# WIRELESS SENSOR NETWORKS FOR SECURITY: ISSUES AND CHALLENGES

Tolga Onel[1], Ertan Onur[1], Cem Ersoy[1] and Hakan Delic[2]
[1]*Department of Computer Engineering*
[2]*Department of Electrical and Electronics Engineering*
*Boğaziçi University*
*Bebek 34342 Istanbul, Turkey*

**Abstract** In this chapter, the sensing coverage area of surveillance wireless sensor networks is considered. The sensing coverage is determined by applying Neyman-Pearson detection 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. For target tracking applications, small wireless sensors provide accurate information since they can be deployed and operated near the phenomenon. These sensing devices have the opportunity of collaboration amongst themselves to improve the target localization and tracking accuracies. Distributed data fusion architecture provides a collaborative tracking framework. Due to the present energy constraints of these small sensing and wireless communicating devices, a common trend is to put some of them into a dormant state. We adopt a mutual information based metric to select the most informative subset of the sensors to achieve reduction in the energy consumption, while preserving the desired accuracies of the target position estimation.

## 1. Introduction

Wireless sensor devices that are employed for security applications have several functionalities. The first one is the distributed detection of the presence of a target, and the estimation of parameters of interest. The target may be tracked for various purposes. The detection, estimation and tracking efforts may or may not be collaborative. The second task involves wireless networking to organize and carry information. Issues related to distributed detection and estimation have long been studied. Moreover, wireless sensor networking is addressed in the literature to a certain extent in the context of ad hoc networking. However, there is not much work done on how the wireless networking constraints affect the distributed detection and estimation duty of the wireless smart sensor networking devices.

The sensing and communication ranges of some propriety devices are listed in [44]. For example, the sensing range of the Berkeley motes acoustic sensor, HMC1002 magnometer sensor and the 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.

For surveillance wireless sensor networks (SWSN), depending on the sensing ranges and the 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 are:

1 How many sensor are to be deployed to provide a required security level [31]?

2 How could the sensor detection be modeled and how is the sensing coverage determined?

3 What are the effects of geographic properties of the field on target detection?

4 How should the sensors be deployed in the region [38]?

5 What is the weakest part of the coverage and how can the breach paths be discovered [11, 46]?

6 How could the false alarms be minimized and the decisions be improved about target detection with collaboration?

7 What are the effects of the signal properties on the sensing coverage?

8 What is the impact of sensor scheduling on the sensing coverage [36, 40, 43]?

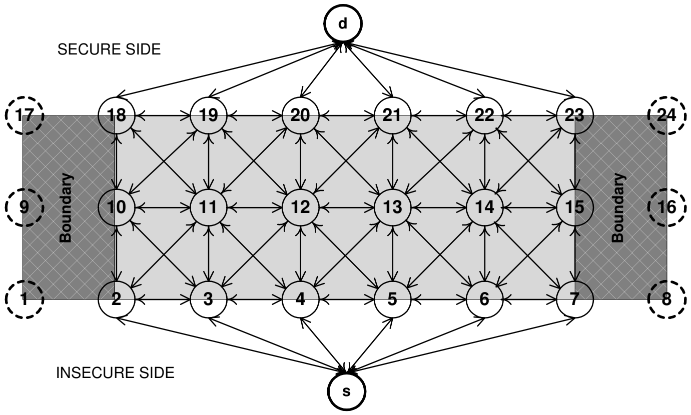

*Figure 1.* A sample field model constructed to find the breach path for length is 5 m., width 2 m., boundary 1 m., and grid size 1 m. ($N = 8, M = 3$).

9 Non-communicating sensors are useless; what should the effective communication and sensing ranges of the sensors be [8, 40]?

10 Should incremental deployment be considered [19]?

## Intrusion Detection

The security level of a WSN 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 determine 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 as in Fig. 1 The field model consists of the grid points, the starting point and the destination point.

The target aims to breach through the field from the starting point that represents the insecure side to the destination point that represents the secure side from the SWN viewpoint. The horizontal and vertical axes are divided into $N - 1$ and $M - 1$ equal parts, respectively. In this grid-based field model along the 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.

Sensor deployment has a direct impact on the performance of target detection. Chvatal's art gallery problem [10] 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 [12], where 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.

Another approach to the breach path problem is finding the path which is as far as possible from the sensor nodes as suggested in [27], where the 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 [24]. 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.

In [26], 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.

The field to be monitored is usually narrow and long in perimeter security applications. Thus, non-uniform deployment may be necessary. He *et al.* conclude that the sensor nodes generate false alarms at a non-negligible rate [18], and an exponentially weighted moving average on the sensor node is sufficient to eliminate transient alarms.

Due to the scarcity of energy resources of sensor nodes, energy conservation at all layers of the sensor network models is a widely studied topic. One method of energy conservation is applying a well-designed sleep schedule of sensor nodes [36, 40, 43]. However, for surveillance applications sleep scheduling of sensor nodes may produce insecure regions in the field. Thus, the primary concern in designing a sleep scheduling for surveillance wireless sensor networks is maintaining the coverage area. In [40], 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.

## Target Tracking

Target tracking, in other words the processing of the measurements obtained from a target in order to maintain an estimate of its current state, has major importance in Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) applications. Emerging wireless sensor technologies facilitate the tracking of targets just from within the phenomenon. Due to environmental perturbations, observations obtained close to the phenomenon are more reliable than observations obtained far from it. Wireless communication characteristics of the emerging wireless sensor nodes provide an excellent distributed coordination mechanism to improve global target localization accuracies. However, again, there is an inherent energy constraint for wireless sensor devices. In order to conserve valuable battery energy of wireless sensor devices, some of the sensors go into the dormant state controlled by the sleep schedule [42]. Only a subset of the sensors are active at any instant of time. Otherwise, a bulk of redundant data would be wandering in the network.

Collaborative target tracking has inherent questions such as how to dynamically determine who should sense, what needs to be sensed, and whom the information must be passed on to. Sensor collaboration improves detection quality, track quality, scalability, survivability, and resource usage [45].

There is a trade-off between energy expenditure and tracking quality in sensor networks [32]. Sensor activation strategies are *naive activation* in which all the sensors are active, *randomized activation* in which a random subset of the sensors are active, *selective activation* in which a subset of the sensors are chosen according to some performance metric, and *duty cycled activation* in which the sensors are active for some duty cycle and in dormant state thereafter.

In information driven sensor querying (IDSQ) [9, 45], the so-called cluster heads decide on the sensors to participate actively in the tracking task. In [25], a dual-space approach is presented in which the subset of sensors towards whom the target is approaching are selected to be active. In the location-centric approach to collaborative sensing and tracking, addressing and communication is performed among geographic regions within the network rather than individual nodes [35, 5]. This makes localized selective-activation strategies simpler to implement. Prediction based target tracking techniques based on Pheromones, Bayesian, and Extended Kalman Filter are presented in [6, 7], and a real implementation presented in [28]. Multiple target tracking is examined in [4, 15, 23].

Censoring sensors [1, 17, 33, 34] is one approach to diminish the network traffic load. Sensors deemed as noninformative do not send their decisions or observations if their local likelihood ratio falls in a certain single interval. A special case of this phenomenon occurs when the lower bound of the no-send region interval used is zero. In this particular case, the problem reduces to sending the local decision/observation if the local likelihood ratio is above some threshold and not sending the local decision/observation if the local likelihood ratio falls below a threshold. A deficiency with this approach occurs for tracking applications if all the sensor local likelihood ratios fall in the no-send region, so that no belief about the target state will be shared among the sensors.

Research [37, 43] has focused on how to provide full or partial sensing coverage in the context of energy conservation. In such an approach, nodes are put into a dormant state as long as their neighbors can provide sensing coverage for them. These solutions regard the sensing coverage to a certain geographic area as binary, i.e., either it provides coverage or not [42]. These approaches consider the sensor selection problem only in terms of coverage and energy saving aspects. They do not consider the detection quality. In tracking applications, when selecting a subset of sensors to contribute to the global decision we have to consider how informative the sensors are about the state of the target.

In some approaches to the sensor selection problem [9, 14], the sensor which will result in the smallest expected posterior uncertainty of the target state is chosen as the next node to contribute to the decision. It is shown in [14] that minimizing the expected posterior uncertainty is equivalent to maximizing the mutual information between the sensor output and the target state. In [39], an entropy-based sensor selection heuristic is proposed for target localization. The heuristic in [39] selects one sensor in each step and the observation of the selected sensor is incorporated into the target location distribution using sequential Bayesian filtering.

## 2. Neyman-Pearson Detection

Using the field model described above, 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 $\alpha$ is given by the Neyman-Pearson formulation [21]. 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.

Suppose that passive signal reception takes place in the presence of additive white Gaussian noise (AWGN) with zero mean and variance $\sigma_n^2$, as well as path-loss with propagation exponent $\eta$. The symbol power at the target is $\psi$, and the signal-to-noise power ratio (SNR) is defined as $\gamma = \psi/\sigma_n^2$. Each breach decision is based on the processing of $L$ data samples. We assume that the data are collected fast enough so that the Euclidean distance $d_{vi}$ between the grid point $v$ and sensor node $i$ remains about constant throughout the observation epoch. Then, given a false alarm rate $\alpha$, the detection probability of a target at grid point $v$ by sensor $i$ is [21, 31]

$$p_{vi} = 1 - \Phi\Big(\Phi^{-1}(1-\alpha) - \sqrt{L\gamma_{vi}}\Big)$$

where $\Phi(x)$ is the cumulative distribution function of the zero-mean, unit-variance Gaussian random variable at point $x$, and

$$\gamma_{vi} = \gamma A d_{vi}^{-\eta}$$

represents the signal-to-noise ratio at the sensor node $i$, with $A$ accounting for factors such as antenna gains and transmission frequency. Active sensing can be accommodated by properly adjusting the constant $A$.

Because the NP detector ensures that

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

instead of $p_{vi}$ we use [31]

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

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.

For those sensor types where the detection probability can not be explicitly tied to signal, noise and propagation parameters (e.g. infrared), the sensing model proposed by Elfes can be used [13]. The detection probability is defined such that different sensor types are represented by generic parameters. When the sensor-to-target distance is smaller (larger) than a threshold, the target is absolutely (not) detected. Elfes's model is employed in [30], where the required number of sensors is determined for a target breach probability level under random sensor placement.

The detection probability $p_v$ at any grid point $v$ is defined as

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

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 $p_{NM+1} = 0$. More clearly, these points are not monitored because they are not in the sensing coverage area. The boundary regions are not taken into consideration.

The weakest breach path problem can now 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. Here we can define the breach probability $P$ of the weakest breach path $V$ as

$$P = \prod_{v_j \in V} (1 - p_{v_j}) \tag{2}$$

where $p_{v_j}$ is the detection probability associated with the grid point $v_j \in V$, defined as in (1). 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. For a number of quality of deployment measures that can be utilized to evaluate a sensor network's intrusion detection capability, see [29].

In order to solve the weakest breach path problem, linear programming algorithms such as simplex can be utilized [3]. However, since we construct a graph to model the field, Dijkstra's shortest path algorithm can be employed [41]. The detection probabilities associated with the grid points cannot be directly used as weights of the grid points, and

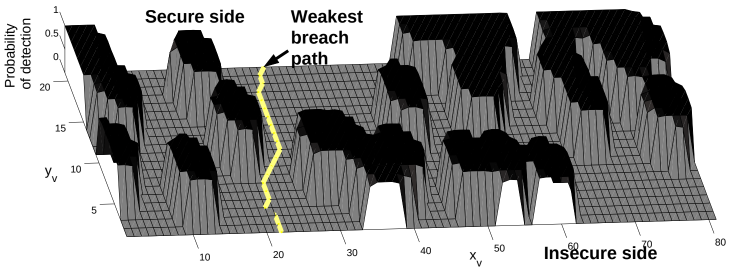

*Figure 2.* A sample sensing coverage and breach path where the field is 70 × 20 m., the boundary is 5 m. wide and the grid size is 1 m. ($N = 81, M = 21, L = 100, R = 30, \alpha = 0.1, \eta = 5, \gamma = 30$ dB.) [31].

consequently they must be transformed to a new measure $d_v$. Specifically, we assign the negative logarithms of the miss probabilities, defined as

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

as weights of the grid points.

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

$$P = 10^{-d_{NM+1}}. \tag{3}$$

The resulting path $V$ is used to calculate the breach probability in (2), which is equal to the value computed in (3) [30].

## 3. Breach Probability Analysis [31]

The system parameter values depend on the particular application. When a house or a factory is to be monitored for intrusion detection, the cost of false alarms is relatively low. On the other hand, the financial and personnel cost of a false alarm is significantly higher when the perimeter security of some mission-critical place such as an embassy or nuclear reactor is to be provided by deploying a 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.

In simulations, an area with dimensions 100 m. × 10 m. is secured by a WSN. The grid size is taken as one meter so that the detection probabilities of targets on adjacent grid points are independent. The boundary width is 10 m. The false alarm rate is set to 0.01, which is rather demanding on the network. Other nominal values are $\eta = 3, L =$

$100, \gamma = 30$ dB, $p_t = 0.9$ and $R = 31$. The results are the averages of 50 runs.

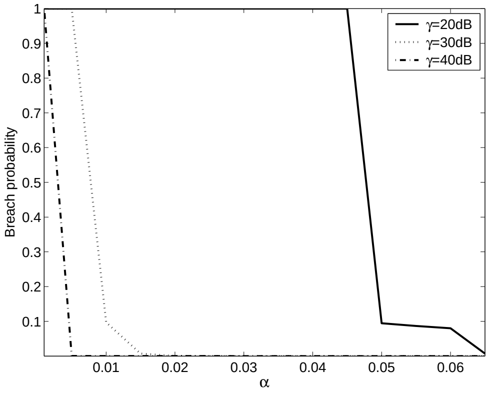

*Figure 3.* The effect of $\alpha$ on the breach probability.

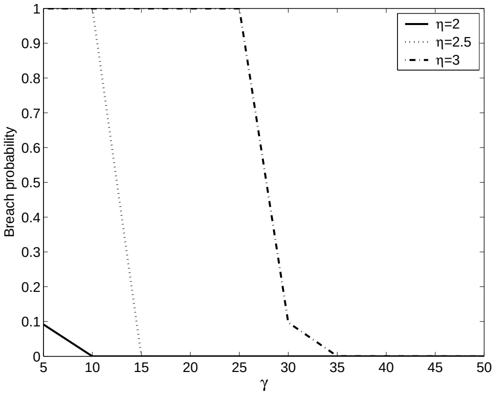

*Figure 4.* The effect of $\gamma$ on the breach probability.

The breach probability $P$ is quite sensitive to the false alarm rate $\alpha$. As shown in Fig. 3b, as $\alpha$ increases, the SWSN allows more false alarms. Because $\alpha$ 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 $\alpha$. Consequently, the breach probability decreases.

As the signal-to-noise ratio $\gamma$ increases, the detection performance improves (see Fig. 4), and the breach probability decreases. Depending on the path-loss exponent, $\gamma = 10$ dB yields minimal breach probability.

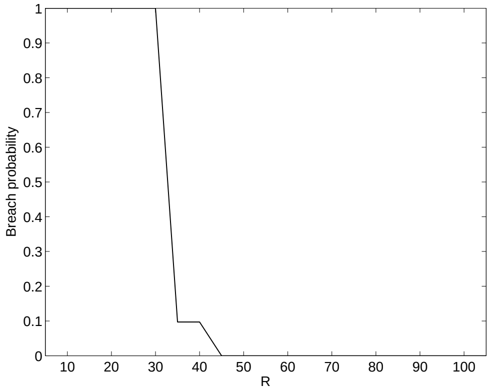

*Figure 5.* The effect of the number of sensor nodes on the breach probability for $y_v \sim \text{Uniform}(0, M-1)$.

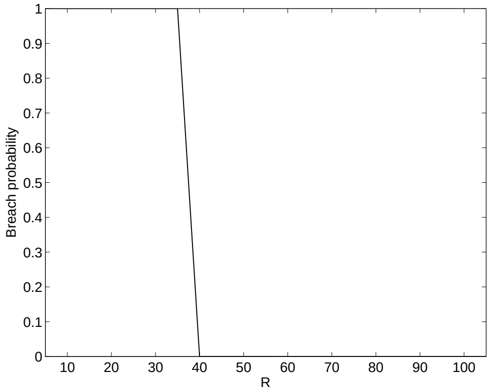

*Figure 6.* The effect of the number of sensor nodes on the breach probability for $y_v \sim \text{Normal}(M/2, N/10)$.

Note that $\eta$ and $\gamma$ display a duality in that if one is fixed, the performance breaks down when the other parameter is below or above some value.

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% 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 the uniformly distributed y-axis scheme, the required number of sensor nodes for a given breach probability is plotted in Fig. 5. A breach probability of 0.01 can be achieved by utilizing 45 sensors. Changing the false alarm rate to $\alpha = 0.1$, the requirement becomes 30 sensor nodes. The rapid decrease in the breach probability at $R = 16$ in Fig. 5a 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 saturation is reached, placing more sensors in the field has marginal effect.

Analyzing Fig. 6, 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.

## 4. Data Processing Architecture for Target Tracking

In this section, we first define the process and observation models for target tracking. Then the foundations of the distributed data fusion architecture are presented.

### Process Model

The target process is a four dimensional vector that consists of the two dimensional position of the target, $(\xi, \eta)$, and the velocity of the target, $(\dot{\xi}, \dot{\eta})$, at each of these dimensions. The target process state vector is defined by

$$\mathbf{x} = [\xi \, \eta \, \dot{\xi} \, \dot{\eta}]^T, \tag{4}$$

and it evolves in time according to

$$\mathbf{x}(k+1) = \mathbf{F}\mathbf{x}(k) + \mathbf{v}(k)$$

where $\mathbf{x}(k)$ is the real target state vector at time $k$ as given in (4), $\mathbf{F}$ is the process transition matrix, and $\mathbf{v}$ is the process transition noise.

### Observation Model

Sensors can only observe the first two dimensions of the process. The velocity of the target is not observable by the sensors. Furthermore, sensors collect range and bearing data, but they cannot observe the coordinates of the target directly. Because sensors observe the target state in polar coordinates, linear filtering formulations do not help. There are two implementation alternatives to remedy this problem: (1) by using the inverse transformation, obtain directly a *converted measurement* of the target position; (2) leave the measurement in its original form. The former yields a purely linear problem, allowing for linear filtering. The latter leads to a *mixed coordinate filter* [2]. In [22], the mean and covariance of the errors of Cartesian measurements, which are obtained by converting polar measurements, are derived. This conversion provides better estimation accuracy than the Extended Kalman Filter (EKF), in which the nonlinear target state measurements are utilized without conversion [22].

The measured range and bearing are defined with respect to the true range $r$ and bearing $\theta$ as

$$\begin{aligned} r_m &= r + \tilde{r} \\ \theta_m &= \theta + \tilde{\theta} \end{aligned}$$

where the errors in range $\tilde{r}$ and bearing $\tilde{\theta}$ are assumed to be independent with zero mean and standard deviations $\sigma_r$ and $\sigma_\theta$, respectively.

The target mean state observed after the unbiased polar-to-Cartesian conversion is given by

$$\varphi^c = \begin{bmatrix} \xi_m^c \\ \eta_m^c \end{bmatrix} = \begin{bmatrix} r_m \cos\theta_m \\ r_m \sin\theta_m \end{bmatrix} - \mu$$

where $\mu$ is the average true bias:

$$\mu = \begin{bmatrix} r_m \cos\theta_m (e^{-\sigma_\theta^2} - e^{-\sigma_\theta^2/2}) \\ r_m \sin\theta_m (e^{-\sigma_\theta^2} - e^{-\sigma_\theta^2/2}) \end{bmatrix}.$$

The covariances of the observation errors are [2, 22]

$$\begin{aligned} \mathbf{R}_{11} = {} & r_m^2 e^{-2\sigma_\theta^2} \left[\cos^2\theta_m (\cosh 2\sigma_\theta^2 - \cosh\sigma_\theta^2) \right. \\ & \left. + \sin^2\theta_m (\sinh 2\sigma_\theta^2 - \sinh\sigma_\theta^2)\right] \\ & + \sigma_r^2 e^{-2\sigma_\theta^2} \left[\cos^2\theta_m (2\cosh 2\sigma_\theta^2 - \cosh\sigma_\theta^2) \right. \\ & \left. + \sin^2\theta_m (2\sinh 2\sigma_\theta^2 - \sinh\sigma_\theta^2)\right], \end{aligned}$$

$$\begin{aligned} \mathbf{R}_{22} = {} & r_m^2 e^{-2\sigma_\theta^2} \left[\sin^2\theta_m (\cosh 2\sigma_\theta^2 - \cosh\sigma_\theta^2) \right. \\ & \left. + \cos^2\theta_m (\sinh 2\sigma_\theta^2 - \sinh\sigma_\theta^2)\right] \\ & + \sigma_r^2 e^{-2\sigma_\theta^2} \left[\sin^2\theta_m (2\cosh 2\sigma_\theta^2 - \cosh\sigma_\theta^2) \right. \\ & \left. + \cos^2\theta_m (2\sinh 2\sigma_\theta^2 - \sinh\sigma_\theta^2)\right] \end{aligned}$$

$$\mathbf{R}_{12} = \sin\theta_m \cos\theta_m e^{-4\sigma_\theta^2} \left[\sigma_r^2 + (r_m^2 + \sigma_r^2)(1 - e^{\sigma_\theta^2})\right].$$

## Distributed Data Fusion Architecture

Information state $\mathbf{y}$ and the information matrix $\mathbf{Y}$ associated with an observation estimate $\hat{x}$, and the covariance of the observation estimate $\mathbf{P}$ at time instant $k$ are given by [16]

$$\begin{aligned}\hat{\mathbf{y}}(k) &= \mathbf{P}^{-1}(k)\hat{\mathbf{x}}(k),\\ \mathbf{Y}(k) &= \mathbf{P}^{-1}(k).\end{aligned}$$

In [16], it is also shown that by means of sufficient statistics, an observation $\varphi$ contributes $\mathbf{i}(k)$ to the information state $\mathbf{y}$ and $\mathbf{I}(k)$ to the information matrix $\mathbf{Y}$ where

$$\begin{aligned}\mathbf{i}(k) &= \mathbf{H}^T\mathbf{R}^{-1}(k)\varphi(k), \qquad (5)\\ \mathbf{I}(k) &= \mathbf{H}^T\mathbf{R}^{-1}(k)\mathbf{H}\end{aligned}$$

and $\mathbf{H}$ is the observation matrix of the sensor.

Instead of sharing the measurements related to the target state among the collaborating sensors, sharing the information form of the observations results in a simple additive fusion framework that can be run on each of the tiny sensing devices. The distributed data fusion equations are

$$\begin{aligned}\hat{\mathbf{y}}(k \mid k) &= \hat{\mathbf{y}}(k \mid k-1) + \sum_{i=1}^{N} \mathbf{i}_i(k), \qquad (6)\\ \mathbf{Y}(k \mid k) &= \mathbf{Y}(k \mid k-1) + \sum_{i=1}^{N} \mathbf{I}_i(k) \qquad (7)\end{aligned}$$

where $N$ is the total number of sensors participating in the fusion process and $\hat{\mathbf{y}}(k \mid k-1)$ represents the information state estimate at time $k$ given the observations including time $k-1$.

Just before the data at time $k$ are collected, if we were given the observations up to the time $k-1$, the predicted information state and the information matrix at time $k$ could be calculated from

$$\begin{aligned}\hat{\mathbf{y}}(k \mid k-1) &= \mathbf{Y}(k \mid k-1)\mathbf{F}\mathbf{Y}^{-1}(k-1 \mid k-1)\hat{\mathbf{y}}(k-1 \mid k-1),\\ \mathbf{Y}(k \mid k-1) &= [\mathbf{F}\mathbf{Y}^{-1}(k-1 \mid k-1)\mathbf{F}^T + \mathbf{Q}]^{-1}\end{aligned}$$

where $\mathbf{Q}$ is the state transition covariance.

State estimate of the target at any time $k$ can be found from

$$\hat{\mathbf{x}}(k \mid k) = \mathbf{Y}^{-1}(k \mid k)\hat{\mathbf{y}}(k \mid k). \qquad (8)$$

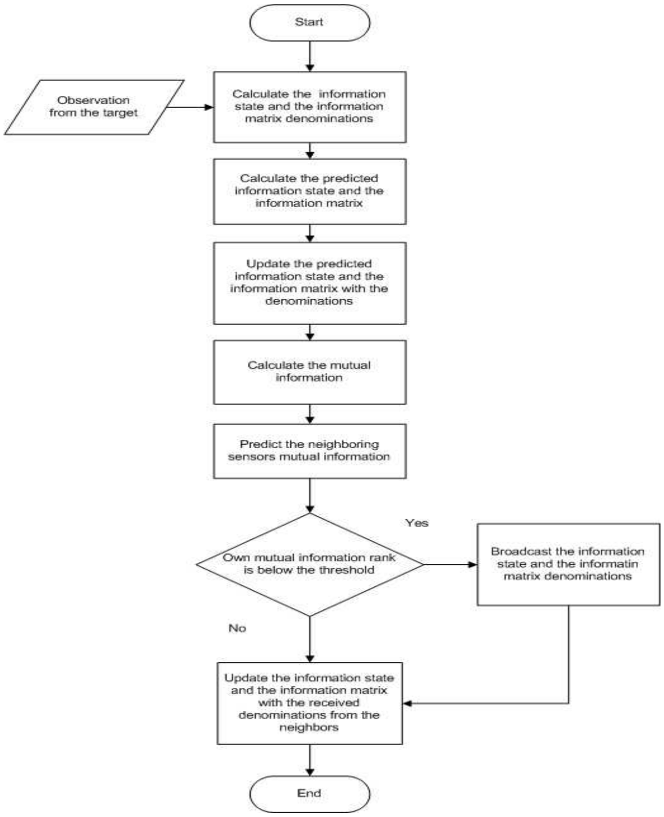
Start
Observation from the target
Calculate the information state and the information matrix denominations
Calculate the predicted information state and the information matrix
Update the predicted information state and the information matrix with the denominations
Calculate the mutual information
Predict the neighboring sensors mutual information
Yes
Own mutual information rank is below the threshold
Broadcast the information state and the informatin matrix denominations
No
Update the information state and the information matrix with the received denominations from the neighbors
End

*Figure 7.* Target tracking algorithm for a sensor.

## 5. Maximum Mutual Information Based Sensor Selection Algorithm

Mutual information measures how much information one random variable tells about another one. In target localization and tracking applications, the random variables of interest are the target state and the observation obtained about the target state. By measuring the mutual information between the target state and the measurement, one can gain insight as to how much the current observation tells about the current target state.

The algorithm employed by a sensor for tracking targets in a collaborative manner within the distributed data fusion framework is depicted in Fig. 7. The information state and the information matrix are defined by (5). The predicted information state and the information matrix are computed by (7). The sensor's current belief is updated by its own sensory observation according to

$$\begin{aligned}\hat{\mathbf{y}}(k \mid k) &= \hat{\mathbf{y}}(k \mid k-1) + \mathbf{i}(k), \\ \mathbf{Y}(k \mid k) &= \mathbf{Y}(k \mid k-1) + \mathbf{I}(k).\end{aligned}$$

Active participation to the current cycle is decided based on the mutual information gained with the last observation. This event can be formulated as

$$J(k, \varphi(k)) = \frac{1}{2} \log \left[ \frac{|\mathbf{Y}(k \mid k)|}{|\mathbf{Y}(k \mid k-1)|} \right]. \tag{9}$$

If the mutual information gain $J$ of the sensor is sufficiently high to participate in the current cycle, the sensor shares its own information about the target state with the neighboring nodes. Otherwise, the sensor does not transmit during the current cycle. In (9), $\mathbf{Y}(k \mid k-1)$ denotes the predicted information matrix at the time instant $k$, given the observation up to the time instant $k-1$. Thus, the sensor has an estimate about the target state information that it will have at time instant $k$, before the observation of the target state at time instant $k$. $\mathbf{Y}(k \mid k)$ is the information matrix at the time instant $k$ after the target state is observed. The mutual information in (9) measures the improvement in the target state estimate achieved with the observation. To decide if the mutual information is adequately high to participate in the current cycle, a sensor needs to know the mutual information values of its neighboring sensors. This information is hard to predict ahead of time. To tackle this problem, we design each sensor to hold a list of its neighboring sensors. The elements of this list are the sensor characteristics like the standard deviation of the target range observations, standard deviation of the target angle observations, and the communication transmission power. Knowing the communication signal transmission power of the neighboring sensor, it is easy to estimate the relative position of the neighboring sensor. This position estimation is done in a sliding window average of the last eight communications received from the neighboring sensor. With the sensors' own observation about the target state, it is again easy to estimate the $\mathbf{Y}(k \mid k)$ value of the neighboring sensor. $\mathbf{Y}(k \mid k-1)$ is the estimation of the cooperated information matrix. Given this information, the mutual information $J$ for the neighboring sensors is estimated. All the neighboring sensors and the sensor itself are sorted according to the decreasing mutual information order. If the sensor detects the target, and the rank of its mutual information is lower than the maximum allowed number of sensors to communicate then the sensor broadcasts its information state and the information matrix denominations to the network. The current belief is updated with the received information from the sensors in the vicinity according to (6). A current state estimate for the target can be found from (8).

## 6. Simulation Results

We run Monte Carlo simulations to examine the performance of the sensor selection algorithm based on the maximization of mutual information for the distributed data fusion architecture. We examine two scenarios: first is the sparser one, which consists of 50 sensors randomly deployed in the 200 m × 200 m area. The second is a denser scenario in which 100 sensors are deployed in the same area. All data points in the graphs represent the means of ten runs. A target moves in the area according to the process model described in Section 4. We utilize the Neyman-Pearson detector [21, 31] with $\alpha = 0.05, L = 100, \eta = 2$, 2-dB antenna gain, , -30-dB sensor transmission power and -6-dB noise power.

The sensor tracks the target locally using the information form of the Kalman filtering [20] as described in Section 4. If the sensor does not detect a target, it updates its belief about the target state just by setting the Kalman filter gain to zero, which means that the sensor tracks the target according to the track history.

In collaborative information fusion, if a sensor is eligible to share its belief about the target state with other sensors, it broadcasts its information state and the information matrix. Sensors that receive these data according to the shadow-fading radio propagation model update their belief about the target state as described in Section 4. The shadow-fading radio propagation model assumes that the antenna heights are 10 cm., the shadow-fading standard deviation is 4, and the carrier frequency is 1.8 GHz. If the received communication signal from a sensor is below 15 dB, then the signal is treated as garbage.

In the simulations, we compare the mean squared error about the target localization for the collaborative tracking framework described in Section 4. We achieve maximum tracking accuracy when all sensors detecting the target participate in the distributed data fusion task. As the number of sensors allowed to participate in the fusion task is reduced, tracking quality deteriorates. This yields higher localization errors about the distributed target position estimations. However, a reduced number of sensors allowed to communicate yields a lower number of communication packets traveling in the network. Reduction in the number of sent packets affects the energy expenditure of the wireless sensor devices directly. Selecting the sensors to actively participate in the fusion task in an intelligent manner improves tracking quality while allowing the same number of sensors to communicate. Figure 8 depicts

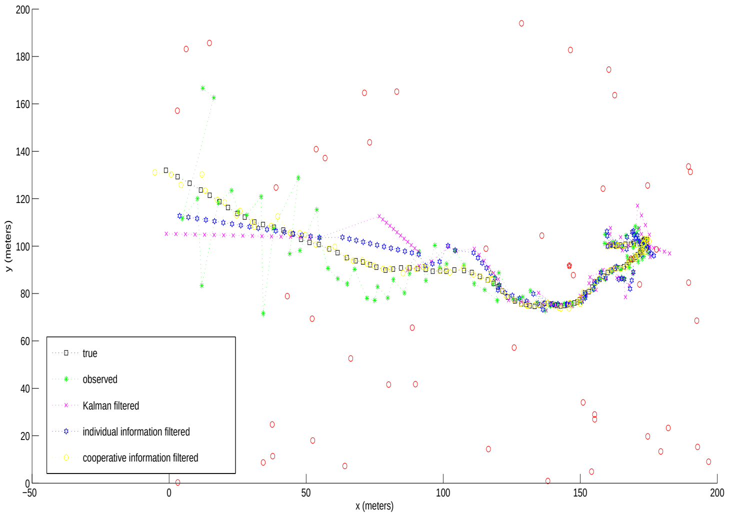

*Figure 8.* Illustration of the 50-sensor scenario.

the 50-sensor scenario, target location observation errors, Kalman and information filtered target localization errors, and cooperative information filtered target localization errors from the viewpoint of the sensor which is marked with a star inside it.

Selecting the participating active sensors randomly means that a sensor detecting the target broadcasts its information immediately if the maximum number of sensors to participate has not yet been reached. The minimum Mahalanobis distance based sensor selection algorithm selects the closest sensors to the target location in terms of the Mahalanobis distance. Mahalanobis distance takes into account the correlations of the data. If the covariance matrix is the identity matrix then Mahalanobis distance is the same as Euclidian distance. Figures 9 and 10 show, for the sparse and dense scenarios respectively, that as the maximum number of sensors allowed to communicate in the vicinity of the current cycle increases, total Mean Squared Error occurring throughout a hundred seconds scenario decreases for all three sensor selection algorithms. Target localization errors are calculated each second. For the cases studied, selecting sensors which improve the global belief about target position according to the mutual information metric results in an average 4.07% improvement in tracking quality with respect to random sensor selection. 2.86% tracking quality improvement is achived with respect to the maximum Mahalanobis distance based sensor selection for

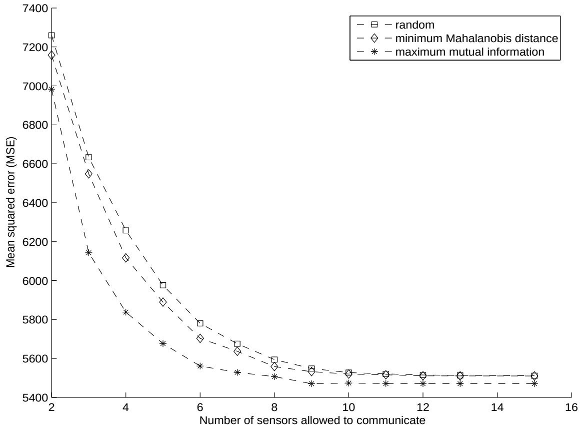

*Figure 9.* Mean squared error comparison for the sparse scenario.

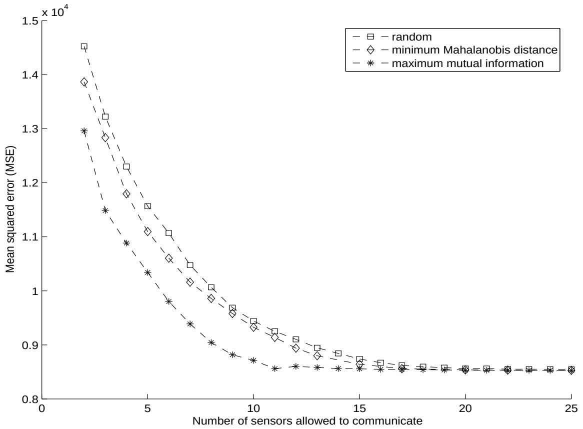

*Figure 10.* Mean squared error comparison for the dense scenario.

the sparse scenario. For the dense scenario of 100 sensors, these improvements with the mutual information based sensor selection algorithm go to 9.65% and 6.32% with respect to the random and the Mahalanobis distance based sensor selection algorithms, respectively.

Figures 11 and 12 depict the total energy exhausted in the network for all three sensor selection algorithms during the hundred seconds scenario. Consumed energy increases as the maximum number of sensors that are allowed to communicate for the current cycle increases. This was a natural result of the increasing number of communication packets in the network. However, the sensor selection algorithm does not have a

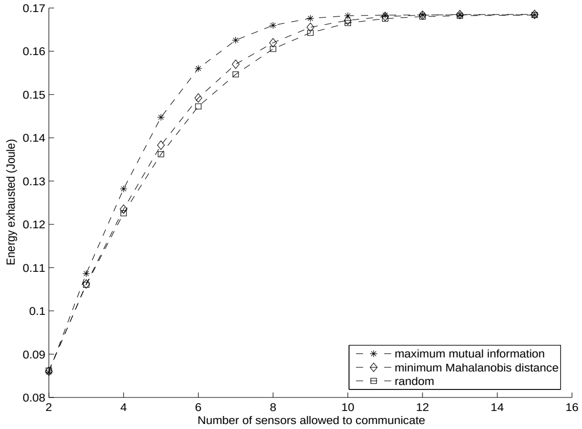

*Figure 11.* Comparison of the consumed energy for the sparse scenario.

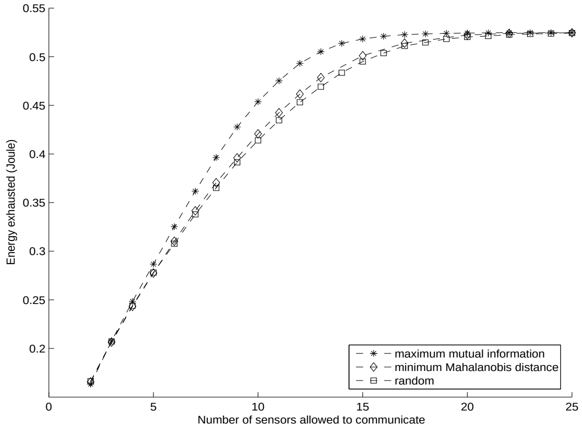

*Figure 12.* Comparison of the consumed energy for the dense scenario.

significant effect on the exhausted energy of the network for any number of allowed sensors to communicate.

## 7. Conclusion

We employ the Neyman-Pearson detector 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. The breach probability is defined as the miss probability of the weakest breach path. The false alarm rate constraint has a significant impact on the intrusion detection performance of the network, which is measured by the breach probability.

The model and results developed herein 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 in the future. Simulating the reliability of the network throughout the entire life of the wireless sensor network is also required. Lastly, especially for perimeter surveillance applications, obstacles in the environment play a critical role in terms of sensing and must be incorporated in the field model.

A mutual information based information metric is adopted to select the most informative subset of sensors to actively participate in the distributed data fusion framework. The duty of the sensors is to accurately localize and track the targets. Simulation results show 36% energy saving for a given tracking quality can be achievable by selecting the sensors to cooperate according to the mutual information metric.

In all tests, we assumed all the sensor nodes send reliable data to the network. In future work, detection of faulty and outlier sensors in the network must be investigated, and precautions need to be taken against them. We considered the effect of sensor selection algorithms in the context of distributed data fusion for tracking a single target. Existence of multiple targets introduces challenges with track-to-track association and track-to-sensor association, as well as issues related to access control and routing.

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

# References

[1] S. Appadwedula, V. V. Veeravalli, and D. L. Jones, “Robust and locally optimum decentralized detection with censoring sensors”, in *Proceedings of the International Conference on Information Fusion*, Annapolis, USA, July 2002, pp. 56-63.

[2] Y. Bar-Shalom, X. R. Li, and T. Kirubarajan, *Estimation with Applications to Tracking and Navigation*, Wiley, 2001.

[3] M. S. Bazaraa and J. J. Jarvis, *Linear Programming and Network Flows*, Wiley, 1977.

[4] R. Bejar, B. Krishnamachari, C. Gomes, and B. Selman, “Distributed constraint satisfaction in a wireless sensor tracking system”, in *Proceedings of the Workshop on Distributed Constraint Reasoning, International Joint Conference on Artificial Intelligence*, Seattle, USA, August 2001.

[5] R. R. Brooks, P. Ramanathan, and A. Sayeed, “Distributed target tracking and classification in sensor network”, *Proceedings of the IEEE*, Vol. 91, No. 8, pp. 1163-1171, August 2003.

[6] R. R. Brooks and C. Griffin, “Traffic model evaluation of ad hoc target tracking algorithms”, *International Journal of High Performance Computing Applications*, Vol. 16, No. 3, pp. 221-234, August 2002.

[7] R. R. Brooks, C. Griffin, and D. S. Friedlander, “Self-organized distributed sensor network entity tracking”, *International Journal of High Performance Computing Applications*, Vol. 16, No. 3, pp. 207-219, August 2002.

[8] J. Carle and D. Simplot-Ryl, “Energy-efficient area monitoring for sensor networks,” *IEEE Computer*, Vol. 37, No. 2, pp. 40-46, February 2004.

[9] M. Chu, H. Haussecker, and F. Zhao, ”Scalable information-driven sensor querying and routing for ad hoc heterogenous sensor networks,” *International Journal of High Performance Computing Applications*, Vol. 16, No. 3, pp. 293-313, August 2002.

[10] V. Chvatal, “A combinatorial theorem in plane geometry,” *Journal of Combinatorial Theory*, Vol. B, No. 13, pp. 39-41, 1975.

[11] 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.

[12] S. S. Dhillon and K. Chakrabarty, “Sensor placement for effective coverage and surveillance in distributed sensor networks,” in *Proceedings of the IEEE Wireless Communications and Networking Conference*, New Orleans, USA, March 2003, pp. 1609-1614.

[13] 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, Editors, IEEE Computer Society Press, 1991, pp. 60-70.

[14] E. Ertin, J. W. Fisher, and L. C. Potter, “Maximum mutual information principle for dynamic sensor query problems”, in *Proceedings of the 2nd International Workshop on Information Processing in Sensor Networks*, Palo Alto, USA, April 2003, pp. 405-416.

[15] Q. Fang, F. Zhao, and L. Guibas, “Counting targets: Building and managing aggregates in wireless sensor networks”, Palo Alto Research Center (PARC), Tech. Rep. P2002-10298, June 2002.

[16] B. Grocholsky, A. Makarenko, and H. Durrant-Whyte, ”Information-theoretic coordinated control of multiple sensor platforms,” in *Proceedings of the IEEE International Conference on Robotics and Automation*, Taipei, Taiwan, September 2003, pp. 1521-1526.

[17] R. Jiang and B. Chen, “Decision fusion with censored sensors”, *Proceedings of ICASSP*, Vol. 2, Montreal, Canada, May 2004, pp. 289-292.

[18] 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, June 2004, pp. 270-283.

[19] 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.

[20] R. E. Kalman, ”A new approach to linear filtering and prediction problems,” *Transactions of the ASME-Journal of Basic Engineering*, Vol. 82, pp. 35-45, 1960, series D.

[21] D. Kazakos and P. Papantoni-Kazakos, *Detection and Estimation*, New York, USA: Computer Science Press, 1990.

[22] D. Lerro and Y. Bar-Shalom, “Tracking with debiased consistent converted measurements versus EKF”, *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 29, No. 3, pp. 1015-1022, July 1993.

[23] D. Li, K. D. Wong, Y. Hu, and A. M. Sayeed, “Detection, classification, tracking of targets in micro-sensor networks”, *IEEE Signal Processing Magazine*, Vol. 19, No. 2, pp. 17-29, March 2002.

[24] X.-Y. Lin, P.-J. Wan and O. Frieder, “Coverage in wireless ad hoc sensor networks,” *IEEE Transactions on Computers*, Vol. 52, No. 6, pp. 753-763, June 2003.

[25] J. Liu, P. Cheung, L. Guibas, and F. Zhao, "A dual-space approach to tracking and sensor management in wireless sensor networks", in *The First ACM International Workshop on Wireless Sensor Networks and Applications*, Atlanta, USA, September 2002.

[26] 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.

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

[28] J. Moore, T. Keiser, R. R. Brooks, S. Phoha, D. Friedlander, J. Koch, A. Reggio, and N. Jacobson, "Tracking targets with self-organizing distributed ground sensors", in *Proceedings of the IEEE Aerospace Conference*, Vol. 5, Big Sky, USA, March 2003, pp. 2113-2123.

[29] E. Onur, C. Ersoy and H. Deliç, "Quality of deployment in surveillance wireless sensor networks", *International Journal of Wireless Information Networks*, Vol. 12, No. 1, pp. 61-67, January 2005.

[30] E. Onur, C. Ersoy and H. Deliç, "How many sensors for an acceptable breach probability level?", *Computer Communications*, Special Issue on Dependable Sensor Networks, in press 2005.

[31] E. Onur, C. Ersoy and H. Deliç, "Sensing coverage and breach paths in surveillance wireless sensor networks", in *Sensor Network Operations*, S. Phoha, T. F. La Porta and C. Griffin, Editors, IEEE Press, 2005.

[32] S. Pattern, S. Poduri and B. Krishnamacharie, "Energy-quality tradeoffs for target tracking in wireless sensor networks", in *Proceedings of Information Processing in Sensor Networks*, Palo Alto, USA, April 2003, pp. 32-36.

[33] N. Patwari and A. O. Hero, "Hierarchical censoring for distributed detection in wireless sensor networks", *Proceedings of IEEE ICASSP*, Vol. 4, Hong Kong, April 2003, pp. 848-851.

[34] C. Rago, P. Willett, and Y. Bar-Shalom, "Censoring sensors: A low communication-rate scheme for distributed detection", *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 32, No. 4, pp. 554-568, April 1996.

[35] P. Ramanathan, "Location-centric approach for collaborative target detection, classification, and tracking", in *Proceedings of the IEEE CAS Workshop on Wireless Communications and Networking*, Pasadena, USA, September 2002.

[36] 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.

[37] D. Tian and N. D. Georganas, "A node scheduling scheme for energy conservation in large wireless sensor networks", *Wireless Communications and Mobile Computing*, Vol. 3, No. 2, pp. 271-290, May 2003.

[38] S. Tilak, N. B. Abu-Ghazaleh and W. Heinzelman, “Infrastructure tradeoffs for sensor networks,” *Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications*, Atlanta, USA, September 2002, pp. 49-58.

[39] H. Wang, K. Yao, G. Pottie, and D. Estrin, “Entropy-based sensor selection heuristic for target localization,” in *Proceedings of the Third Symposium on Information Processing in Sensor Networks*, Berkeley, USA, April 2004, pp. 36-45.

[40] X. Wang, G. Xing, Y. Zhang, C. Lu, R. Pless and C. Gill, “Integrated coverage and connectivity configuration in wireless sensor networks,” in *Proceedings of the First International ACM Conference on Embedded Networked Sensor Systems*, Los Angeles, USA, November 2003, pp. 28-39.

[41] M. A. Weiss, *Data Structures and Algorithm Analysis in C++*, 2nd Edition, Addison-Wesley, 1999.

[42] T. Yan, T. He and J. A. Stankovic, “Differentiated surveillance for sensor networks,” SENSYS 2003.

[43] 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.

[44] H. Zhang and C.-J. Hou, “On deriving the upper bound of $\alpha$-lifetime for large sensor networks,” *Technical Report UIUCDCS-R-2004-2410*, University of Illinois at Urbana-Champaign, Department of Computer Science, February 2004.

[45] F. Zhao, J. Shin and J. Reich, “Information-driven dynamic sensor collaboration for tracking application,” *IEEE Signal Processing Magazine*, Vol. 19, No. 1, pp. 61-72, March 2002.

[46] 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.