

Sensing Coverage and Breach Paths in Surveillance Wireless Sensor Networks*

Ertan Onur*, Cem Ersoy*, Hakan Deliç[◊]

*NETLAB, Department of Computer Engineering

[◊]BUSIM Laboratory, Department of Electrical and Electronics Engineering

Boğaziçi University

Bebek 34342 Istanbul, Turkey

January 24, 2005

Abstract

In this paper, the sensing coverage area of surveillance wireless sensor networks is considered. The sensing coverage is determined by applying the Neyman-Pearson detection model and defining the breach probability on a grid-modeled field. Using a graph model for the perimeter, Dijkstra's shortest path algorithm is used to find the weakest breach path. The breach probability is linked to parameters such as the false alarm rate, size of the data record and the signal-to-noise ratio. Consequently, the required number of sensor nodes and the surveillance performance of the network are determined. The false alarm rate and the field width turn out to be the two most influential parameters on the breach probability.

*This work is supported by the State Planning Organization of Turkey under the grant number 03K120250, and by the Boğaziçi University Research Projects under the grant number 04A105.

1 Introduction and Related Work

Wireless sensor networks (WSN) are appropriate tools to monitor an area for surveillance. The primary challenges in building a surveillance wireless sensor network (SWSN) pertain to the decisions to be considered while deploying the sensors. These decisions may consist of communication and sensing range of sensor nodes and density of the SWSN, deployment strategy to be applied (random, regular, planned, etc.) and sink deployment. Depending on the range and the number of sensors, the sensing coverage area of the SWSN may contain breach paths. The probability that a target traverses the region through the breach path gives precious insight about the level of security provided by the SWSN. Thus, it is the aim of this paper to analyze the probability of the weakest breach path, and draw important inferences regarding the sensing and deployment parameters in a SWSN.

The sensing and communication ranges of some propriety devices are listed in [13]. For example, the sensing range of the Berkeley motes acoustic sensor, HMC1002 magnetometer sensor and thrubeam type photoelectric sensor are nearly one meter, 5 meters and 10 meters respectively. The communication range of the Berkeley motes MPR300, MPR400CB and MPR520A are 30, 150 and 300 meters, respectively. The ratio of the communication and sensing ranges shows that the network must be densely deployed. The high redundancy level of the network necessitates energy conservation schemes.

The effect of sensor deployment on the performance of target detection is considered in [1], 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 [14]. The problem is stated as maximizing the coverage area within a cluster in cluster-based sensor networks 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 [3], 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 net-

work infrastructure in [9], 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. However, 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.

In [5], 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 are left unanswered. It is not clear what the threshold value of the minimum exposure has to be to determine the required number of sensor nodes. Determining the threshold becomes too complex when different types of sensors are utilized.

The research efforts summarized above are all based on a generic sensing model which merely says that the detection performance of a sensor is inversely proportional to some power of the sensor-to-target distance. Such a superficial understanding of the sensor operation, which just takes into account the path loss, neglects such crucial parameters as the false alarm rate and the number of data processed per sensor decision, as well as the noise phenomenon with an acting signal-to-noise ratio (SNR) at the receiving end. This shortcoming leads to the inability to establish a link with other deployment-critical issues such as the required number of sensor nodes for a specified sensing coverage level and energy efficiency. Another common modeling flaw is to assume the same sensing capability for all sensor nodes. This is clearly not possible since different propagation and noise conditions will imply nonidentical detection capabilities, even if one supposes that the same type of sensors are deployed. The exposure calculations and deployment strategies described above become either “extremely difficult” if the sensor types are of different characteristics [5]. The need for a unifying sensing model is evident.

He *et al.* report that sensor nodes generate false alarms at a nonnegligible rate when a SWSN is run in an energy-efficient manner [2]. This observation further suggests that the sensing model must include the false alarms in its formulation. Motivated by the desire to gain more insight about the impact

of the parameters listed in the preceding paragraph, we employ in this paper the Neyman-Pearson detection model (NPDM) for each sensor, which ties performance to a maximum allowable false alarm rate, the size of the data set collected by the sensors at each stage of the decision process, and the signal-to-noise ratio. We define the breach path as that which has the lowest end-to-end detection probability, a quantity that is defined in a precise manner in the next section. We then proceed to find the breach path through Dijkstra's shortest path algorithm by assigning the negative logarithms of the miss probabilities as weights of the grid points. With NPDM and the associated use of Dijkstra's algorithm, we study the breach probability as a function of all parameters for both uniformly and normal-distributed random sensor deployment. One of the notable outcomes is the evaluation of the relationship between the field shape and the required number of sensor nodes.

In the next section we describe the weakest breach path problem and present how to find the sensing coverage using the Neyman-Pearson detection model. Dijkstra's shortest path algorithm is proposed as a solution to this problem by defining a grid-based field model. After presenting the problem formally, the results are analyzed in Section 3. After the results and discussions, we draw our conclusions in Section 4.

2 The Weakest Breach Path Problem

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 have to be segmented in order to deal with the complexity. Segmentation can be done according to the environmental properties of the perimeter such as altitude and topography. In this paper, we work with a single segment.

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

In order to simplify the formulations, we model the field as a cross-connected grid. A sample field model is presented in Fig. 1. The field model consists of the grid points, starting point and the destination point.

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. In this grid-based field model along the

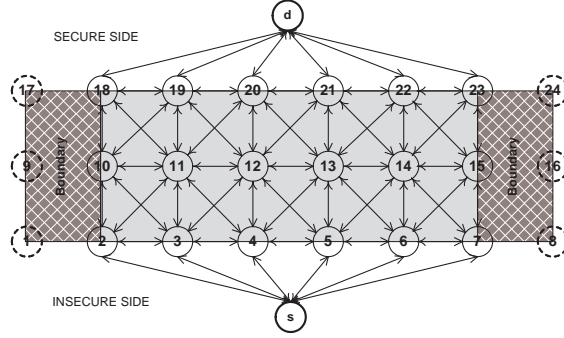


Figure 1: A sample field model constructed to find the breach path for the length is 5 m., width is 2 m., boundary is 1 m., and the grid size is 1 m. ($N = 8, M = 3$).

y-axis, we add boundary regions to the two sides of the field. Thus, there are NM grid points plus the starting and destination points. In order to simplify the notation, instead of using two dimensional grid point indices (x_v, y_v) where $x_v = 0, 1, \dots, N - 1$ and $y_v = 0, 1, \dots, M - 1$, we utilize 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

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

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 the condition that $v = w$. The first condition of the partial function of connection matrix \mathbf{C} states that each grid point (excluding 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.

2.1 Neyman-Pearson Detection Model

Using the field model described above, the detection probabilities are to be computed for each grid point to find the breach probability. 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 [4]. Two hypotheses that represent the presence and absence of a target are set up. The Neyman-Pearson (NP) detector computes the likelihood ratio of the respective probability density functions, and compares it against a threshold which is designed such that a specified false alarm constraint is satisfied. Note that NPDM is also used in [11], which introduces the co-grid method and follows a different context than the breach path problem. However, NPDM is not combined with the path-loss model unlike what follows here, and parametric links with detection performance are not established in [11].

Suppose that signal reception takes place in the presence of additive white Gaussian noise (AWGN) with zero mean and variance $N_0/2$, as well as path-loss with propagation exponent η . Each breach decision is based on the processing of L data samples. Suppose further that the data are collected fast enough so that the sensor-to-target distance remains about constant throughout the observation epoch. Then, given the NP detection model with false alarm rate α , the detection probability of a target at grid point v by sensor i is

$$p_{vi} = 1 - \Phi\left(\Phi^{-1}(1 - \alpha) - \sqrt{\gamma L} d_{vi}^{-\eta}\right) \quad (2)$$

where $\Phi(x)$ is the cumulative distribution function of the zero-mean, unit-variance Gaussian random variable at point x , and d_{vi} is the Euclidean distance between the grid point v and sensor node i [4, 7]. Note that

$$\gamma = \frac{2A\psi}{N_0} \quad (3)$$

controls the signal-to-noise ratio, where the sensor node transmits with power ψ , and A accounts for factors such as the antenna gains and the transmission frequency. Using NPDM, the detection probability p_v at any grid point v is defined as

$$p_v = 1 - \prod_{i=1}^R (1 - p_{vi}) \quad (4)$$

where R is the number of sensor nodes deployed in the field and p_{vi} is as defined in Eq. 2. The miss probabilities of the starting and destination points are one, that is $p_0 = 1$ and $p_{NM+1} = 1$. More clearly, these points are not monitored because they are not in the sensing coverage area. The boundary

regions are not taken into consideration because we want the breach path pass through the field, not through the boundaries.

The weakest breach path problem can now be defined as finding the permutation of a subset of grid points $V = [v_0, v_1, \dots, v_k]$ 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 , $j = 0, 1, \dots, k$, 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

$$P = \prod_{\forall v_j \in V} (1 - p_{v_j}) \quad (5)$$

where p_{v_j} is the detection probability associated with the grid point $v_j \in V$. A sample sensing coverage and breach path is shown in Fig. 2. Using the two-dimensional field model and adding the detection probability as the third axis, we obtain hills and valleys of detection probabilities. 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 smallest detection probabilities.

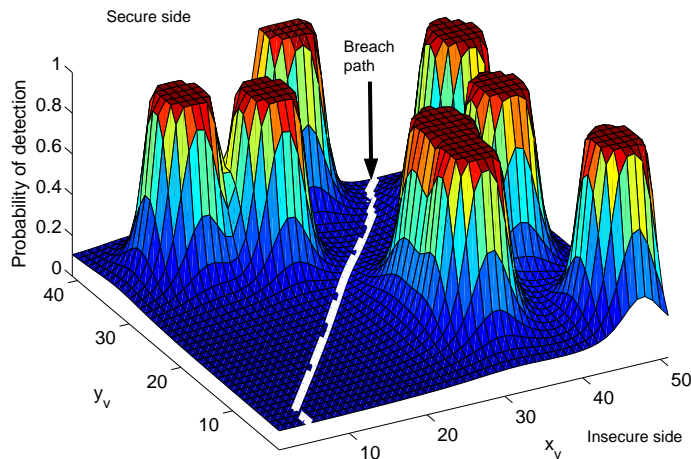


Figure 2: A sample sensing coverage and breach path where the field is 40×40 m., the boundary is 5 m. wide and the grid size is 1 m. ($N = 51$, $M = 41$, $L = 100$, $R = 9$, $\alpha = 0.01$, $\eta = 2$, $\gamma = 20$ dB.) The breach probability is 0.0031.

In order to solve the weakest breach path problem, *Dijkstra's shortest path algorithm* [10] can be used. The detection probabilities associated with the grid points cannot be directly used as weights of the grid points. Consequently, the detection probabilities of the grid points must be transformed to

Table 1: Parameter values used in the simulations for the LCFA and HFCA scenarios.

Parameter	LCFA	HCFA
Length	20 m.	100 m.
Width	5 m.	10 m.
Boundary	5 m.	10 m.
Grid size	1 m.	1 m.
N	31	121
M	6	11
α	1×10^{-2}	1×10^{-3}
η	2	3
γ	20 dB	20 dB
L	100	100
R	5	50

a new measure d_v . Since the logarithm is a monotonically increasing function, we assign the negative logarithms of the miss probabilities, defined as

$$d_v = -\log(1 - p_v) \quad (6)$$

as weights of the grid points. This algorithm finds the path with the smallest negative logarithm value that turns out to be the largest breach probability. A similar application of Dijkstra's algorithm can be found in [6] for a network with decision fusion, where the sensor detection is not NP-optimal.

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

$$P = 10^{-d_{NM+1}}. \quad (7)$$

The found path, V can be used to calculate the breach probability as in Eq. 5 that is equal to the breach probability value defined in Eq. 7.

In the next section, the effects of the NPDM parameters on the breach probability are investigated. Furthermore, we analyze the effect of the field shape on the breach probability and provide a method to find the required number of sensor nodes.

3 Breach Probability Analysis

In this paper, two SWSN scenarios are considered.

- 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.
- High-Cost False Alarm (HCFA): In this class of applications, the financial and personnel cost of a false alarm is significantly higher compared to LCFA. For example, the perimeter security of some mission-critical place such as an embassy or nuclear reactor is to be provided using SWSN to monitor unauthorized access. The cost of a false alarm might involve the transportation of special forces and/or personnel of related government agencies to the embassy/museum, as well as, the evacuation of residents in the surrounding area, which has an higher impact compared to LCFA.

Considering the impact of false alarms in these scenarios, the false alarm rate in NPDM is taken 1×10^{-3} and 1×10^{-2} for HCFA and LCFA, respectively. The other parameter values are listed in Table 2.1. 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. These models can be considered as the building blocks that may be used to cover larger fields.

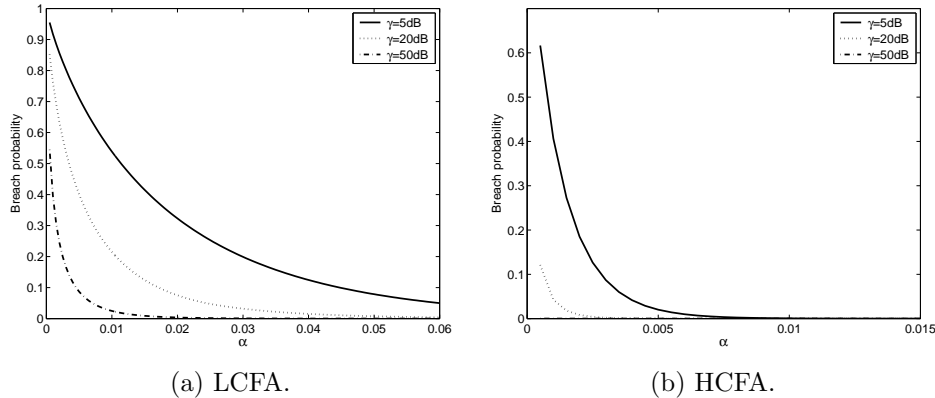


Figure 3: The effect of α on the breach probability.

3.1 Effects of Parameters on the Breach Probability

The false alarm rate α has a significant effect on the breach probability P . As shown in Fig. 3.a for the LCFA scenario and in Fig. 3.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

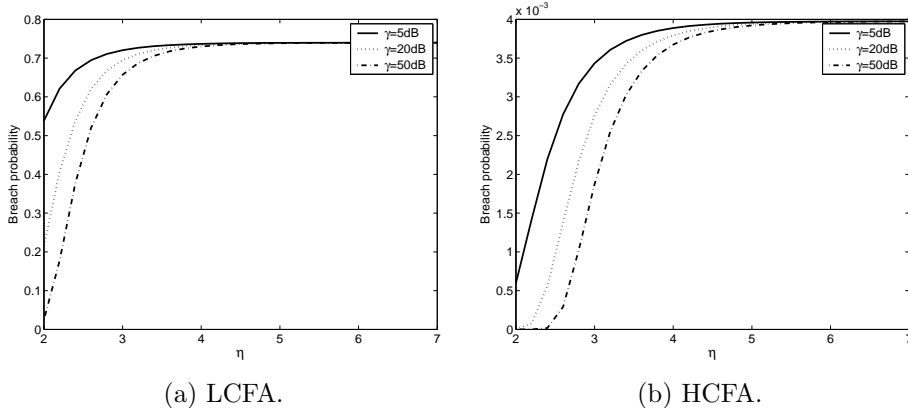


Figure 4: The effect of η on the breach probability.

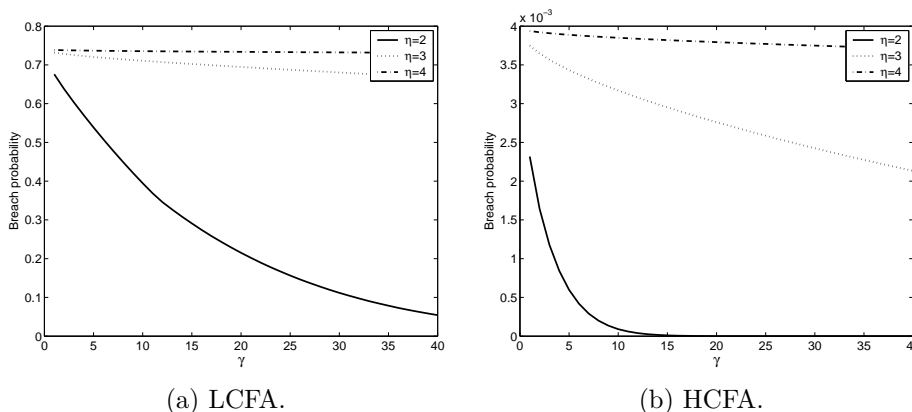


Figure 5: The effect of γ on the breach probability.

α detection model. Consequently, the breach probability decreases. However, note the fact that

$$\lim_{d_{vi} \rightarrow \infty} p_{vi} = \alpha. \quad (8)$$

where p_{vi} is as defined in Eq. 2. Thus, large α values will mislead to seemingly excellent detection performance.

Although α is very influential on breach probability, η does not have an appreciable impact when the SNR is small. For larger γ values, η significantly increases the breach probability as shown in Figures 4.a and 4.b This is due to the fact that the detection probability of NPDM is inversely proportional to the distance on the order of η . For LCFA or HCFA, the effect of η is significant when $\eta \leq 4$.

As the signal-to-noise ratio γ increases, the detection performance of NPDM improves (see Fig. 5.a for the LCFA and Fig. 5.b for the HCFA

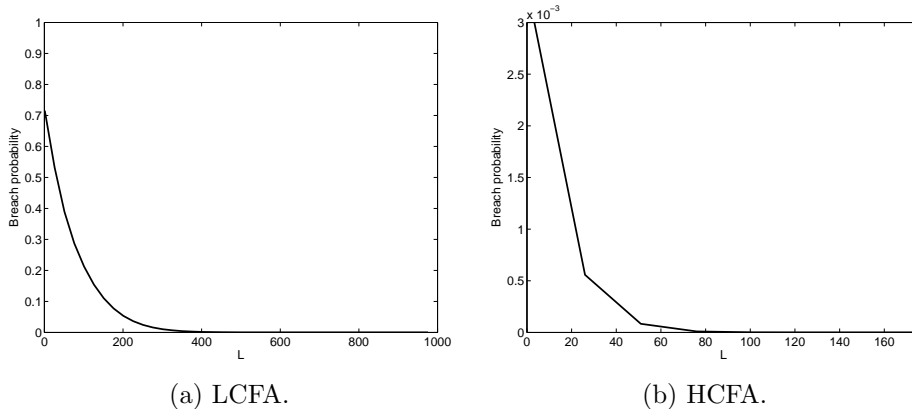


Figure 6: The effect of L on the breach probability.

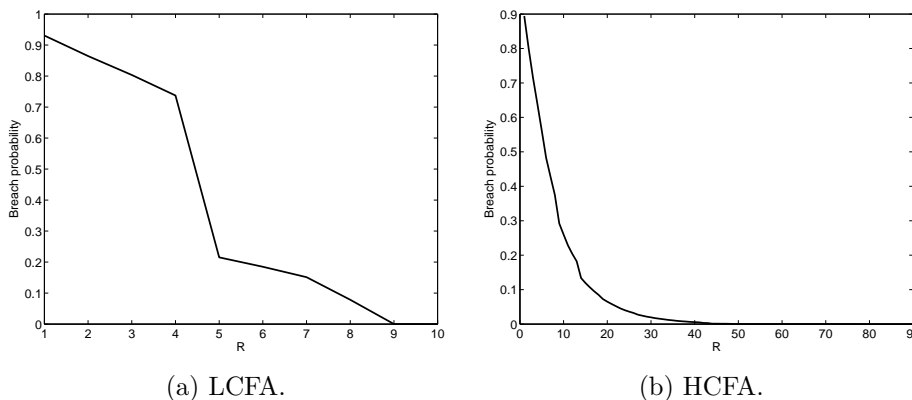


Figure 7: The effect of the number of sensor nodes on the breach probability where $y_v \sim \text{Uniform}(0, M - 1)$.

scenario), and the breach probability decreases. For closer targets, SNR has more influence on the detection probability of NPDM compared to the distant ones. Thus, the density of the network varies the SNR effect significantly. For dense fields, higher SNR decreases breach probability more.

Finally, Fig. 6.b depicts that a data record of 100 samples per breach decision is sufficient for good sensing performance for HCFA. However, for larger values of α , more samples per breach decision are required to be taken as depicted in Fig. 6.b. Despite the performance requirements, for active sensors, restrictions on energy consumption may prohibit collecting too many samples.

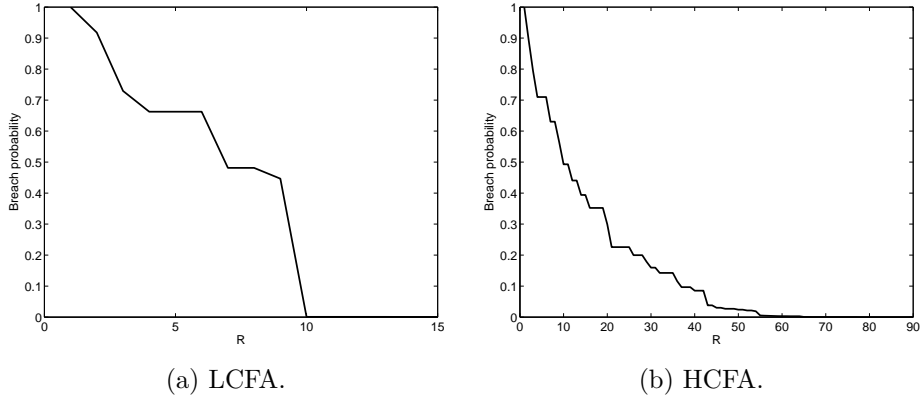


Figure 8: The effect of the number of sensor nodes on the breach probability $y_v \sim \text{Normal}(M/2, N/10)$.

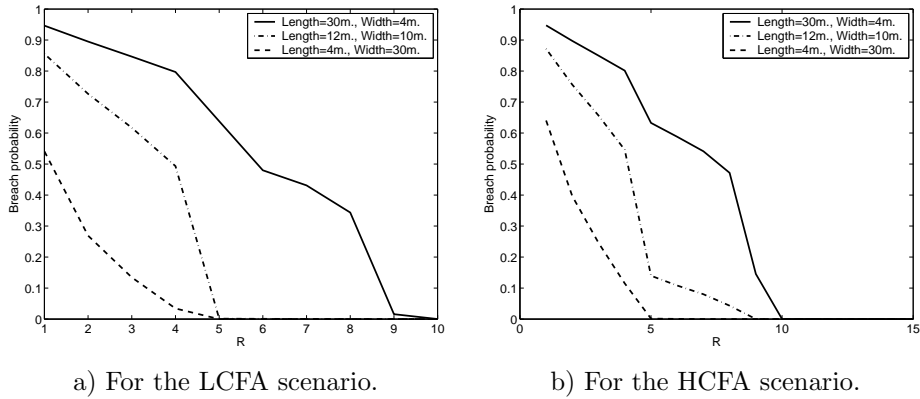


Figure 9: The effect of the field shape on breach probability where $y_v \sim \text{Uniform}(0, M - 1)$.

3.2 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 standard deviation of 10% 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 Fig. 7.a for LCFA and in Fig. 7.b for HCFA. Analyzing these figures, it can be concluded that

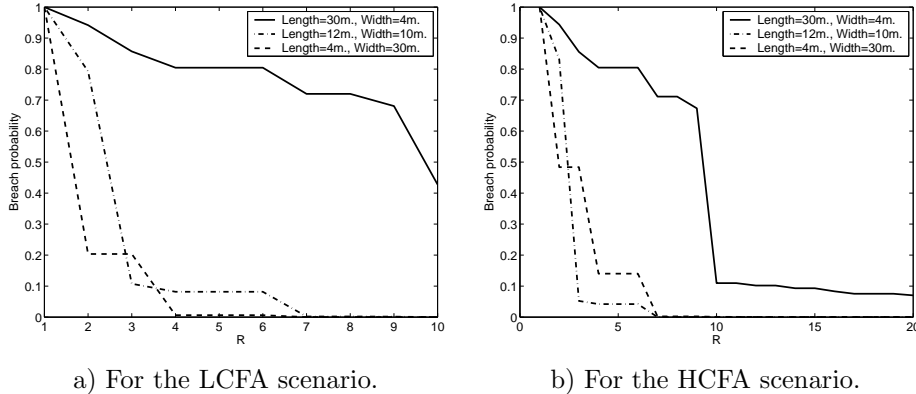


Figure 10: The effect of the field shape on breach probability where $y_v \sim \text{Normal}(M/2, N/10)$.

a breach probability of 0.01 can be obtained by utilizing 9 sensor nodes for LCFA and 51 sensor nodes for HCFA. If we take the LCFA scenario and change only $\alpha = 1 \times 10^{-3}$ and $\eta = 3$, the requirement becomes 41 sensor nodes. Whereas, if we take the HCFA scenario and set $\alpha = 1 \times 10^{-2}$ and $\eta = 2$, the requirement becomes 13 sensor nodes. Since both scenarios assume the same SNR and α affects the breach probability more than η (see Fig. 3 and 4), the false alarm rate α is more influential here. The rapid decrease in the breach probability around 4 sensor nodes in Fig. 7.a can be justified by the fact that most of the grid points are covered with high detection probabilities (saturated) around that many sensor nodes. Consequently, an additional sensor node decreases the breach probability considerably; however, once the saturation is reached, the decrease is not so large anymore.

Analyzing Fig. 8, the effect of saturation is seen more clearly for the normally distributed y-axis scheme. For this deployment scheme, since the sensor node may fall outside the field, the breach probability decreases slower compared to the uniformly distributed y-axis scheme. Thus, the required number of sensor nodes for a given breach probability level is larger.

3.3 Effect of Field Shape on the Breach Probability

Depending on the application, the field shape of the grid model may vary. Thus, the effect of the field shape on the breach probability will provide useful insights for designing better applications. In Figures 9 and 10, the effect of the field shape on 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

Table 2: 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	25	42
30	4	10	10
24	5	9	10
20	6	9	9
15	8	8	9
12	10	5	9
10	12	5	9
8	15	5	8
6	20	5	6
5	24	5	5
4	30	5	5
3	40	4	5

compared to the thicker and short fields. For example, with six sensor nodes, it is possible to provide a breach probability below 0.01 for a field where the length is 4 m. and the width is 30 m. However, with the same number of sensor nodes the breach probability turns out to be around 0.48 for the field where the length is 30 m. and width is 4 m.

In Tables 2 and 3, different grid sizes are simulated for LCFA and HCFA, respectively, and the required number of sensor nodes are tabulated for a breach probability less than or equal to 0.01. As the size of the grid becomes shorter and thicker the required number of sensor nodes decreases. For the HCFA scenario where $\alpha = 1 \times 10^{-3}$, as the field gets shorter and thicker, the difference between the required number of sensor nodes for the uniformly and normally distributed y_v schemes increases. However, the largest difference is obtained for the fields where the width is smallest. The normally distributed y_v scheme is more effective on 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. For square-like fields, uniformly distributed y_v scheme does not have a significant impact on the number of sensor nodes.

Table 3: 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	35	37
30	4	20	35
24	5	20	20
20	6	10	10
15	8	10	9
12	10	7	7
10	12	3	3
8	15	3	3
6	20	3	3
5	24	7	7
4	30	4	7
3	40	4	7

4 Conclusions

In this paper, we employ the Neyman-Pearson detection model to find the sensing coverage area of the surveillance wireless sensor networks. In order to find the breach path, we apply Dijkstra’s shortest path algorithm by using the negative log of the miss probabilities as the grid point weights. Two scenarios are studied: the low and high cost false alarm scenarios where the former tolerates false alarms more than the latter. By defining the breach probability as the miss probability of the weakest breach path, it can be concluded that the false alarm rate is the most influential parameter on the breach probability, as well as, the required number of sensor nodes for a given breach probability level. For values smaller than 4, the propagation exponent is also effective, while the SNR is an important parameter for close targets. On analyzing the effect of 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 paper 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. Similar qualitative and/or quantitative inferences about the relationships between various other parameters can also be made.

Wireless sensor networks are prone to failures. Furthermore, the sensor nodes die due to their limited energy resources. Therefore, the failures of sensor nodes must be modelled and incorporated into the breach path calculations. As a future work, we will be modelling the failures and simulating the reliability of the network throughout the entire life of the wireless sensor network. Furthermore, especially for the perimeter surveillance applications, the obstacles in the environment plays a critical role in terms of sensing and must be incorporated in the field model.

References

- [1] T. Clouqueur, 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, August 2003.
- [2] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan and L. Gu, "Energy-efficient surveillance system using wireless sensor networks," *The Second International Conference on Mobile Systems, Applications, and Services*, Boston, USA, June 2004.
- [3] A. Howard, M. J. Mataric and G. S. Sukhatme, "An incremental self-deployment algorithm for mobile sensor networks," *Autonomous Robots*, Vol. 13, No. 2, pp. 113-126, September 2002.
- [4] D. Kazakos and P. Papantoni-Kazakos, *Detection and Estimation*, New York, USA: Computer Science Press, 1990.
- [5] S. Megerian, 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, September 2002.
- [6] V. Phipatanasuphorn and P. Ramanathan, "Vulnerability of sensor networks to unauthorized traversal and monitoring", *IEEE Transactions on Computers*, Vol. 53, No. 3, pp. 364-369, March 2004.
- [7] T. S. Rappaport, *Wireless Communications: Theory and Practice*, Upper Saddle River, USA: Prentice-Hall, 1996.
- [8] D. Tian and N. D. Georganas, "A coverage-preserving node scheduling scheme for large wireless sensor networks," *Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications*, Atlanta, USA, September 2002, pp. 32-41.

- [9] S. Tilak, N. B. Abu-Ghazaleh and W. Heinzelman, "Infrastructure trade-offs for sensor networks," *Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications*, Atlanta, USA, September 2002, pp. 49-58.
- [10] M. A. Weiss, *Data Structures and Algorithm Analysis in C++*, 2nd Edition, Addison-Wesley, 1999.
- [11] G. Xing, C. Lu, R. Pless and J. A. O'Sullivan, "Co-grid: an efficient coverage maintenance protocol for distributed sensor networks," *The 3rd International Symposium on Information Processing in Sensor Networks*, Berkeley, USA, April 2004.
- [12] F. Ye, G. Zhong, S. Lu and L. Zhang, "Peas: A robust energy conserving protocol for long-lived sensor networks," *Proceedings of the 23rd International Conference on Distributed Computing Systems*, Providence, USA, May 2003, pp. 28-37.
- [13] H. Zhang and C.-J. Hou, "On deriving the upper bound of α -lifetime for large sensor networks," *Technical Report UIUCDCS-R-2004-2410*, University of Illinois at Urbana-Champaign, Department of Computer Science, February 2004.
- [14] Y. Zou and K. Chakrabarty, "Sensor deployment and target localization based on virtual forces," *Proceedings of the IEEE INFOCOM*, San Francisco, USA, April 2003, pp. 1293-1303.