Surveillance Wireless Sensor Networks: Deployment Quality Analysis

Ertan Onur[1], Cem Ersoy[1], Hakan Deliç[2], and Lale Akarun[3]
[1]Computer Networks Research Laboratory
[3]Perceptual Intelligence Laboratory
Department of Computer Engineering
Boğaziçi University
Bebek 34342 Istanbul, Turkey
E-mail: {onur,ersoy,akarun}@boun.edu.tr
[2]Wireless Communications Laboratory
Department of Electrical and Electronics Engineering
Boğaziçi University
Bebek 34342 Istanbul, Turkey
E-mail: delic@boun.edu.tr

Abstract

Surveillance wireless sensor networks (SWSNs) are deployed at perimeter or 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 can be employed that reveal the weaknesses in the coverage of SWSNs with respect to the success ratio and time for detecting intruders. In this paper, probabilistic sensor models are adopted, and the quality of deployment issue is surveyed and analyzed in terms of novel measures. Furthermore, since the presence of obstacles in the surveillance terrain has a negative impact on previously proposed deployment strategies and analysis techniques, we argue in favor of utilizing image segmentation algorithms by imitating the sensing area as a gray-scale image that is

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

referred to as the iso-sensing graph. Finally, the effect of sensor count on the detection ratio and time-to-detect the target is analyzed through OMNeT++ simulation of a SWSN in a border surveillance scenario.

I. INTRODUCTION

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 data collection center. Many areas of employment are envisaged for WSNs ranging from the monitoring of endangered animals populations to military surveillance.

In this paper, 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, whose assessment we need meaningful measures for. 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 network lifetime is directly related to the energy resources of the sensors and can be extended by energy-aware protocols. The detection 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. This necessitates time-synchronization in order to meet the required accuracy in the network by increasing the probability of intrusion detection while keeping the false alarm rate at a reasonable level.

Network failure, partial or wholly, may not only be due to the power exhaustion of the

sensor nodes. A group of sensors may be intentionally destroyed, leading to area failures in a SWSN which must be studied along with the failure distribution of power-deprived sensors. An example of area failure is the effective elimination of sensor nodes through the presence of strong jamming. What must be done in terms of sensor deployment once an area failure occurs is an open research topic. Since sensor failures are common, fault tolerance of the network should be investigated because loss of individual sensors or a group of sensors should not hamper the task accomplishment of the network.

After defining several demonstrative surveillance scenarios and the typical sensor models in the following sections, a brief survey of the deployment quality is presented. Following the definitions, some surveillance wireless sensor network examples are evaluated.

II. Surveillance Scenarios

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. 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.

The detection of intrusions through a country's borders is a significant military application where interesting challenges related to WSN 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. 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. Segmentation can be carried out according to the geographical properties of the border such as topology and altitude.

Depending on the deployment style, the coordinates of the sensor positions may follow a particular distribution. For instance, if sensors are thrown off an aircraft that flies over the middle of the field, most sensors are expected to fall somewhere close to the central line and several sensors are likely to end up further out. One could then argue that the sensor distribution is uniform along the axis of flight, while it is Gaussian in the orthogonal direction as shown in Fig. 1(a). The topographical properties of the area may also affect the deployment outcome. In case of a valley, the deepest locations will collect more sensors. These problems require three-dimensional field models, and the analysis of non-uniform deployment. For plain and easily-accessible fields such as embassy/museum garden as shown in Fig. 1(b), deterministic deployment is appropriate. Through advance analysis based on good models, decisions as to where to position the sensors can provide better deployment quality.

III. Sensor Models

Different types of sensors may have to be utilized in a WSN to address the problem at hand. For outdoor intrusion detection systems such as country border surveillance, microwave, ultrasonic, infrared and/or radar sensors are typical. Because the working principle of these sensors differ, one needs a common measure such as the probability of detecting a target, p_d, to compare the performance of the sensor technologies. The factors that affect p_d are sensor-, environment- and target-related: target-to-sensor distance, propagation characteristics, the amount of energy emitted, the size and the motion pattern of the target, etc. Moreover, the false alarm rate constraint on each sensor (as well as on the SWSN itself if data/decision fusion is allowed), which limits the percentage of intrusion decisions when no target or an object that is not regarded as a target

exists, also bounds the detection performance of the network.

A. Probabilistic Sensor Models

A common approach in WSN research is to use the simple binary detection model. Here, the sensor detects a target with probability one only if the target-to-sensor distance d is below a threshold distance d_t (see Fig. 2(a)). Such a simplification where d alone determines the outcome may be acceptable for indoor deployment, especially when line-of-sight is ensured. On the other hand, the received signal quality in the uncontrollable outdoor settings depends so much on the propagation environment that more sophisticated models are required for proper design and analysis [1]. In Elfes's model, the detection probability is described such that the physical properties of the sensors are accommodated by generic model parameters [2]. If the sensor-to-target distance d is smaller than a threshold value d_t^1, then the target is absolutely detected, i.e., $p_d = 1$ (see Fig. 2(b)). When $d > d_t^2 > d_t^1$ for a second threshold d_t^2, the target cannot be detected and $p_d = 0$. On the other hand, the detection probability is an exponentially decaying function of d if the target lies in the range $d_t^1 < d < d_t^2$. The rate of decay is determined by two parameters, λ, β, that reflect that sensor characteristics. Specifically, the probability that a sensor detects a target is

$$p_d = \begin{cases} 1 & \text{if } d \leq d_t^1, \\ e^{-\lambda(d-d_t^1)^\beta} & \text{if } d_t^1 < d < d_t^2, \\ 0 & \text{if } d_t^2 \leq d, \end{cases} \tag{1}$$

where the parameters d_t^1, d_t^2, λ and β are adjusted according to the physical properties of the sensor.

Unlike the binary detection and Elfes's models, the Neyman-Pearson (NP) detector incorporates both the false alarm rate and the signal characteristics in the model. It is generally assumed that the sensors operate in the presence of additive white Gaussian noise and the signal experiences path-loss with a certain propagation exponent. 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 [1]. Two hypotheses that represent the presence and absence of a target are set up. The NP detector 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 signal reception takes place in the presence of additive white Gaussian noise and path-loss with propagation exponent η. Then, given the NP formulation with false alarm rate α, the detection probability is

$$p_d = 1 - \Phi\Big(\Phi^{-1}(1-\alpha) - \sqrt{\gamma(d)}\Big) \tag{2}$$

where $\gamma(d)$ is the signal-to-noise ratio (SNR) at the sensor when the target is at a distance d and $\Phi(x)$ is the cumulative distribution function of the zero-mean, unit-variance Gaussian random variable at point x. In Equation 2, we have the proportionality

$$\gamma(d) \sim d^{-\eta}.$$

Using standard bounds on $\Phi(x)$ [3], it is possible to write

$$p_d \approx A\left(\gamma(d), \eta, \alpha\right) \exp\left\{\Phi^{-1}(1-\alpha) - \sqrt{\gamma(d)}\right\} \tag{3}$$

where $A\left(\gamma(d), \eta, \alpha\right)$ is a constant that is indicative of the SNR level. Comparing (1) to (3), where both detection probabilities exhibit an exponential behavior, one can readily see that Elfes's model can accommodate the Neyman-Pearson detector through proper parameter matching.

B. Exposure Based Sensor Models

As an alternative to using detection probability as a performance measure, the received energy level also gives an intuition about observability. The expected observability of a target in a field is referred to as exposure [4]. For example, the total amount of energy received by the sensors along all the points on the breach path is defined as the path exposure. Let $S_i(d)$ be the signal energy of the target measured by the ith sensor at a distance d. A simple exposure based sensor model is

$$S_i(d) = \frac{K}{d^k}$$

where the nonnegative constant $k, 2 < k < 5$, is the decay factor of the energy emitted by the target, K [5]. A multiplicative constant between zero and one can be incorporated to model the effect of obstacles on the emitted energy. While designing a WSN application, the main question about the exposure is the fusion of the exposure levels when different types of sensors are utilized. A general metric such as the detection probability may be more valuable when various sensors collaborate.

C. A Sensor Example: Micropower impulse radar (MIR)

One state-of-the-art in radar-based sensors is the micropower impulse radar (MIR) invented in 1993 [6]. MIR is a low-power system that uses ultra-wideband (UWB) pulses and works at short distances. Electromagnetic emissions are less than one milliwatt and there is no interference with other electronic devices. An MIR detector is inexpensive because it can be designed with off-the-shelf components, and it is small in size (~ 10 cm^2). Modified versions of MIR motion sensors can be used for search and rescue applications, medical diagnostics, intrusion sensing, and perimeter security. Considering all these advantages, MIR sensors are applicable to SWSNs, as well. It is possible to integrate this radar with a transceiver and a processor to build a wireless sensor node [7]. Commercial MIR devices are available that detect motion up to about 15 to 18 meters using the Doppler effect and can operate on 3.5 to 6.0 volt power sources

IV. Quality of Deployment

Once some set of sensors is deployed for, say, border surveillance, how will one be sure that the deployment provides the necessary security level? To analyze if the requirement is met, one needs a measure that represents the quality of the deployment, which is directly related to the sensing coverage of the network. The ratio of the poorly sensed area to the total area of the field 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 detection probability for that point is less than some threshold. 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. When setting up barrier coverage, random deployment may result in a well-secured region, in which a tiny breach hole may exist. To reveal such situations, one has to check if there is a path passing through the field where each point on this path is poorly sensed.

A. Deployment Quality Measures

The total energy of the signal that is emitted from the target and received by the sensors along all the points on the breach path is defined as the path exposure. The path with the least exposure

value is assumed to be the best path for the target in breach of security [4], which is also the worst case from the viewpoint of the SWSN. Designing a SWSN according to the worst case scenario is costly. It is a safe assumption to think that the target does not know sensor positions. Thus, the target will not figure out the best path for itself, and the designer may assume that it traverses the region without any predictable and systematic pattern. This intuition suggests the use of an average case measure.

When a decision about the presence/absence of a target is to be made, the individual detections 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 signal-to-noise ratio and propagation conditions. From a network viewpoint, what matters is the performance of the sensor with the best detection capability that is referred to as observability by the closest sensor [4]. Hence, summing up the exposure levels of these sensors without considering the correlations may be misleading.

Although sensing is the main functionality of a SWSN, it is useless without the ability to communicate data. The sensing and communication coverage problems are addressed separately [8]. Optimization of the sensing coverage and analysis of the deployment quality measure should be carried out in conjunction with the communication requirements. Because WSNs 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 [8]. 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 [9].

B. Iso-Sensing Graph Approach

Suppose that the surveillance field is modeled as a grid and we know the positions of all sensors. Using a relevant sensor model, 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. A sample iso-sensing graph is shown in Fig. 3. The name implies the resemblance to topographic maps where the z-axis denotes the altitude. In an iso-sensing graph higher altitudes show larger detection probabilities, and the target should prefer paths with the lowest altitudes to evade detection. To reveal those paths, image processing algorithms can be utilized by considering the iso-sensing graph as an image. One such algorithm is Watershed Segmentation [10], which is best-understood with an analogy to water flooding from the minimal points of a three-dimensional topographic surface. As the water rises, dams are built where the floods will merge. After the completion of immersion, water reaches the maximum level, and only the dams that separate the valleys are not submerged. Consequently, the topographic surface is partitioned into regions that are divided by the dams referred to as watersheds. The iso-sensing graph can be considered as a two-dimensional image where the miss probabilities are quantized to gray-scale color values. The watershed algorithm can be applied to the iso-sensing graph of a WSN in order to find the possible breach paths. After deploying the sensors in the field and determining the iso-sensing graph of the network, utilizing the miss probabilities on the grid points produces hills and valleys where the altitude is now mapped to the miss probability. The minima of this surface are the sensor node positions. Thus, analogously, it can be considered that water starts flooding from the sensor nodes. After applying the watershed algorithm, the contour points (dams) correspond to possible breach paths.

When obstacles are incorporated in the field model, a line-of-sight problem arises. That is, some parts of the field cannot be covered and sensed because of the obstruction, in which case the Voronoi segmentation approach [5] to determine the breach paths will not work. However, the iso-sensing graph definition can be extended to model the obstacles. By assuming that obstacles not only block the line-of-sight of sensors but also the traversal of any intruders, the detection probability of the grid points on which the obstacles are positioned can be assumed to be one (see Fig. 3). The watershed segmentation algorithm takes the obstacles into account, and the contours do not overlap with them.

The analytical or experimental approaches described in this section mostly present the worst case scenarios. When we assume that the target does not know the sensor locations, providing an average case security level is more cost efficient. Next, we present the simulation of a simple

border surveillance scenario which gives an intuition about the security level provided with a fixed number of sensors in the next section.

V. Evaluation of the Deployment Quality

There are several discrete event simulators that can be used to model WSNs. In this section, we present results produced with OMNeT++, which is a public-source discrete event simulation environment [11]. 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 as shown in Fig. 4. While the sensors are connected in the figure, sensor communication is not considered in the simulation, and only the physical layer sensing operation is modeled in accordance with the binary or Elfes's detector. The circles in Fig. 4 depict the sensing coverage areas.

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 2 m/s 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 Fig. 5. 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 Fig. 5(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 unnoticed becomes shorter.

Figure 5 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 $d_t^2 = 28$ meters, $d_t^1 = 8$ meters, $\lambda = 0.2$ and $\beta = 0.6$. For comparison with the binary detector, here $p_d = 0.5$ when $d = 18$ 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 surveillance application referred to as *A Line in the Sand* is presented in [12]. 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 5 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 [12] are met. Figure 5 depicts that 60 Elfes detectors are adequate to provide the required levels of the same metrics. The doubling of the number of nodes when binary detection is adopted stresses the importance of having proper sensor models for WSN deployment.

VI. Conclusion

The quality of deployment in SWSNs is considered with border surveillance taken as the target application. Suitable measures are discussed for the assessment of the deployment quality. A simple simulation environment is developed to evaluate the impact of the node density on the detection ratio and on the time-to-detect an intruder.

Deployment quality measures reveal the weaknesses in the sensor distribution of the SWSNs from the viewpoint that sensing is the main functionality of the network. Decisions regarding the necessity of incremental deployment schemes or redeployments can be made based on these measures. For further research, the breach path problems should be studied along with the relevant communication issues. The network lifetime must be linked to the quality of deployment. The topology management should incorporate the deployment quality measures by continuously monitoring the network's sensing coverage capability.

REFERENCES

[1] E. Onur, 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.

[2] A. Elfes, "Occupancy grids: A stochastic spatial representation for active robot perception," in *Autonomous Mobile Robots: Perception, Mapping, and Navigation (Vol. 1)*, S. S. Iyengar and A. Elfes, Eds. Los Alamitos, CA: IEEE Computer Society Press, 1991, pp. 60–70.

[3] S. F. Wilson, *Digital modulation and coding*. Upper Saddle River, NJ, USA: Prentice-Hall, 1996.

[4] 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, Sept. 2002.

[5] 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, Aug. 2003.

[6] T. E. McEwan, "Differential pulse radar motion sensor," U.S. Patent 5 966 090, Dec. 10, 1999.

[7] P. K. Dutta, A. K. Arora, and S. B. Bibyk, "Towards radar-enabled sensor networks," in *Proc. of the Fifth International Conference on Information Processing in Sensor Networks*, Nashville, TN, USA, Apr. 2006, pp. 467–474.

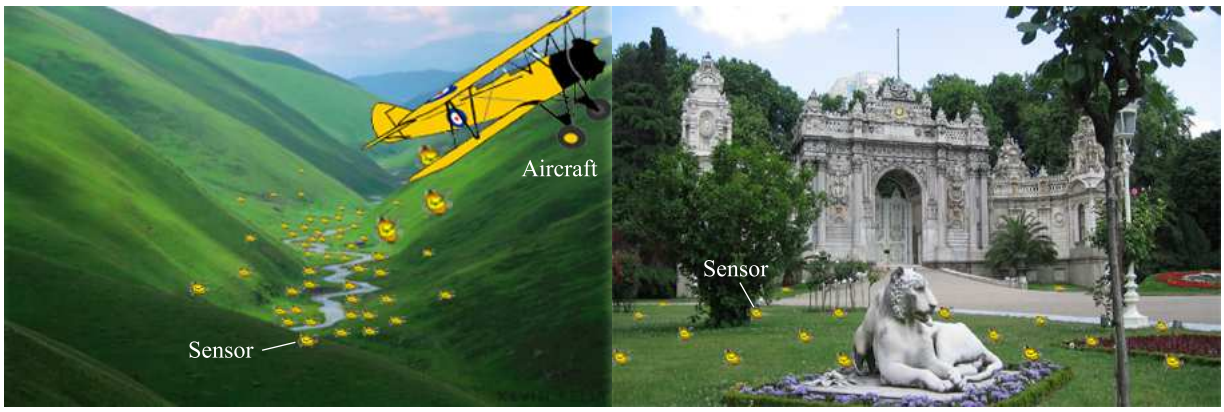
[8] G. Xing, X. Wang, Y. Zhang, C. Lu, R. Pless, and C. Gill, "Integrated coverage and connectivity configuration for energy conservation in sensor networks," *ACM Transactions on Sensor Networks*, vol. 1, no. 1, pp. 36–72, Aug. 2005.

[9] V. Ravelomanana, "Extremal properties of three-dimensional sensor networks with applications," *IEEE Transactions on Mobile Computing*, vol. 3, no. 3, pp. 246–257, July 2004.

[10] E. Onur, C. Ersoy, H. Deliç, and L. Akarun, "Coverage in sensor networks when obstacles are present," in *Proc. of the IEEE International Conference on Communications*, vol. 9, İstanbul, Turkey, June 2006, pp. 4077–4082.

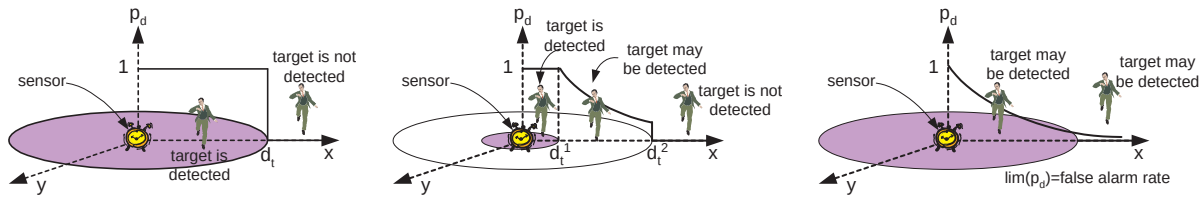
[11] A. Varga, "Software tools for networking: Omnet++," *IEEE Network Interactive*, vol. 16, no. 4, 2002.

[12] A. Arora, 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.



(a) Random deployment. (b) Uniform deployment (Dolmabahçe Palace, Istanbul).

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



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

Fig. 2. Sensor models.

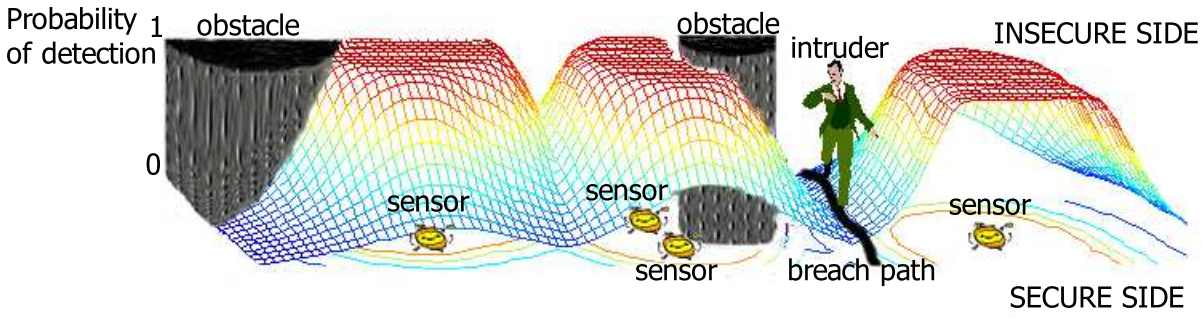


Fig. 3. In this figure, a simple surveillance scenario is depicted. An intruder is breaching from the insecure side of the region to the secure side following the weakest breach path. Four Neyman-Pearson detectors are deployed. Two circular obstacles exist in the region. The obstacles block not only the line-of-sight of the sensors but also the target movement. The z-axis shows the probability of detection. For each grid point in the region, the detectability is calculated and the iso-sensing graph is produced.

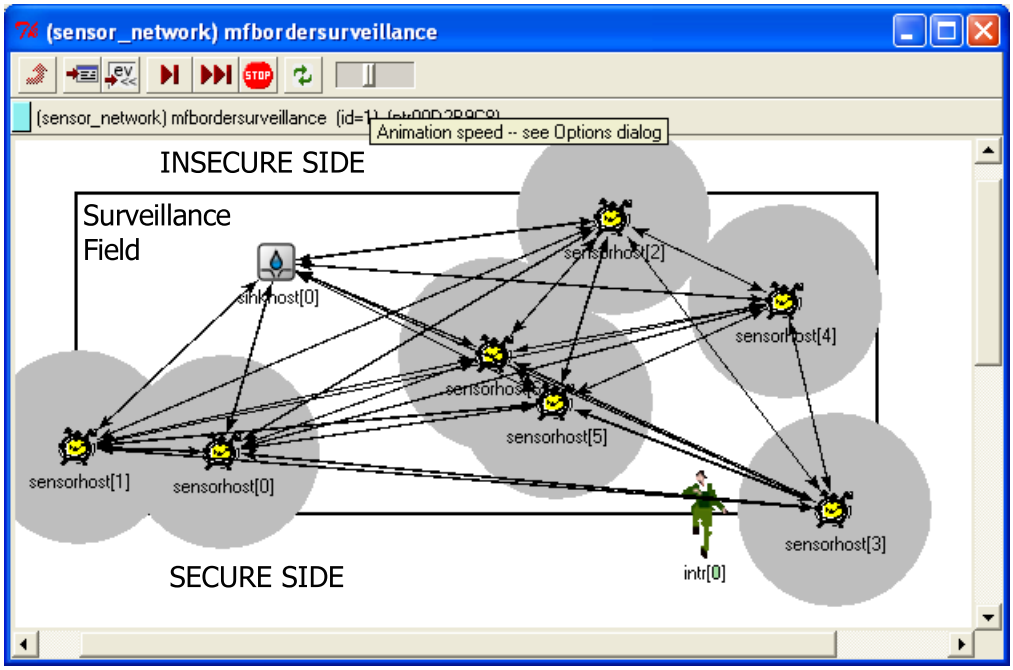
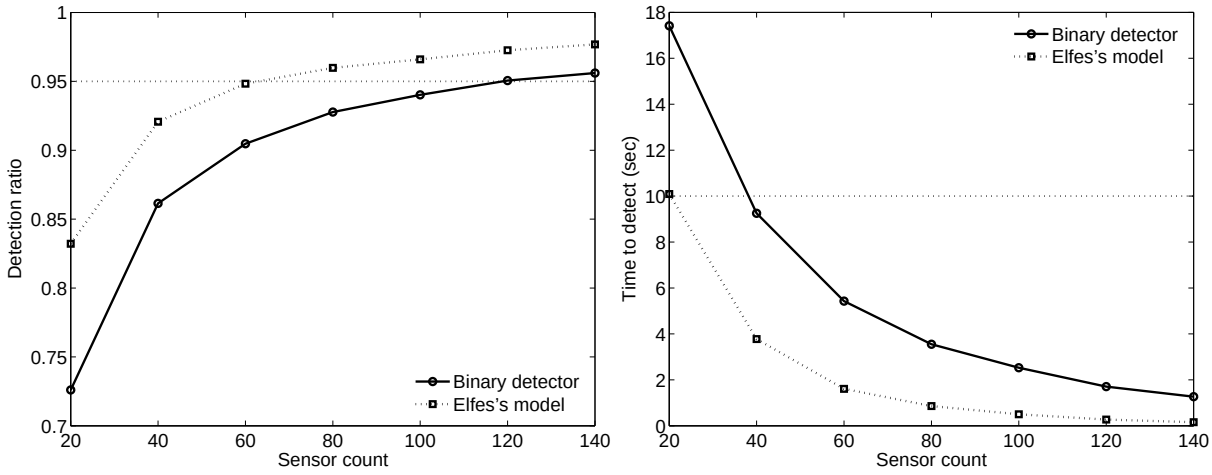


Fig. 4. SWSN simulation with OMNeT++.



(a) Effect of sensor count on detection ratio.

(b) Effect of sensor count on time-to-detect the target.

Fig. 5. Effect of sensor count on the detection ratio and time-to-detect the target when binary or Elfes's detectors are utilized.