

Quality of Deployment in Surveillance Wireless Sensor Networks

Ertan Onur,¹ Cem Ersoy,¹ and Hakan Deliç²

When wireless sensors are used to keep an area under surveillance, a critical issue is the quality of the deployment from the sensing coverage viewpoint. In this paper, we propose several quality measures, which indicate if the deployment provides sufficient coverage, or whether redeployment is required or not. The terrain is modeled as a grid and the placement of the sensors is uniformly distributed. Neyman–Pearson detection is utilized to determine the effects of false-alarm and signal characteristics on the measures.

KEY WORDS: Surveillance; wireless sensor networks; deployment quality.

1. INTRODUCTION

When analyzing the service quality of a wireless sensor network (WSN), 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. A commonly employed model assumes binary detection, where the target is detected if it is closer than a threshold distance, and it goes unnoticed otherwise [1, 2]. In contrast, Neyman–Pearson detection (NPD) [3, 4] and Elfes’s model [5] have the detection probabilities as a function of the sensor-to-target distance. In this paper, we utilize Neyman–Pearson detector, which maximizes the detection probability under the constraint of a prespecified false alarm requirement, which is a significant issue in WSNs [6].

The positions of the sensors influence the sensing coverage [7, 8]. 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 [4] and [9], respectively.

Obstacles in the field have a significant impact on the sensing performance. In [10], 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 [7].

In this paper, we analyze the quality of deployment in surveillance WSNs. To that end, the field and sensor models are outlined in the next section. Various deployment quality measures are introduced in Section 3. Along with the maximum detection probability on the weakest breach path defined in [4], we propose three measures to analyze the poorly detected areas. Numerical comparisons are presented in Section 4. Finally, conclusions are drawn in Section 5.

2. THE FIELD AND SENSOR MODELS

The field is modeled as an $N \times M$ grid and two auxiliary nodes are added to represent the start and the destination nodes. The aim of the target is to

¹ NETLAB, Department of Computer Engineering, Boğaziçi University, Bebek 34342, Istanbul, Turkey. E-mail: onur@boun.edu.tr

² Wireless Communications Laboratory, Department of Electrical and Electronics Engineering, Boğaziçi University, Bebek 34342, Istanbul, Turkey.

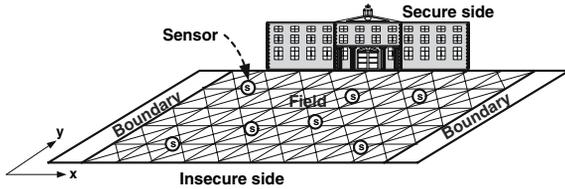


Fig. 1. A sample field model.

breach through the field from the start node which lies in the insecure side to the destination node at the secure side. Each grid point (excluding start and destination nodes) is connected to the other grid points which are either one-hop away or cross-diagonal. The start node is connected to all of the initial horizontal grid points of the field. All of the final horizontal grid points are connected to the destination node. Otherwise, the two grid points are not connected. The field model is enlarged with the boundary regions on both the left and the right sides because if the sensor is deployed close to these sides, truncation will mislead the results. A sample field model is shown in Figure 1.

The decision rule that maximizes the detection probability subject to a maximum allowable false alarm rate α is given through Neyman–Pearson optimization [3]. Two hypotheses that represent the presence and absence of a target are formed, and the likelihood ratio of the respective probability density functions are computed and compared against a threshold which is set so 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 exponent η . Each breach decision is made after processing a snapshot of L data samples. Suppose that the sensor-to-target distance remains about constant throughout the snapshot. Then, given the Neyman–Pearson detector with false alarm rate α , the detection probability of a target at grid point (i, j) by sensor k is

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

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

$$\gamma = \frac{A\psi}{\sigma_n^2} \quad (2)$$

controls the signal-to-noise ratio (SNR), where the signal is emitted from the target with power ψ , and A

accounts for factors such as the transmission frequency and propagation losses.

The self-organizing nature of the WSNs eases the deployment process. Depending on the deployment style, the coordinates of the sensor 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. 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 sensors. These problems require three-dimensional field models and analysis of non-uniform deployment. In this paper, the coordinates of the sensor positions are assumed to be drawn from independent uniform distributions so that there is no bias in any direction.

The sensor observations are generally correlated because the same grid point might be monitored by multiple sensors. Therefore, the network's probability of detection of a target on grid point (i, j) , which is denoted by p_{ij} , is equivalent to the detection probability of the closest sensor to that grid point [9]. Then,

$$p_{ij} = \max_{k=1,2,\dots,R} p_{ijk},$$

where $i=1,2,\dots,N$, $j=1,2,\dots,M$ and R is the total number of sensors deployed in the field.

3. DEPLOYMENT QUALITY MEASURES

In this paper, we study the quality of deployment in surveillance WSNs in terms of the security provided. Several deployment quality measures are introduced and evaluated within the next sections.

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. Suppose that the WSN detection performance on point (i, j) is sufficiently reliable only at those distances for which $p_{ij} > p_t$, 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 of the field be represented by the indicator n_{ij} ,

$$n_{ij} = \begin{cases} 1 & \text{if } p_{ij} < p_t, \\ 0 & \text{otherwise,} \end{cases} \quad (3)$$

which represents inadequately monitored grid points with unity value. Then, the deployment quality measure Q_{PD} is defined as,

$$Q_{PD} = \frac{\sum_{i,j} n_{ij}}{NM}, \quad (4)$$

where the numerator counts the poorly detected grids and NM is the total number of grid points in the field. 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.

3.2. Redeployment Measure

Depending on the application, redeployment scenarios are probable. After representing the field according to Eq. 3, we obtain a binary image on which image processing techniques such as connected component labeling can be applied.

For a grid point (x, y) that resembles a pixel in an image, the *4-connected neighborhood* is defined as the set of grid points $N_4(x, y) = \{(x+1, y), (x-1, y), (x, y+1), (x, y-1)\}$ and the *8-connected neighborhood* is the set of grid points $N_8(x, y) = N_4(x, y) \cup \{(x+1, y+1), (x-1, y-1), (x-1, y+1), (x+1, y-1)\}$. 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 $(x_2, y_2) \in N_8(x_1, y_1)$. Furthermore, (x_1, y_1) and (x_2, y_2) are assumed to be connected if there is a path of grid points from (x_1, y_1) to (x_2, y_2) 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. Further information about the connected component labeling can be found in [11].

Suppose that we have the grid labels $\ell_{ij} \in \mathbb{Z}$, where $\ell_{ij} = 0$ denotes the background of the image and $\ell_{ij} > 0$ are the label values. After applying the connected component labeling algorithm on the binary image, 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

$$Q_{RD} = \frac{\sum_{(i,j): \ell_{ij} \in L} n_{ij}}{NM}. \quad (5)$$

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. 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 ℓ_{ij} matrix can be used. If any two of the nodes 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} .

3.4. Breach Detection Probability

The weakest breach path can be defined as the permutation of a subset of grid points $V = [s, (i_0, j_0), (i_1, j_1), \dots, (i_k, j_k), d]$ 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. Here, we can define the miss probability of a target as

$$p_m = \prod_{(i,j) \in V} (1 - p_{ij}), \quad (6)$$

where p_{ij} is the detection probability associated with the grid point $(i, j) \in V$. To determine the weakest breach path, we propose the application of Dijkstra's algorithm defined in [4].

The deployment quality measure called the breach detection probability on the weakest breach path, P_{BD} , can be defined as

$$P_{BD} = \max_{(i,j) \in V} p_{ij}. \quad (7)$$

The P_{BD} 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.

4. ANALYSIS OF DEPLOYMENT QUALITY MEASURES

In this paper, the SWSN scenario described by the parameter values listed in Table I is investigated. The simulation results shown in the following tables are the averages of 100 distinct deployment runs. These models can be considered as the building blocks that may be used to cover larger fields.

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 II), 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.

Table I. Parameter Values in the Simulations

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

Table II. 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

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 III. The number of grid points having $p_{ij} < p_t$ 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 SNR γ produces better P_{BD} and smaller component areas. However, γ does not impact the deployment quality measures as much as η does (see Table IV).

4.2. Reliability Threshold and Deployment Density

In Table V, 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,

Table III. 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

Table IV. 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 V. The Effect of p_t on the Deployment Quality Measures

p_t	Q_{RD} (%)	Q_{PD} (%)	Q_{CS} (%)
0.75	1.40	7.65	2
0.80	1.73	9.50	6
0.85	2.22	11.84	13
0.90	2.74	14.49	25
0.95	3.30	18.93	50

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.

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 $p_{ij} < p_t$ increases (see Table VI). 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_{ij} probabilities. Thus, the quality of deployment improves as seen in Table VII. 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

Table VI. 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 VII. 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

than P_{BD} take smaller values. Obstacles are not modeled 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.

When more sensors are deployed, since p_{ij} increases, fewer grid points have $p_{ij} < p_t$, 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.

4.3. Discrete Event Simulation

In order to validate the miss 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 1×10^4 times and the ratio of the number of detections to 1×10^4 represent the miss rate, r_m .

The parameter values in the simulations are as in Table I. For different number of sensors, the miss probability associated with the weakest breach path is compared with the simulation results in Table VIII. The discrete event simulations are in agreement with earlier results.

Table VIII. Verification of the Miss Probability Through Discrete Event Simulations

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

5. CONCLUSION

In this paper, we took a probabilistic approach to analyze the quality of deployment in surveillance WSNs. The sensors are assumed to follow the Neyman–Pearson optimization. Several deployment quality measures are proposed and the effect of the sensor model parameters, width of the field, and the number of sensors are analyzed.

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. As a future work, the cost of the sensors and the deployment can be incorporated in the design and the trade-offs can be analyzed.

ACKNOWLEDGMENTS

This work was 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. A preliminary version of this work was presented in part at the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Barcelona, Spain, September 2004, and also in the 8th International Conference on Telecommunications, Zangreb, Croatia, June 2005.

REFERENCES

1. Z. Abrams, A. Goel and S. Plotkin, Set k-cover algorithms for energy efficient monitoring in wireless sensor networks, *Proceedings of the Third International Symposium on Information Processing in Sensor Networks*, Berkeley, USA, pp. 424–432, April 2004.
2. N. Heo and P. K. Varshney, A distributed self spreading algorithm for mobile wireless sensor networks, *Proceedings of the IEEE Wireless Communications and Networking Conference*, Vol. 3, pp. 1597–1602, March 2003.
3. D. Kazakos and P. Papantoni-Kazakos, *Detection and Estimation*, Computer Science Press, New York, USA, 1990.
4. E. Onur, C. Ersoy, and H. Deliç, Sensing coverage and breach paths in surveillance wireless sensor networks, *Sensor Network Operations*, S. Phoha, T. F. La Porta, and C. Griffin, eds., IEEE Press, 2005.
5. A. Elfes, Occupancy grids: a stochastic spatial representation for active robot perception, *Autonomous Mobile Robots: Perception, Mapping and Navigation*, Vol. 1, S. S. Iyengar and A. Elfes, ed., IEEE Computer Society Press, pp. 60–70, 1991.
6. 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, *Proceedings of the Second International Conference on Mobile Systems, Applications and Services*, Boston, USA, pp. 270–283, June 2004.
7. 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.
8. Y. Zou and K. Chakrabarty, Sensor deployment and target localization based on virtual forces, *Proceedings of the IEEE INFOCOM*, San Francisco, USA, pp. 1293–1303, March 2003.
9. E. Onur, C. Ersoy, and H. Deliç, How many sensors for an acceptable breach detection probability? *Computer Communications* in press, 2005.
10. S. Ganeriwal, 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*, New Orleans, USA, April 2004.
11. R. M. Haralick and L. G. Shapiro, *Computer and Robot Vision*, Vol. I Addison-Wesley, Boston USA, 1992 pp. 28–48.



Ertan Onur was born in Izmir, Turkey, on February 21, 1975. He received the B.S. degree in computer engineering from Ege University, Izmir, Turkey in July 1997 and the M.S. degree in computer engineering from Bogazici University, Istanbul, Turkey in June 2001. Currently he is enrolled as a PhD student at computer engineering department of Bogazici University. After finishing his B.S. degree, he worked for LMS Durability Technologies GmbH, Kaiserslautern, Germany. During the M.S. degree he worked in Turkcell Project at Bogazici University and for Global Bilgi, Turkcell as a project leader. Currently, he is working for Argela Technologies as an R&D engineer. Mr. Onur's research interests are in the area of telecommunications, analysis and design of computer networks. Mr. Onur is a student member of IEEE and Netlab at Bogazici University.



Cem Ersoy received his BS and MS degrees in electrical engineering from Bogazici University, Istanbul, in 1984 and 1986, respectively. He worked as an R&D engineer in NETAS A.S. between 1984 and 1986. He received his PhD in electrical engineering from Polytechnic University, Brooklyn, New York in 1992. Currently, he is a professor and department head in the Computer Engineering Department of Bogazici University. His research interests include performance evaluation and topological design of communication networks, wireless communications and mobile applications. Dr. Ersoy is a Senior Member of IEEE.



Hakan Deliç received the B.S. degree (with honors) in electrical and electronics engineering from Bogazici University, İstanbul, Turkey, in 1988, and the M.S. and the Ph.D. degrees in electrical engineering from the University of Virginia, Charlottesville, in 1990 and 1992, respectively. He was a Research Associate with the University of Virginia Health Sciences Center from 1992 to 1994. In September 1994, he joined the University of Southwestern Louisiana, Lafayette, where he was on the Faculty of the Department of Electrical and Computer Engineering until February 1996. He was a Visiting Associate Professor in the Department of Electrical and Computer Engineering, University of Minnesota, Minneapolis, during the 2001–2002 academic year. He is currently a professor of electrical and electronics engineering at Bogazici University. His research interests lie in the areas of communications and signal processing. His current research focuses on wireless multiple access, application of signal processing techniques to wireless networking, ultra-wideband communications, iterative decoding, robust systems, and sensor networks. He frequently serves as a consultant to the telecommunications industry. Dr. Deliç is Senior Member of IEEE.