area of the field-of-interest Q_{PD} defined in Equation 3.6 is greater then a threshold value (e.g. 0.05) the network is regarded as dead.

Redeployment lifetime (τ^{rd}) If the ratio of redeployment measure Q_{RD} defined in Equation 3.7 is greater then a threshold value (e.g. 0.05) the network is regarded as dead.

Connected sides lifetime (τ^{cs}) If there is a single poorly detected region that connects the secure and insecure sides of the field, then the network is regarded as dead.

First dead sensor lifetime (τ^{first}) The network is regarded as dead after the battery depletion of the first sensor.

In the previous chapter we proposed several deployment quality measures considering the spatial correlations without considering the effect of sensor failures in time. In this work, we analyze the temporal changes in the iso-sensing graph and deployment quality with a realistic dicrete event simulator. The nondeterministic nature of intrusions hardens the analytical modeling of the surveillance applications. Next, the application scenarios and the simulation setup to analyze the temporal behavior of the deployment quality measures are presented.

5.2. Application Scenarios and Simulation Setup

The rate of events has a significant impact on the operations of the SWSN. To analyze the effect of event rate we utilize two scenarios:

Rare-event surveillance scenario (RES): Assume a scenario where fugitives try to cross the country border illegally. The objective of the fugitive is to pass through the border monitored by a SWSN. Since, the intrusions will not be frequent, we refer to such scenarios as rare-event surveillance (RES) scenario.

Frequent-event surveillance scenario (FES): Assume a scenario where visitors of a historic arena such as the Temple of Artemis at Ephesus in Turkey is to be monitored. The objective of the SWSN is to detect the visitors whom are trying to enter unallowed parts of the arena. Compared to RES scenario, more frequent event detections are expected. Hence, this scenario is referred to as frequent-event surveillance (FES) scenario.

When compared to other applications of WSNs, RES scenario is not common because the sensor nodes are in *low-power listening* state most of the time during their lifetime. In the surveillance applications, since the main functionality is to sense, the sensing units of the nodes are active during the network lifetime. For an individual sensor, when compared to the energy consumptions of the radio module, the sensing unit consumes negligible power. However, for RES scenario, the situation is the opposite. Most of the power is consumed by the radio that is in *low power listening* mode and by the active sensing unit.

The simulation results show that more than 99 per cent of the power is used for low-power listening and sensing and the remaining power is consumed to receive and send packets. For the FES scenario, around 13 per cent of the power is consumed for communication. These results are obtained from 30 runs of the simulations where 100 sensors are deployed.

5.2.1. Simulation Setup

To analyze the temporal changes in the deployment quality, we developed a discrete event simulator using OmNet++ [72]. The field-of-interest is 300×50 m^2. Determining the sink positions is an optimization problem [92]. For the sake of simplicity, the sink is placed in the middle of the field although the position of the sink influences the battery consumption depending on the applied routing strategy [93]. Distributed Bellman-Ford routing strategy as described in [92] is utilized as the network layer of the sensor nodes. This strategy produces a minimum energy tree topology where the cost of the sensor-to-sink communication is minimized. The cost is defined as the power consumed to send a packet based on the inter-node distance. The sink is to be informed about the operational states of the individual sensor nodes. Hence, the sensor nodes periodically send an *alive* message to the sink. The period is an input parameter and it may be adjusted towards satisfying the application requirements. In the simulations, one *alive* message per hour is sent by the sensors since we do not assume any intentional destructions of the sensors. The sensors fail only because of power depletions. The sink continuously monitors the operational states and whenever a sensor does not send the *alive* message, the route establishment procedure is started by the sink. The energy consumptions of the route establishment phase is included in the calculations.

A sensor node is composed of a wireless communication module, one or more sensing units, and a processing unit. Energy consumptions are due to packet sending, packet receiving, low-power listening, sensing and processing. The sensor model consists of the communication and the sensing stacks. The application layer and the battery are the core units of the model. After defining the overall simulation setup, in the next sub-sections the sensor node, sensor and intruder models are described.

5.2.1.1. Wake-up Circuitry Model. In the surveillance scenario, detections occur rarely. When a sensor detects an intruder, it communicates the decision about the presence of an intruder to the sink. Except for periodic messaging (e.g. periodic *alive* messages sent to the sink), sensors only communicate when a detection occurs. As proposed

Table 5.1. Current consumptions of the transmission circuitry of the Chipcon CC1000 radio chip

Power level (dBm)	**Current drain** (mA)
-20	3.3
-5	8.9
0	10.4
5	14.8
10	26.7

in [94], we keep the communication stack in *low power listening* mode unless an event is detected. To wake up the communication stack, a low-power wake-up circuitry is modelled as proposed in [95, 96]. The wake-up circuitry consumes around 1 μA. Assuming perfect medium access (MAC) layer without any sleep scheduling is acceptable. The wake-up circuitry enables the communication stack when an intruder is detected, otherwise the communication stack is in *low power listening* mode. The delay introduced by the wake-up circuitry is 2.8 ms [94].

5.2.1.2. Radio Model. The physical layer of the communication stack uses single channel radio model. Many of the commercialized sensor motes such as Berkeley Mica2 motes [97], Exscal motes [98] use the Chipcon CC1000 radio chip [99]. This chip operates in the 300 to 1000 MHz range with a data rate between 0.3 to 76.8 kbps, supports multi-channel, and provides the received signal strength indicator to the application layer. The output power can be adjusted between -10 and 10 dBm and it is programmable. Hence, it is possible to set the output power while transmitting a packet according to the next hop distance. The sensitivity of the receiver is -110 dBm for a data rate of 1.2 kbps. When this chip is in *off-mode*, it consumes 0.2 μA. In receive mode, 7.4 mA is consumed at 433 MHz. The current consumptions for different transmission powers at 433 MHz are shown in Table 5.1. The maximum communication range with these parameters is 55 meters assuming free-space propagation model.

5.2.1.3. Sensor Model. Elfes's sensor detection model is employed in the simulations. We model a passive-infrared sensor with this model where the parameters are $r = 25$ meters, $r_e = 5$ meters, $\lambda = 0.1$ and $\beta = 0.9$. To decide on the detections, a random number is produced between zero and one. The probability of detecting the intruder is calculated as in Eq. 2.3 using the sensor-to-intruder distance. If the random number is smaller than the calculated detection probability, the application layer is informed about the intruder which in turn sends a message about the intrusion decision to the sink. Since the main functionality of the network is to sense, we assume that the sensing stack is always *active* in the simulations. As published by Dutta *et al.* in [100], the current consumption of the infrared sensor is 0.3 mA in *active* mode. The latency for the infrared sensor to switch from the *off-mode* to the *active* mode is more than one second. Hence, the assumption that the sensing unit is always active becomes more acceptable.

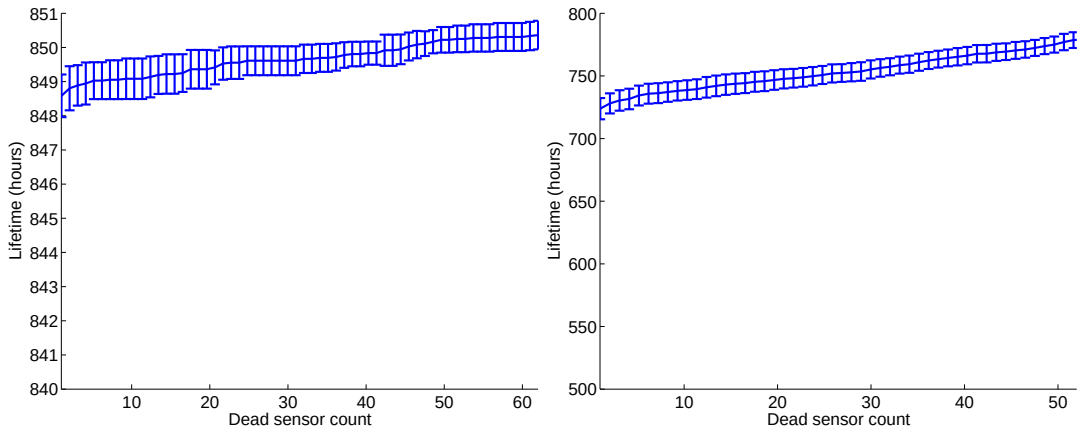
5.2.1.4. Intruder Mobility Model. The objective of the target is to pass from the insecure side of the perimeter to the secure side. We assume that the intruder does not know the sensor positions. A randomly positioned intruder in the insecure side walks through the perimeter. The step interval of the intruder is one second where the velocity is two meters per second. The intruder follows the trajectory for five seconds and changes its trajectory with a randomly chosen angle. At each trajectory change period, a uniformly distributed number between zero and 180 is generated and used as the angle of the trajectory change. The new position is calculated using the randomly generated angle and the step distance. The intruder is reflected from the vertical borders of the perimeter. After an intruder's traversal, another intruder tries to traverse the region in the same fashion which is referred to as re-occurrence. For the RES scenario, the re-occurrence period of the intruder is arranged to be uniformly distributed between 18 and 30 hours with a mean of one day. For the FES scenario, the re-occurrence period is uniformly distributed between 0.01 and 0.02 hours with a mean of 54 seconds. As the intruder traverses the field, the sensors take samples at each second. If a sensor decides on target presence, it communicates its decision to the sink. The energy consumptions of the routing overhead is included in the calculations.

5.3. Analysis of the Network Lifetime

After defining the simulation setup, in this section, we present the temporal behavior of the deployment quality.

5.3.1. Temporal Behavior of the Deployment Quality

For the RES and FES scenarios, the individual lifetimes of the first 50 per cent of the initially deployed sensors are depicted in Figure 5.1 as they progressively die out. The error bars in these figures depict that the variance in the simulation results are in acceptable ranges. For both scenarios, the trend in the lifetime is similar. Several sensors deplete their batteries quickly after the death of the first sensor, then, the battery depletions slow down. For rare event detection scenarios, the difference between the value of any network lifetime definition and the lifetime of the first dead sensor are nearly equal. As the rate of the events increase, the network lifetime definition based on the first dead sensor is misleading because after a couple of battery depletions, the network is still in an acceptable operational status in terms of the sensing capability. For the RES scenario, the tenth sensor dies in an hour after the first sensor dies. For the FES scenario, this value is 20 hours. Most of the power consumption for

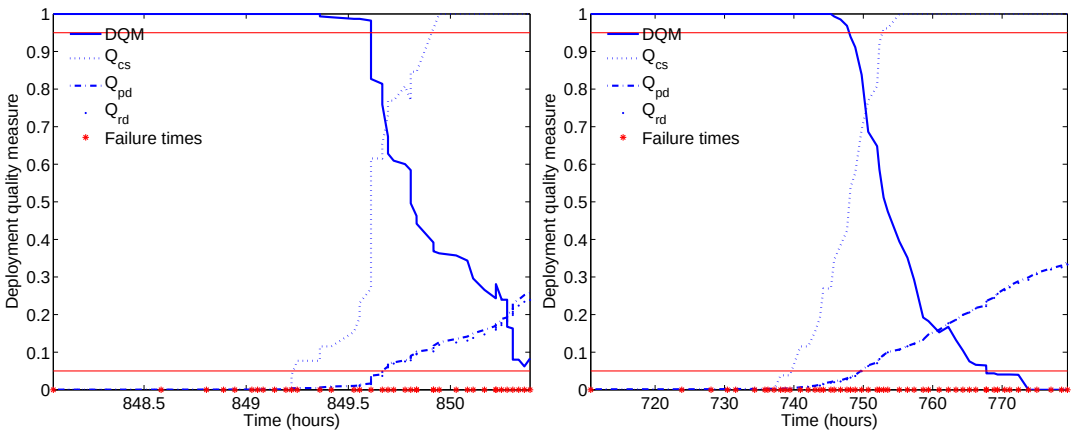


(a) Rare-event detection (b) Frequent-event detection

Figure 5.1. The lifetime of the individual sensors

the RES scenario is due to the low-power listening radio and active sensing units. The detections and the related communication activities have a negligible impact on the power depletions of the sensors. However, for the FES scenario, communication activities of the sensors influence the power depletions and the inter-death times of the sensors are regulated according to the packet transmission and reception loads of the sensors. Relay nodes die faster.

The temporal changes in the deployment quality for the RES and FES scenarios are depicted in Figure 5.2. The threshold values are 0.95 for the DQM and 0.05 for Q_{PD}, Q_{RD} and Q_{CS}. These figures depict the effect of dead sensors on the deployment quality clearly. For the RES and the FES scenarios, the effect is similar. The change in the redeployment and poorly detected area measures are the same. This suggest that a single gap occurs in the field-of-interest. As the sensors die, the DQM value decreases and sensing gaps occur in the field-of-interest. The sharp decrease in DQM and the sharp increase in Q_{CS} indicates a local failure of the sensors, as well. When distributed Bellman-Ford routing is applied, the sensors close to the sink die faster because of the relay-node functionality. This spatio-temporal phenomenon is regarded as the energy hole problem in the literature [101]. As the sensors die, the change in the DQMs increases because the same offered load is carried by the residual network.

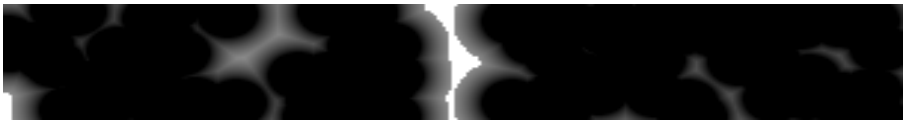


(a) Rare-event detection (b) Frequent-event detection

Figure 5.2. The temporal changes in the deployment quality measures

(a) Initial iso-sensing graph (MDIS)

(b) 10^{th} sensor dies



(c) Connected sides occur after the 15^{th} sensor dies

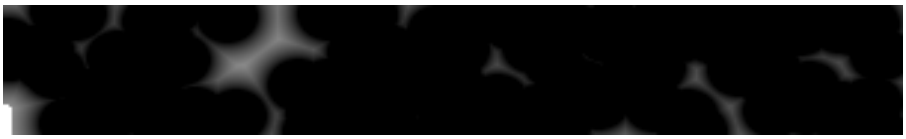
(d) 20^{th} sensor dies

(e) 30^{th} sensor dies

Figure 5.3. Demonstration of the energy hole problem when sensors are uniformly deployed in the field-of-interest of 300×50 m^2

5.3.2. Energy Hole Problem

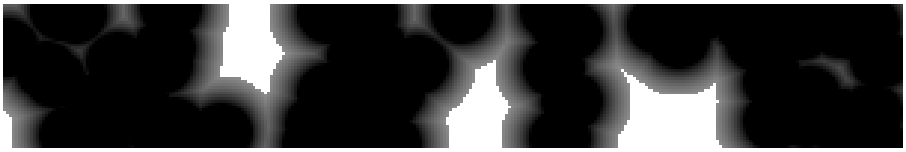
Ahmed *et al.* define the hole problem in [101] as the result of some anomalies in the wireless sensor networks that impair the functionality of the network. Specifically,



(a) Initial iso-sensing graph (MDIS)

(b) 20^{th} sensor dies

(c) 40^{th} sensor dies



(d) 50^{th} sensor dies

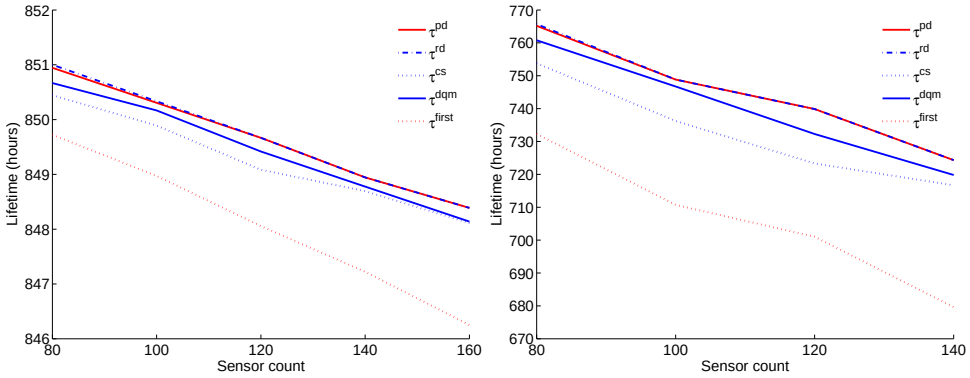
Figure 5.4. Demonstration of the energy hole problem when two sinks are deployed in the field-of-interest of 300×50 m^2

the coverage hole is defined as the area not covered by any sensor, due to the anomalies such as random deployment creating voids, node failures, and jamming. In this work, we consider the coverage hole as the sensing gap which is a consequence of the dead sensors in a region. The communication in a SWSN is converge-cast, in other words, most of communication is initiated by the sensors to the sink. Hence, depending on the routing strategy applied some bottleneck sensors exist in the deployment. The bottleneck nodes are the ones deployed close to the sink.

Figures 5.3 and 5.4 demonstrate the energy hole problem in the simulations where one and two sinks are deployed, respectively. The field is 300×50 m^2 and 100 sensors are deployed. For the one sink demonstration, the sink is in the middle, and for the two-sink demonstration, the sink positions are (100,25) and (200,25). The initial iso-sensing graph is shown in Figure 5.3(a). The black region is well-secured. As time passes, sensors start to die. The sink is in the middle of the field. As the figure depicts, the sensors around the sink dies faster and a gap is produced around the sink. Since the width of the field is narrow, the gap is connected both to the secure and insecure sides. After the first 10 sensors die, the sensing coverage does not have any breach paths. After the death of the 15^th sensor, the connected sides measure becomes one, although most of the area is well covered. As more sensors die, the gap gets larger and the Q_{PD} and Q_{RD} measures increase. Notice that there is a single big gap. Consequently, Q_{PD} and Q_{RD} measures are equal. For the two-sink demonstration, the energy holes occur around the sinks and around the boundary region between the clusters produced by the minimum energy tree routing. Notice that in Figure 5.4, there is still no gap connecting both sides after the death of the 50^{th} sensor. But, the faded regions imply the potential breach holes. Gaussian deployments where the mean is the sink position may reduce the effect of the energy hole problem.

5.3.3. Deployed Number of Sensors

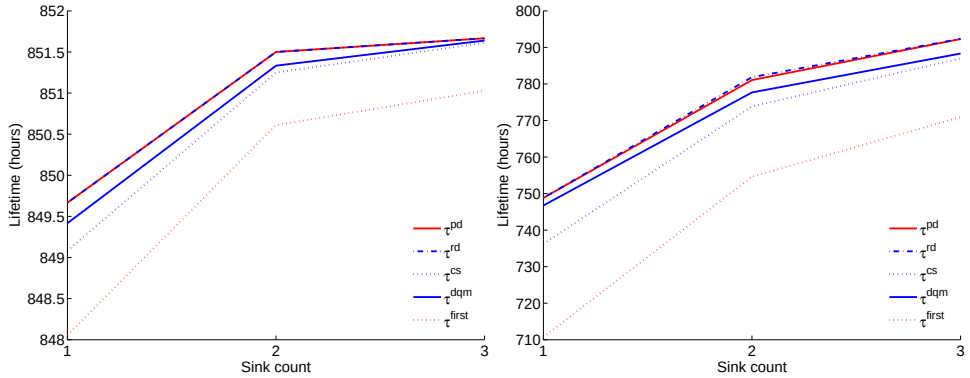
The impact of the redundant deployment on the lifetime of SWSNs is shown in Figure 5.5. As the number of deployed sensors increase, the lifetime decreases. This is a significant phenomenon. For the RES scenario, the impact is negligible compared to the results for the FES scenario. Increasing the initially deployed sensor count from 80 to 160 decreases the lifetime of the network by around four hours. However, for the FES scenario, the decrease is around 40 hours. As the number of deployed sensors increases, more *alive* messages are sent and more detections occur. As a consequence of more communication, the relay nodes close to the sink carry more traffic and deplete their batteries even faster. In other words, the energy hole problem occurs rapidly as more sensors are deployed.



(a) Rare-event detection (b) Frequent-event detection

Figure 5.5. The effect of the number of sensors on the network lifetime

Figure 5.5 also depicts that the sensing gap is not large however it is connected to both sides of the field-of-interest. For both of the scenarios, the lifetime values decrease as the sensor count increases. For the RES scenario, it can be concluded that it is acceptable to use the first node's failure time as the network lifetime. However, for the FES scenario, other deployment quality based lifetime definitions are more appropriate. That is for the FES scenario, $\tau^{rd} \sim \tau^{pd} > \tau^{dqm} > \tau^{cs} > \tau^{first}$ and for the RES scenario $\tau^{rd} \sim \tau^{pd} \sim \tau^{dqm} \sim \tau^{cs} \sim \tau^{first}$.



(a) Rare-event detection (b) Frequent-event detection

Figure 5.6. The effect of deployed number of sinks on the network lifetime

5.3.4. Deployed Number of Sinks

The packets are forwarded to the data collection centers referred to as sinks and the data flow in wireless sensor networks is converge-cast. Any packet is sent to the sink in a multi-hop fashion that necessitates relay node functionality. The effect of the deployed number of sinks on the network lifetime is presented in Figure 5.6 for the RES and the FES scenarios. Due to low communication requirement in the RES scenario, the sink count is not influential on the network lifetime because a small amount of power is consumed due to the communication activity. However, for the FES scenario, the overall communication requirement is large. Hence, the power consumed for the relay functionality becomes influential. Increasing the number of sinks, decreases the hops encountered by packets. Thus, the power consumed for the relay functionality decreases and the overall network lifetime increases as more sinks are deployed.

In these simulations, the field-of-interest is 300×50 m^2. For the one sink scenario, the sink is in the middle of the field. For the two sinks scenario, the position of the two sinks are (100,25) and (200,25). For the three sinks scenario, the positions are (75,25), (150,25) and (225,25). For the FES scenario, as seen in Figure 5.6(b), as additional sinks are deployed, the increase in the network lifetime deaccelerates. For example, if one sink is deployed, the network lifetime defined as the time of the first dead sensor is 710 hours. If two sinks are deployed, the network lifetime increases around 40 hours. The increase in the network lifetime is around 20 hours if the third sink is introduced. As the number of sinks increases, the topology of the network changes from multi-hop to one-hop fashion. After deploying a fixed number of sinks in the field-of-interest, the power consumed for the relay functionality of the sensor nodes reduces to zero which results in less gain in the network lifetime with additional sink deployments. Hence, a convergence trend is seen in Figure 5.6.

5.3.5. Effect of Intruder Mobility

The rate of the events in a SWSN have a significant impact on the network lifetime. As the rate of the events increases, the number of successful detections increase

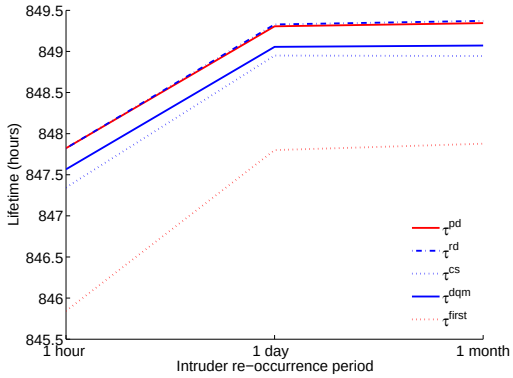
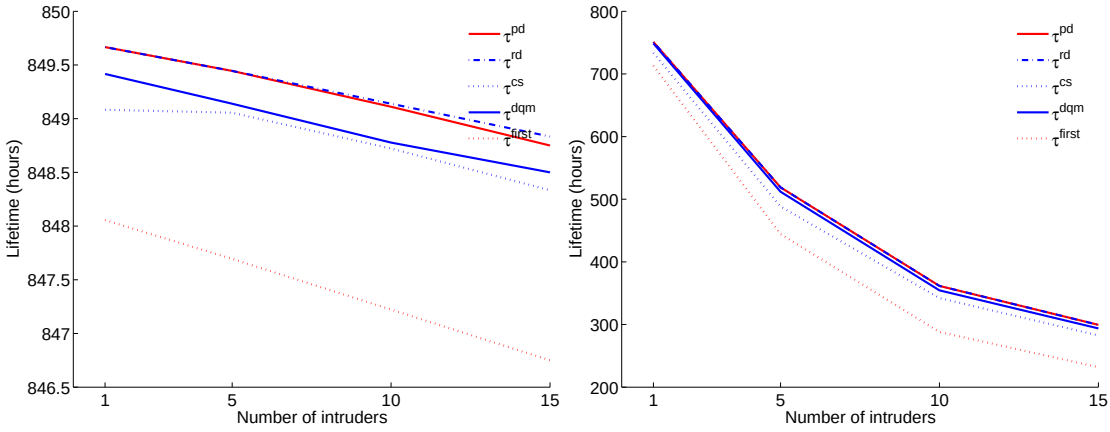


Figure 5.7. The effect of the intruder re-occurrence period (time between the occurrence of two distinct intruders) on the network lifetime

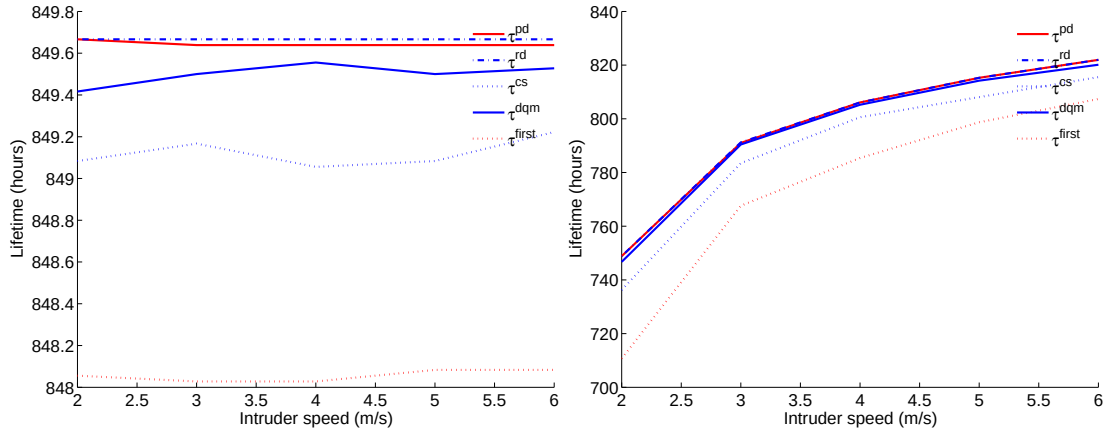
and consequently the communication costs increase. In the simulations, no aggregation methods are applied. Hence, each detection results in a packet that is routed from the initiating sensor to the sink following the minimum energy tree path. The intruder re-occurrence period affects the rate of the events. As more intruders try to traverse the region, more detections occur and more packets are produced to communicate the sensor decisions. In Figure 5.7, the impact of the intruder re-occurrence period on the network lifetime is shown. As the re-occurrence period gets larger, fewer penetrations are observed. If the FES and the RES scenarios are considered as the two extreme cases, from FES to RES the network lifetime increases.

In the simulations, another parameter that affects the rate of the events is the intruder count. As more intruders penetrate simultaneously, more detections occur. As seen in Figure 5.8, as the intruder count increases, the network lifetime decreases. For the RES scenario, the decrease is negligible since the low-power listening period is much more dominant than the duty period of the sensors. For the scenarios where events occur more frequently, the effect of the number of intruders on the network lifetime is very significant. When Figure 5.8(b) is analyzed, if 10 intruders try to penetrate through the field-of-interest, the network lifetime becomes the half of the value where only one intruder penetrates at a time.



(a) Rare-event detection (b) Frequent-event detection

Figure 5.8. The effect of the number of intruders on the network lifetime



(a) Rare-event detection (b) Frequent-event detection

Figure 5.9. The effect of the intruder speed (meters per second) on the network lifetime

The speed of the intruder is influential on the event generations. As the speed of the intruder increases, less samples can be taken by the sensors, and the probability of detection decreases causing a decay in the event rate. Again, for the RES scenario, the speed of the target has a negligible effect on the network lifetime. For the FES scenario, as the speed of the single intruder increase, the network lifetime increases significantly.

This is due to the fewer communication requirement based on the intrusion detections. This phenomenon indirectly shows the trade-off between the sample rate of the sensors and the lifetime. If sensors take more samples, then more communication is required to inform the sink about the detections which in turn reduces the network lifetime.

5.3.6. Comparative Evaluation of Sensing Range and Sensor Count

One of the issues in the design of the SWSN is determining the required number of sensors. The deployment quality depends on the sensing range and the number of sensors. In previous chapters, we presented how to determine the required number of sensors to provide an initial deployment quality level when the sensing ranges of the sensors are known. In this section, we analyze the trade-off between the sensing range and the required number of sensors in terms of its effect on the network lifetime. If sensors with larger sensing ranges are deployed, the required number of sensors is smaller compared to those deployments of sensors with smaller sensing ranges.

For different sensing ranges as shown in Table 5.2, the required number of sensors are calculated to provide an initial deployment quality of 0.95 calculated with Algorithm shown in Figure 3.7. The Elfes's sensor detection model is used where $r_e = 5$ meters, $\lambda = 0.5$ and $\beta = 0.5$. As the sensing range increases, the required number of sensors decrease. For example, for $r = 15$ meters, 116 sensors are required, whereas, for $r = 25$ meters, 63 sensors are adequate. As concluded from Figure 5.5, increasing the deployed number of sensors decreases the lifetime. However, as seen in Table 5.2, the lifetime of the network remains nearly equal by changing the sensor count and sensing range at the same time. Decreasing the sensing range of sensors results in fewer detections and the overall communication activity of the network decreases. Consequently, the effect seen in Figure 5.5 is not observed here. This concludes that deploying only the required number of sensors without redundancy to provide the initial deployment quality threshold is the best strategy in terms of the network lifetime.

Table 5.2. The effect of the number of sensors R and sensing range r on the network lifetime (hours) when Elfes's detectors are deployed where $r_e = 5$ meters, $\lambda = 0.5$ and $\beta = 0.5$

r	R	τ^{pd}	τ^{rd}	τ^{cs}	τ^{dqm}	τ^{first}
15	116	822.61	829.1	822.61	822.61	822.61
20	88	805.73	809.8	793.07	807.35	793.07
25	63	791.09	792.9	775.56	785.23	767.23

6. CONCLUSIONS

In this thesis, we formulate the weakest breach path problem and employ the breach probability and the maximum breach detection probability on the path for the performance assessment of SWSN. In doing so, the effects of various sensor and propagation parameters are analyzed. Ultimately, the goal is to determine the required number of sensors to bound the breach probability and to obtain an acceptable breach detection probability level. The evaluations lead to the conclusion that the breach detection probability is most sensitive to the false alarm rate. The SNR has an impact when the path loss exponent is small. Operating at a high SNR is ineffective if the signal attenuates faster with target-to-sensor distance. Therefore, placing the sensors such that they have an unobstructed view of the target is crucial. Increasing the number of data collected for a breach decision by a single sensor enhances the performance of the SWSN. However, the trade-off between the data size and power consumption must be further investigated. As the number of sensors deployed increases, the breach detection probability improves as expected. However, the trade-off between the cost of sensors and the deployment, and the performance of the SWSN must be analyzed.

By defining the breach probability as the miss probability of the weakest breach path, the false alarm rate constraint has a significant impact on the breach probability, as well as the required number of sensor nodes for a given breach probability level. For fields where the signal attenuates faster with distance, large SNR levels are needed. Upon analyzing the effect of the field shape on breach probability, it is concluded that the differences between the breach probabilities of uniformly and normally distributed y-axis schemes are larger for narrower fields. Furthermore, the width of the field has a noticeable impact on the breach probability. The model and results developed in this thesis give clues that link false alarms to energy efficiency. Enforcing a low false alarm rate to avoid unnecessary response costs implies either a larger data-set (L) and hence a greater battery consumption, or a denser sensor network, which increases the deployment cost.

We applied the watershed segmentation algorithm on the sensing coverage and reduced the solution space to find the weakest breach path in surveillance wireless sensor networks. The sensor detection model proposed by Elfes is utilized to calculate the sensing coverage. This model has two significant properties: the detection model is a truncated one and it acts as a binary detection model when $\lambda = 1$, $\beta = 1$ or $\lambda = 0$, $\beta = 0$. Utilizing two scenarios, namely the embassy perimeter security and country border surveillance scenarios, we analyzed the effects of detection model parameters, sensor requirement and field width. The breach probability increases in λ and/or β. With constant number of sensor nodes, the breach probability also increases if the field is widened, especially when the width is larger than $r + r_e$. Furthermore, increasing the number of sensors does not affect the breach probability until a sensor is deployed close to the weakest path.

In this thesis, we propose several deployment quality measures and the utilization of the watershed segmentation algorithm to find the possible breach paths in a surveillance field with obstacles. In order to apply the watershed segmentation, the iso-sensing graph is defined and a recursive algorithm is designed to find the deployment quality measure defined as the maximum detection probability on the weakest breach path. The simulations indicate the impact of the false alarm rate and the sensor count on the deployment quality measure.

The wireless sensor network application designer may merely use MDIS (KIS with $K = 1$) if the required security level is not extremely high. Otherwise, using RIS or KRIS is more appropriate. Furthermore, to use KIS or KRIS is beneficial when large number of sensors are to be deployed and a sleep scheduling algorithm is to be implement to prolong the lifetime of the network. The false alarm rate and the path-loss exponent affect the deployment quality measures significantly. The choice of the threshold value to find the poorly detected areas in the field is also critical. As more sensors are deployed in the region, the quality of the deployment is enhanced.

An analytical model to determine the deployment quality is proposed in this thesis where binary detectors are utilized. Using this model, it is possible to calculate

the required number of sensors to provide the predetermined deployment quality level. Furthermore, some routing protocols depend on the neighboring degree of sensors. The sensing- and communication neighboring degrees can be calculated with this model. The analytical evaluation results closely match the simulation outcomes. The designer of the network may use the sensing- and communication-neighboring degrees as decision criteria along with the threshold DQM level.

Simulations have shown that the energy hole problem in surveillance applications of wireless sensor networks needs rigorous analysis. To find the bottleneck sensors whose deaths creates sensing gaps in the field-of-interest can be identified right after deployment. The routing strategy, sink positions and sensor deployment scheme affect the potential energy holes in the field-of-interest. Another conclusion drawn from the discrete event simulations is that for rare-event detection scenarios such as border surveillance applications, most of energy is consumed by the low-power listening of the radio and the active sensing unit. Hence, redundant deployments do not extend the lifetime of the network. Consequently, deploying exactly the required number of sensors providing an initial deployment quality is the right approach. More sensors do not contribute to the network lifetime. Also, the lifetime of the first dead sensors is almost equal to the network lifetime if events are very rare. As the major conclusion of the discrete event simulations, we can state that deploying only the required number of sensors without redundancy to provide the initial deployment quality threshold is the best strategy in favor of the network lifetime.

As future work of this thesis, the effect of energy holes on the deployment quality can be analyzed and algorithms to reveal the potential energy holes just after deployment can be proposed. The effects of different routing strategies and medium access layer protocols on the hole problem can be analyzed. Moreover, appropriate medium access control and routing protocols can be proposed considering the deployment quality. Three dimensional field models with realistic obstacles will increase the quality of the work.

REFERENCES

1. Romer, K. and F. Mattern, "The design space of wireless sensor networks", *IEEE Wireless Communications*, Vol. 11, No. 6, pp. 54–61, 2004.

2. Akyildiz, I., W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102–114, 2002.

3. Vieira, M., C. C. Jr, D. C. da Silva Jr, and J. da Mata, "Survey on wireless sensor network devices", *Emerging Technologies and Factory Automation*, pp. 16–19, 2003.

4. Callaway, E., *Wireless Sensor Networks: architectures and protocols*, CRC Press, 2004.

5. Baronti, P., P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", *Computer Communications*, Vol. 30, No. 7, pp. 1655–1695, 2007.

6. Burrell, J., T. Brooke, and R. Beckwith, "Vineyard Computing: Sensor Networks in Agricultural Production", *IEEE Pervasive Computing*, Vol. 03, No. 1, pp. 38–45, 2004.

7. Mainwaring, A., D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring", *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pp. 88–97, Atlanta, Georgia, USA, 2002.

8. Szewczyk, R., E. Osterweil, J. Polastre, M. Hamilton, A. Mainwaring, and D. Estrin, "Habitat monitoring with sensor networks", *Communications of the ACM*, Vol. 47, No. 6, pp. 34–40, 2004.

9. Kim, S., S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, "Wireless sensor networks for structural health monitoring", *Proceedings of the 4th international conference on Embedded networked sensor systems*, pp. 427–428, Boulder, Colorado, USA, 2006.

10. Yu, Y., L. J. Rittle, V. Bhandari, and J. B. LeBrun, "Supporting concurrent applications in wireless sensor networks", *Proceedings of the 4th international conference on Embedded networked sensor systems*, pp. 139–152, Boulder, Colorado, USA, 2006.

11. Sridharan, M., R. Ramnath, E. Ertin, and A. Arora, "Mobility centric campus area sensor network for locality specific applications", *Proceedings of the 4th international conference on Embedded networked sensor systems*, pp. 371–372, Boulder, Colorado, USA, 2006.

12. Pandey, R. and J. Koshy, "A software framework for integrated sensor network applications", *Proceedings of the first international conference on Integrated internet ad hoc and sensor networks*, p. 11, ACM Press, Nice, France, 2006.

13. Handziski, V., A. Köpke, A. Willig, and A. Wolisz, "TWIST: a scalable and reconfigurable testbed for wireless indoor experiments with sensor networks", *Proceedings of the second international workshop on Multi-hop ad hoc networks: from theory to reality*, pp. 63–70, Florence, Italy, 2006.

14. Chelius, G., A. Fraboulet, and E. Fleury, "Demonstration of wrldsens: a fast prototyping and performance evaluation of wireless sensor network applications & protocols", *Proceedings of the second international workshop on Multi-hop ad hoc networks: from theory to reality*, pp. 131–133, Florence, Italy, 2006.

15. Hu, W., V. N. Tran, N. Bulusu, C. T. Chou, S. Jha, and A. Taylor, "The design and evaluation of a hybrid sensor network for Cane-Toad monitoring", *Proceedings of the 4th international symposium on Information processing in sensor networks*, p. 71, Los Angeles, California, 2005.

16. Chong, C.-Y. and S. P. Kumar, "Sensor networks: evolution, opportunities, and challenges", *Proceedings of the IEEE*, Vol. 91, No. 8, pp. 1247–1256, 2003.

17. Onur, E., C. Ersoy, and H. Deliç, "Sensing coverage and breach paths in surveillance wireless sensor networks", Phoha, S., T. F. L. Porta, and C. Griffin (editors), *Sensor Network Operations*, pp. 68–86, Wiley Interscience-IEEE Press, New York, USA, Jun 2006.

18. Tilak, S., N. B. Abu-Ghazaleh, and W. Heinzelman, "Infrastructure tradeoffs for sensor networks", *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pp. 49–58, New York, NY, USA, 2002.

19. Clouqueur, T., V. Phipatanasuphorn, P. Ramanathan, and K. K. Saluja, "Sensor deployment strategy for target detection", *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pp. 42–48, New York, NY, USA, 2002.

20. 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, Aug 2003.

21. Zou, Y. and K. Chakrabarty, "Sensor Deployment and Target Localization Based on Virtual Forces", *Proceedings of the IEEE INFOCOM*, pp. 1293–1303, Apr 2003.

22. Wang, X., G. Xing, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated coverage and connectivity configuration in wireless sensor networks", *Proceedings of the First International Conference on Embedded Networked Sensor Systems*, pp. 28–39, Nov 2003.

23. Ye, F., G. Zhong, J. Cheng, S. Lu, and L. Zhang, "PEAS: A Robust Energy Conserving Protocol for Long-lived Sensor Networks", *Proceedings of the 23rd IEEE Conference on Distributed Computing Systems*, p. 28, DC, USA, May 2003.

24. Tian, D. and N. D. Georganas, "A coverage-preserving node scheduling scheme for large wireless sensor networks", *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, pp. 32–41, Atlanta, Georgia, USA, 2002.

25. Carle, J. and D. Simplot-Ryl, "Energy-Efficient Area Monitoring for Sensor Networks", *IEEE Computer*, Vol. 37, No. 2, pp. 40–46, 2004.

26. Howard, A., M. J. Matarić, and G. S. Sukhatme, "An Incremental Self-Deployment Algorithm for Mobile Sensor Networks", *Autonomous Robots*, Vol. 13, No. 2, pp. 113–126, Sep 2002.

27. Habib, S. J., "Modeling and simulating coverage in sensor networks", *Computer Communications*, Vol. 30, No. 5, pp. 1029–1035, 2007.

28. Huang, C.-F. and Y.-C. Tseng, "The coverage problem in a wireless sensor network", *Mobile Networks and Applications*, Vol. 10, No. 4, pp. 519–528, 2005.

29. Ganeriwal, S., A. Kansal, and M. B. Srivastava, "Self aware actuation for fault repair in sensor networks", *Proceedings of the IEEE International Conference on Robotics and Automation*, Vol. 5, pp. 5244– 5249, New Orleans, USA, May 2004.

30. Onur, E., C. Ersoy, and H. Deliç, "How Many Sensors for an Acceptable Breach Probability Level?", *Computer Communications*, Vol. 29, No. 2, pp. 172–182, Jan 2006.

31. He, T., S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, J. Hui, and B. Krogh, "Energy-efficient surveillance system using wireless sensor networks", *Proceedings of the second international conference on Mobile systems, applications, and services*, pp. 270–283, Boston, MA, USA, Jun 2004.

32. Megerian, S., F. Koushanfar, M. Potkonjak, and M. B. Srivastava, "Worst and Best-Case Coverage in Sensor Networks", *IEEE Transactions on Mobile Computing*, Vol. 4, No. 1, pp. 84–92, Jan/Feb 2004.

33. Megerian, S., F. Koushanfar, G. Qu, G. Veltri, and M. Potkonjak, "Exposure in wireless sensor networks: theory and practical solutions", *Wireless Networks*, Vol. 8, No. 5, pp. 443–454, Sep 2002.

34. 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*, pp. 519–528, Cambridge, Massachusetts, USA, 2007.

35. Mehta, D. P., M. A. Lopez, and L. Lin, "Optimal coverage paths in ad-hoc sensor networks", *Proceedings of the IEEE International Conference on Communications*, Vol. 26, pp. 507–511, Anchorage, USA, May 2003.

36. Li, X.-Y., P.-J. Wan, and O. Frieder, "Coverage in Wireless Ad-hoc Sensor Networks", *IEEE Transactions on Computers*, Vol. 52, No. 6, pp. 753–763, Jun 2003.

37. Meguerdichian, S., F. Koushanfar, M. Potkonjak, and M. Srivastava, "Coverage problems in wireless ad-hoc sensor network", *Proceedings of the IEEE INFOCOM*, pp. 1380–1387, Anchorage, USA, Apr 2001.

38. Chvatal, V., "A combinatorial theorem in plane geometry", *Journal of Combinatorial Theory*, Vol. B, No. 13, pp. 39–41, 1975.

39. Dhillon, S. S. and K. Chakrabarty, "Sensor placement for effective coverage and surveillance in distributed sensor networks", *Proceedings of the IEEE Wireless Communications and Networking Conference*, pp. 1609–1614, New Orleans, USA, Mar 2003.

40. Adlakha, S. and M. Srivastava, "Critical density thresholds for coverage in wireless sensor networks", *Proceedings of the IEEE Wireless Communications and Networking Conference*, pp. 1615–1620, New Orleans, USA, Mar 2003.

41. Lu, J. and T. Suda, "Coverage-aware self-scheduling in sensor networks", *Proceedings of the IEEE 18th Annual Workshop on Computer Communications*, pp. 117–123, DanaPoint, California, USA, Oct 2003.

42. Dasgupta, K., M. Kukreja, and K. Kalpakis, "Topology-Aware Placement and Role Assignment for Energy-Efficient Information Gathering in Sensor Networks", *Proceedings of the Eighth IEEE International Symposium on Computers and Communications*, p. 341, Washington, DC, USA, 2003.

43. Zhang, H. and J. C. Hou, "On the upper bound of α-lifetime for large sensor networks", *ACM Transactions on Sensor Networks*, Vol. 1, No. 2, pp. 272–300, 2005.

44. Zhang, H. and J. C. Hou, "Maintaining Coverage and Connectivity in Large Sensor Networks", *Ad Hoc and Sensor Wireless Networks*, Vol. 1, No. 1-2, pp. 89–124, 2005.

45. Wu, J. and S. Yang, "Coverage Issue in Sensor Networks with Adjustable Ranges", *Proceedings of the 2004 International Conference on Parallel Processing Workshops (ICPPW'04)*, pp. 61–68, Washington, DC, USA, 2004.

46. Huang, C.-F., Y.-C. Tseng, and H.-L. Wu, "Distributed protocols for ensuring both coverage and connectivity of a wireless sensor network", *ACM Transactions on Sensor Networks*, Vol. 3, No. 1, p. 5, 2007.

47. Bai, H., X. Chen, B. Li, and D. Han, "A Location-free Algorithm of Energy-Efficient Connected Coverage for High Density Wireless Sensor Networks", *Discrete Event Dynamic Systems*, Vol. 17, No. 1, pp. 1–21, 2007.

48. Xing, G., X. Wang, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated coverage and connectivity configuration for energy conservation in sensor networks", *ACM Transactions on Sensor Networks*, Vol. 1, No. 1, pp. 36–72, Aug 2005.

49. Ravelomanana, V., "Extremal Properties of Three-Dimensional Sensor Networks with Applications", *IEEE Transactions on Mobile Computing*, Vol. 3, No. 3, pp. 246–257, Jul 2004.

50. Wang, L. and Y. Xiao, "A survey of energy-efficient scheduling mechanisms in sensor networks", *Mobile Networks and Applications*, Vol. 11, No. 5, pp. 723–740, 2006.

51. Liu, C., K. Wu, Y. Xiao, and B. Sun, "Random Coverage with Guaranteed Connectivity: Joint Scheduling for Wireless Sensor Networks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 17, No. 6, pp. 562–575, Jun 2006.

52. Ren, S., Q. Li, H. Wang, X. Chen, and X. Zhang, "Design and Analysis of Sensing Scheduling Algorithms under Partial Coverage for Object Detection in Sensor Networks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 18, No. 3, pp. 334–350, 2007.

53. Hsin, C. F. and M. Liu, "Randomly Duty-cycled Wireless Sensor Networks: Dynamics of Coverage", *IEEE Transactions on Wireless Communications*, Vol. 5, No. 11, pp. 3182–3192, Nov 2006.

54. Wang, W., V. Srinivasan, K.-C. Chua, and B. Wang, "Energy-efficient coverage for target detection in wireless sensor networks", *Proceedings of the 6th international conference on Information processing in sensor networks*, pp. 313–322, ACM Press, New York, NY, USA, 2007.

55. Liang, W. and Y. Liu, "Online Data Gathering for Maximizing Network Lifetime in Sensor Networks", *IEEE Transactions on Mobile Computing*, Vol. 6, No. 1, pp. 2–11, 2007.

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

57. Demirkol, I., C. Ersoy, and F. Alagoz, "MAC protocols for wireless sensor networks: a survey", *IEEE Communications Magazine*, Vol. 44, No. 4, pp. 115–121, 2006.

58. Al-Karaki, J. and A. Kamal, "Routing techniques in wireless sensor networks: a survey", *IEEE Wireless Communications*, Vol. 11, No. 6, pp. 6–28, 2004.

59. Akkaya, K. and M. Younis, "A survey on routing protocols for wireless sensor networks", *Ad Hoc Networks*, Vol. 3, No. 3, pp. 325–349, 2005.

60. Chen, J., S. Kher, and A. Somani, "Distributed fault detection of wireless sensor networks", *Proceedings of the workshop on Dependability issues in wireless ad hoc networks and sensor networks*, pp. 65–72, Los Angeles, CA, USA, 2006.

61. Elfes, A., "Occupancy Grids: A Stochastic Spatial Representation for Active Robot Perception", Iyengar, S. S. and A. Elfes (editors), *Autonomous Mobile Robots: Perception, Mapping, and Navigation*, Vol. 1, pp. 60–70, IEEE Computer Society Press, Los Alamitos, CA, 1991.

62. Cao, Q., T. Yan, J. Stankovic, and T. Abdelzaher, "Analysis of Target Detection Performance for Wireless Sensor Networks", *Lecture Notes in Computer Science: Distributed Computing in Sensor Systems*, Vol. 3560, pp. 276–292, Jun 2005.

63. Kazakos, D. and P. Papantoni-Kazakos, *Detection and Estimation*, Computer Science Press, New York, USA, 1990.

64. McEwan, T. E., "Differential Pulse Radar Motion Sensor", *U.S. Patents*, 5966090, Oct 1999.

65. Dutta, P. K., A. K. Arora, and S. B. Bibyk, "Towards Radar-Enabled Sensor Networks", *Proceedings of the Fifth International Conference on Information Processing in Sensor Networks*, pp. 467–474, Nashville, TN, USA, Apr 2006.

66. Bazaraa, M., J. Jarvis, and H. Sherali, *Linear programming and network flows*, John Wiley & Sons Inc., New York, NY, USA, 1990.

67. Weiss, M., *Data structures and algorithm analysis in C++*, Benjamin-Cummings Publishing Co. Inc., Redwood City, CA, USA, 1994.

68. Veltri, G., Q. Huang, G. Qu, and M. Potkonjak, "Minimal and maximal exposure path algorithms for wireless embedded sensor networks", *Proceedings of the 1st international ACM conference on Embedded networked sensor systems*, pp. 40–50, November 2003.

69. Cardei, M. and J. Wu, "Coverage in Wireless Sensor Networks", Ilyas, M. (editor), *Handbook of Sensor Networks*, CRC Press, 2004.

70. 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. 583–598, Jun 1991.

71. Santaló, L. A., *Integral Geometry and Geometric Probability*, Addison-Wesley, Reading, Massachusetts USA, 1976.

72. Varga, A., "Software Tools for Networking: OmNet++", *IEEE Network Interactive*, Vol. 16, No. 4, 2002.

73. Arora, A., P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, M. Gouda, Y. Choi, T. Herman, S. Kulkarni, U. Arumugam, M. Nesterenko, A. Vora, and M. Miyashita, "A line in the sand: a wireless sensor network for target detection, classification, and tracking", *Computer Networks*, Vol. 46, No. 5, pp. 605–634, Dec 2004.

74. Yan, T., T. He, and J. A. Stankovic, "Differentiated surveillance for sensor networks", *Proceedings of the Conference on Embedded Networked Sensor Systems*, pp. 51–62, California, USA, Nov 2003.

75. Cärbunar, B., A. Grama, J. Vitek, and O. Cärbunar, "Redundancy and coverage detection in sensor networks", *ACM Transactions on Sensor Networks*, Vol. 2, No. 1, pp. 94–128, Feb 2006.

76. Aurenhammer, F., "Voronoi diagrams – a survey of a fundamental geometric data structure", *ACM Computing Surveys*, Vol. 23, No. 3, pp. 345–405, Sep 1991.

77. Kansal, A., E. Yuen, W. J. Kaiser, G. J. Pottie, and M. B. Srivastava, "Sensing uncertainty reduction using low complexity actuation", *Proceedings of the third international symposium on Information processing in sensor networks*, pp. 388–395, Berkeley, California, USA, Apr 2004.

78. Lin, F. Y. S. and P. L. Chiu, "A Near-Optimal Sensor Placement Algorithm to Achieve Complete Coverage/Discrimination in Sensor Networks", *IEEE Communications Letters*, Vol. 9, No. 1, pp. 43–45, Jan 2005.

79. Mechitov, K., S. Sundresh, Y. Kwon, and G. Agha, "Cooperative tracking with binary-detection sensor networks", *Proceedings of the First International Conference on Embedded Networked Sensor Systems*, pp. 332–333, New York, NY, USA, 2003.

80. Zou, Y. and K. Chakrabarty, "Uncertainty-aware and coverage-oriented deployment for sensor networks", *Journal of Parallel and Distributed Computing*, Vol. 64, No. 7, pp. 788–798, Jul 2004.

81. Chakrabarty, K., S. S. Iyengar, H. Qi, and E. Cho, "Grid Coverage for Surveillance and Target Location in Distributed Sensor Networks", *IEEE Transactions on Computers*, Vol. 51, No. 12, pp. 1448–1453, Dec 2002.

82. Cardei, M. and J. Wu, "Energy-Efficient Coverage Problems in Wireless Ad Hoc Sensor Networks", *Computer Communications*, Vol. 29, No. 4, pp. 413–420, 2006.

83. Wu, J. and S. Yang, "Energy-Efficient Node Scheduling Models In Sensor Networks With Adjustable Ranges", *International Journal of Foundations of Computer Science*, Vol. 16, No. 1, pp. 3–17, Feb 2005.

84. Roerdink, J. B. and A. Meijster, "The Watershed Transform: Definitions, Algorithms and Parallelization Strategies", *Fundamenta Informaticae*, Vol. 41, No. 1–2, pp. 187–228, Jan 2000.

85. Meyer, F., "Topographic distance and watershed lines", *Signal Processing*, Vol. 38, No. 1, pp. 113–125, 1994.

86. Haralick, R. and L. Shapiro, *Computer and Robot Vision*, Addison-Wesley Longman Publishing Co. Inc., Boston, MA, USA, 1992.

87. Xing, G., X. Wang, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated coverage and connectivity configuration in wireless sensor networks", *ACM Transactions on Sensor Networks*, Vol. 1, No. 1, pp. 401–412, 2005.

88. Miller, L. E., "Distribution of link distances in a wireless network", *Journal of Research of the National Institute of Standards and Technology*, Vol. 106, No. 2, pp. 401–412, Mar/Apr 2001.

89. Su, X., "A combinatorial algorithmic approach to energy efficient information collection in wireless sensor networks", *ACM Transactions on Sensor Networks*, Vol. 3, No. 1, p. 6, 2007.

90. Blough, D. and P. Santi, "Investigating upper bounds on network lifetime extension for cell-based energy conservation techniques in stationary adhoc networks", *Proceedings of the Conference on Mobile Computing and Networking*, pp. 183–192, 2002.

91. Dietrich, I. and F. Dressler, "On the Lifetime of Wireless Sensor Networks", Technical report, Erlangen-Nürnberg: Friedrich-Alexander-Universität, 2006.

92. Oyman, E. I., *Multiple Sink Location Problem and Energy Efficiency in Large Scale Wireless Sensor Networks*, Ph.D. thesis, 2004.

93. Koşar, R. and C. Ersoy, "Sink Placement in Wireless Sensor Networks Using Genetic Algorithms", *Proceedings of the Learning and Intelligent Optimization Conference*, Andalo, Trento, Italy, Feb 2007.

94. Gu, L. and J. Stankovic, "Radio-Triggered Wake-Up Capability for Sensor Networks", *10th IEEE Real-Time and Embedded Technology and Applications Symposium*, p. 27, Toronto, Canada, May 2004.

95. 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*, pp. 173–177, 1997.

96. 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.

97. Mica2 Motes, http://www.xbow.com/.

98. Exscal Motes, http://cast.cse.ohio-state.edu/exscal/.

99. Evjen, P. M., "Low Cost RF Solutions for AMR Systems", *Metering International*, , No. 4, pp. 41–42, 2002.

100. Dutta, P., M. Grimmer, A. Arora, S. Bibyk, and D. Culler, "Design of a wireless sensor network platform for detecting rare, random, and ephemeral events", *Proceedings of the 4th international symposium on Information processing in sensor networks*, p. 70, 2005.

101. Ahmed, N., S. S. Kanhere, and S. Jha, "The holes problem in wireless sensor networks: a survey", *Mobile Computing and Communications Review*, Vol. 9, No. 2, pp. 4–18, 2005.