Vulnerability of Sensor Networks to Unauthorized Traversal and Monitoring

Veradej Phipatanasuphorn Parameswaran Ramanathan

Department of Electrical and Computer Engineering
University of Wisconsin-Madison
Madison, WI 53706–1691
parmesh@ece.wisc.edu, (608) 263-0557
Fax: (608) 265-4623

ABSTRACT

There is a growing interest in the use of wireless ad hoc sensor networks to monitor, detect, and track the movement of specified targets in a geographic region. A common concern in the deployment of such networks is whether or not a target can pass or intrude a sensor field without being detected. Recent papers in literature have defined a measure called exposure to quantify the likelihood of a target passing through a sensor field without being detected. These papers differ in the definition of exposure. Also, the existing definitions of exposure are indicators of the likelihood of intrusion and not a direct measure of it.

In this paper, we directly work with probability of detection instead of its indicators. We also probabilistically account for the presence of noise in the sensor readings. In the presence of noise, there is a tradeoff between the probability of a target passing through a sensor field without detection and the false alarm probability (i.e., the probability of falsely detecting the presence of target). We analytically characterize this tradeoff and illustrate the tradeoff for example deployments.

We also introduce a variant of the traversal problem called unauthorized monitoring. This problem is of interest if sensor fields are used to secure an asset. We analytically characterize the probability of unauthorized monitoring and the tradeoff between this probability and its false alarm probability in the presence of noise.

Index Terms: Wireless ad hoc networks, sensor deployment, sensor exposure prooblem.

The work reported here is supported in part by the Defense Advanced Research Projects Agency (DARPA) and the Air Force Research Laboratory, Air Force Material Command, and USAF under agreement number F30602-00-2-055. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright annotation thereon.

1 Introduction

Due to recent advances in technology, it is now possible to build low cost devices with sensing, processing, and wireless communication capabilities [1]. A large number of these devices can be deployed in a region of interest to form a network that monitors, detects, and tracks specified targets as they move through the sensor field [2]. A common concern in such networks is whether or not a target can intrude a given sensor field without being detected. Recent papers have quantified this concern using a notion called *exposure* [3, 4, 5]. The papers differ in the definition of exposure.

For instance, in [3], the authors propose two different measures of exposure: maximal breach and maximal support. The *maximal breach* path through a sensor field is defined as a path where its closest distance to any of the sensors is as large as possible while the *maximal support* path is defined as a path where the farthest distance from the closest sensor is as small as possible. Algorithms for efficiently determining the maximal breach and maximal support path for a given sensor field are also described. In [4], exposure is defined as the total energy that the sensors will gather from the target as it moves through the field. The smaller this energy the lesser the likelihood of detecting the target. An algorithm for determining a path with the least exposure in this sense is also developed in [4]. The algorithms in [3, 4] are centralized. Distributed versions of algorithms to accomplish the same objectives are described in [5].

One of the problems considered in this paper is similar to the ones in [3, 4, 5]. However, there are some key differences. First, the definition of exposure is different. We define the exposure of a path as the probability of detecting a target traversing the field using the path. Although, the total energy measure in [4] is an indicator of this probability, the relationship between total energy and the detection probability is not linear. In particular, it depends on the detection algorithm being used by the sensors. Second, energy measurements at sensors are typically very noisy. The probability of detecting a target moving through a field depends on this noise. In the presence of noise, there is usually a non-zero probability of incorrectly detecting a target when there is actually no target in the field, i.e., false alarm. In fact, there is usually a tradeoff between the probability of false alarm and the probability of detection. That is, to achieve higher probabilities of detection one must endure higher probabilities of false alarm. In this paper, we analytically characterize this tradeoff and develop algorithms for finding a path with the least exposure.

The second problem considered in this paper is a variant of the above problem called unauthorized monitoring. This problem is of interest in situations where a sensor field is used to protect an asset from unauthorized monitoring, i.e., in situations where the sensor field is deployed to detect intruders who try to gather valuable information from an asset by monitoring it for a

certain duration. Once again, in the presence of noise, there is tradeoff between probability of detection and probability of false alarm. We analytically characterize this tradeoff and develop algorithms for finding a path with the least exposure.

The rest of this paper is organized as follows. The unauthorized traversal and monitoring problems are formulated in Section 2. The solutions to the two problems are developed in Section 3. A numerical characterization of the tradeoff between exposure and false alarm is presented in Section 4. The paper concludes in Section 5.

2 Problem Formulation

Consider a rectangular sensor field with n sensors deployed at locations s_i, $i = 1, \ldots, n$. A target at location u emits a signal which is measured by the sensors. The signal from the target decays exponentially with distance. If the decay coefficient is k, the signal energy of a target at location u measured by the sensor at s_i is given by

$$S_i(u) = \frac{K}{||u - s_i||^k},$$

where K is the energy emitted by the target and $||u - s_i||$ is the geometric distance between the target and the sensor. Depending on the environment the value k typically ranges from 2.0 to 5.0 [6].

Energy measurements at a sensor are usually corrupted by noise. If N_i denotes the noise energy at sensor i during a particular measurement, then the total energy measured at sensor i when the target is at location u is

$$E_i(u) = S_i(u) + N_i = \frac{K}{||u - s_i||^k} + N_i.$$

The sensors collaborate to arrive at a consensus decision as to whether a target is present in the region. There are two basic approaches for reaching this consensus: Value fusion and Decision fusion [7]. In value fusion, one of the sensors gathers the energy measurements from the other sensors, totals up the energy and compares the sum to a threshold to decide whether a target is present. If the sum exceeds the threshold, then the consensus decision is that a target is present. In contrast, in decision fusion, each individual sensor compares its energy measurement to a threshold to arrive at a local decision as to whether a target is present. The local decisions (1 for target present and 0 otherwise) from the sensors are totaled at a sensor and the sum is compared to another threshold to arrive at the consensus decision. In some situations, value fusion outperforms decision fusion and vice versa.

Value Fusion. The probability of consensus target detection when the target is at location u is

$$\begin{aligned} D_v(u) &= \text{Prob}\left[\sum_{i=1}^{n} \frac{K}{||u-s_i||^k} + N_i \geq \eta\right] \\ &= \text{Prob}\left[\sum_{i=1}^{n} N_i \geq \eta - \sum_{i=1}^{n} \frac{K}{||u-s_i||^k}\right], \end{aligned}$$

where η is the value fusion threshold. If the noise processes at the sensors are independent, then the probability density function of $\sum_{i=1}^{n} N_i$ equals the convolution of the probability density function of N_i, $i = 1, \ldots, n$. In particular, if the noise process at each sensor is Additive White Gaussian Noise (AWGN), then $\sum_{i=1}^{n} N_i$ has a Chi-square distribution of degree n.

Due to the presence of noise, the sensors may incorrectly decide that a target is present even though there is no target in the field. The probability of a consensus false target detection is

$$F_v = \text{Prob}\left[\sum_{i=1}^{n} N_i \geq \eta\right]. \tag{1}$$

As above, if the noise processes at the sensors are independent and AWGN, then false probability can be computed from the Chi-square distribution of degree n.

Decision Fusion. For decision fusion, the probability of consensus target detection when the target is located at u is

$$\begin{aligned} D_d(u) &= \text{Prob}\left[\sum_{i=1}^{n} h_{d,i}(u) \geq \eta_2\right] \\ &= \sum_{j=\eta_2}^{n} \binom{n}{j} \cdot (\text{Prob}\left[h_{d,i}(u) = 1\right])^j \cdot (\text{Prob}\left[h_{d,i}(u) = 0\right])^{(n-j)} \end{aligned}$$

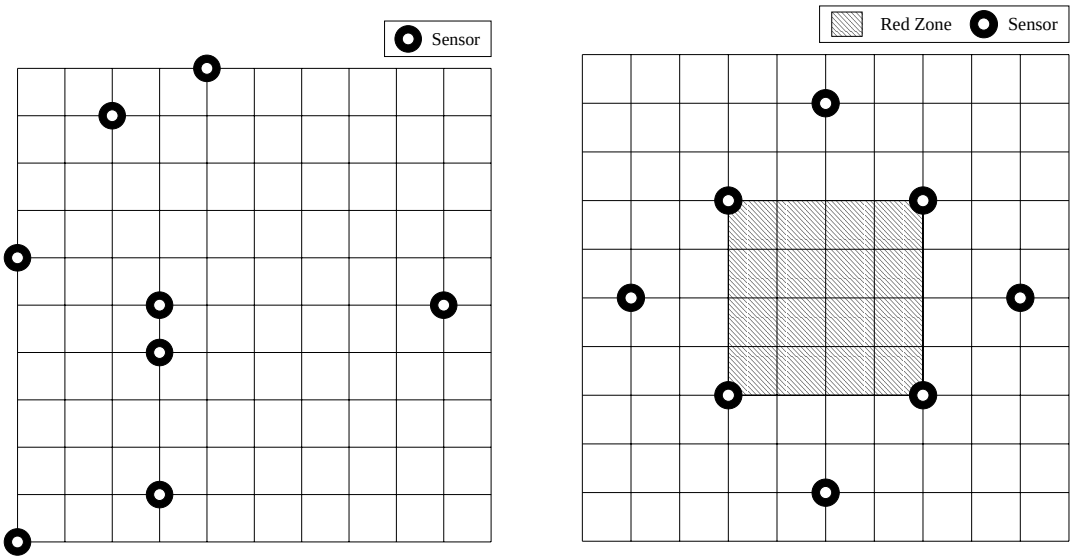
where

$$\begin{aligned} \text{Prob}\left[h_{d,i}(u) = 1\right] &= \text{Prob}\left[N_i \geq \eta_1 - \frac{K}{||u-s_i||^k}\right] \quad \text{and} \\ \text{Prob}\left[h_{d,i}(u) = 0\right] &= 1 - \text{Prob}\left[h_{d,i}(u) = 1\right]. \end{aligned}$$

can be computed from Chi-square distribution of degree 1 for AWGN noise process.

The probability of false target detection at sensor i is

$$\begin{aligned} \text{Prob}[g_{d,i} = 1] &= \text{Prob}[N_i \geq \eta_1] \quad \text{and} \\ \text{Prob}[g_{d,i} = 0] &= 1 - \text{Prob}[g_{d,i} = 1]. \end{aligned}$$



(a) UT Problem (b) UM Problem

Figure 1: Example sensor fields for UT and UM problems.

Therefore, the probability of consensus false target detection is

$$\begin{aligned} F_d &= \text{Prob}\left[\sum_{i=1}^{n} g_{d,i} \geq \eta_2\right] \\ &= \sum_{j=\eta_2}^{n} \left(\begin{array}{c} n \\ j \end{array} \right) \cdot (\text{Prob}\left[g_{d,i} = 1\right])^{j} \cdot (\text{Prob}\left[g_{d,i} = 0\right])^{(n-j)} . \end{aligned}$$

The above equations serve as an analytic basis for the two problems, namely Unauthorized Traversal (UT) and Unauthorized Monitoring (UM), considered in this paper. In particular, we define *exposure* to be the probability of detecting the target or an intruder carrying out the unauthorized activity, where the activity depends on the problem under consideration. The analytic expression for the exposure depends on the problem and the associated activity.

Unauthorized Traversal (UT) Problem: We are given a sensor field with n sensors at locations s_1, s_2, ..., s_n (see Figure 1(a)). We are also given the stochastic characterization of the noise at each sensor and a tolerable bound, α, on the false alarm probability. Let P denote a path from the west to the east periphery of the sensor field. A target traversing the sensor field using path P is detected if it is detected at some point $u \in P$. The *exposure* of path P is the net probability of detecting a target that traverses the field using P. The problem is to find the path P with the least exposure.

Unauthorized Monitoring (UM) Problem: We are given a sensor field with n sensors at locations s_1, s_2, ..., s_n (see Figure 1(b)). We are also given the stochastic characterization of the noise at each sensor and a tolerable bound, α, on the false alarm probability. Within the sensor field, there is an asset at a specified location. An area around the asset is identified as the red zone (e.g., the shaded area in Figure 1(b)). An intruder can gain unauthorized valuable information about the asset if he/she spends at least T time units in the red zone. Let P denote a path from the sensor field periphery to a point in the red zone. The *exposure* of path P is the net probability of detecting an intruder who enters the red zone using path P, spends at least T time units inside the red zone, and exits using path P. The problem is to find the path P with the least exposure.

3 Proposed Solutions

3.1 UT Problem

Let P denote a path from the west to the east periphery through the sensor field. A target that traverses the field using P is not detected if and only if it is not detected at every point $u \in P$. As a result, the net probability of not detecting a target traversing the field using P is the product of the probabilities of no detection at each point $u \in P$. That is, if $G(P)$ denotes the net probability of not detecting a target as it traverses over path P, then,

$$\log G(P) = \int_{u \in P} \log(1 - D(u)) du,$$

where $D(u)$ is either $D_v(u)$ of $D_d(u)$ depending on whether the sensors use value or decision fusion to arrive at a consensus decision. Since the exposure of P is $(1 - G(P))$, the problem is to find the path which minimizes $(1 - G(P))$ or equivalently the path that minimizes $|\log G(P)|$[1].

In general, the path P that minimizes $|\log G(P)|$ can be fairly arbitrary in shape. The proposed solution does not exactly compute this path. Instead, we rely on the following approximation. We first divide the sensor field into a fine grid and then assume that the target only moves along this grid. The problem then is to find the path P on this grid that minimizes $|\log G(P)|$. Note that, the finer the grid the closer the approximation. Also, one can use higher order grids such as in [4] instead of the rectangular grid we use in this paper. The higher order grids change the runtime of the algorithm but the approach is the same as with the rectangular grid.

[1]Note that, $G(P)$ lies between 0 and 1 and thus $\log G(P)$ is negative.

1. **Generate** a suitably fine rectangular grid.
2. **For each** line segment l between adjacent grid points
3. **Compute** $|\log m_l|$ using Equation 2
4. **Assign** l a weight equal to $|\log m_l|$
5. **Endfor**
6. **Add** a link from virtual point a to each grid point on the west
7. **Add** a link from virtual point b to each grid point on the east
8. **Assign** a weight of 0 to all the line segments from a and b
9. **Compute** the least weight path P from a to b using Dijkstra's algorithm
10. **Let** w equal the total weight of P.
11. **Return** P as the least exposure path with an exposure equal to 10^{-w}.

Figure 2: Pseudo-code of the proposed solution for the UT problem.

On this grid, consider two adjacent points, say v_1 and v_2. Let l denote the line segment between v_1 and v_2. Also let m_l denote the probability of not detecting a target traveling between v_1 and v_2 on the line segment l. Then, from the discussion above,

$$\log m_l = \int_{u \in l} \log(1 - D(u)) du, \tag{2}$$

where $D(u)$ is either $D_v(u)$ or $D_d(u)$ depending on whether the sensors are using value or decision fusion. Note that, m_l lies between 0 and 1 and, therefore, $\log m_l$ is negative. Assign a non-negative weight equal to $|\log m_l|$ to each such segment l on this grid. Also, create a fictitious point a and add a line segment from a to each grid point on the west periphery of the sensor field. Assign a weight equal to 0 for each of these line segments. Similarly, create a fictitious point b and add a line segment from b to each grid point on the east periphery of the sensor field. Assign a weight equal to 0 for each of these line segments.

The problem of finding the least exposure path from west periphery to east periphery is then equivalent to the problem of finding the least weight path from a to b on this grid. Such a path can be efficiently determined using the Dijkstra's shortest path algorithm [8]. A pseudo-code of the overall algorithm is shown in Figure 2.

Example: Figure 3 shows a sensor field with eight sensors at locations marked by dark circles. Assume the noise process at each sensor is Additive White Gaussian with mean 0 and variance 1. Further assume that the sensors use value fusion to arrive at a consensus decision. Then, from Equation 1, we chose a threshold $\eta = 3.0$ to achieve a false alarm probability of 0.187%. The field has been divided into a 10×10 grid. The target emits an energy $K = 12$ and the energy decay factor is 2. The figure shows the weight assigned to each line segment in the grid as described above. The least exposure path found by the Dijkstra's algorithm for this weighted grid

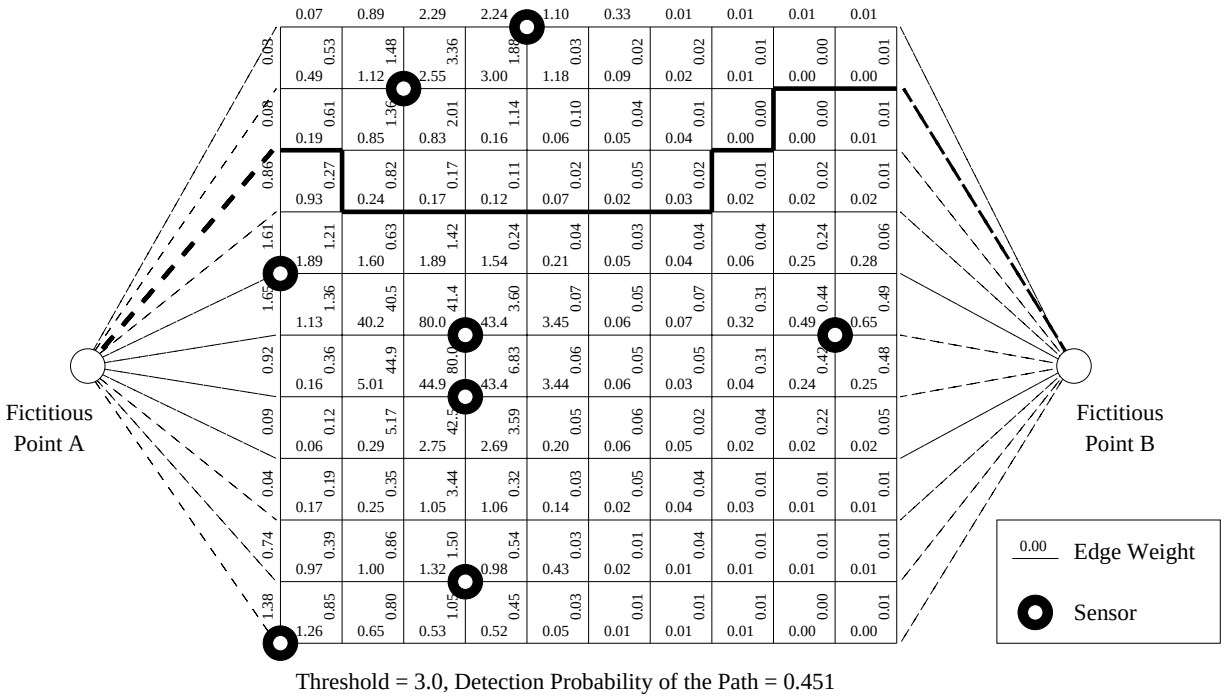


Figure 3: Illustration of the proposed solution for an example UT problem.

is highlighted. The probability of detecting the target traversing the field using the highlighted path is 0.451.

3.2 UM Problem

Let P denote a path from a point in the field periphery to a point x in the red zone. Let $R(P)$ denote the portion of the path inside the red zone and let $Y(P)$ denote the portion of the path outside the red zone. Let $|R(P)|$ denote the length of $R(P)$. If the intruder moves with velocity v, then the intruder will require $|R(P)|/v$ time units to travel to x inside the red zone. Since the same amount of time will be required in the red zone while exiting the field, the intruder must spend $t = (T - 2 \cdot |R(P)|/v)$ at point x. Let $H(P)$ denote the probability of not detecting an intruder who enters and exits using P and spends t time units at point x. The exposure then is $(1 - H(P))$. The problem is to find a point x in the red zone and an associated path with the least $(1 - H(P))$ or equivalently with the least $|\log H(P)|$.

As in the case of the UT problem, we do not exactly compute the path P that minimizes $|\log H(P)|$. Instead, we approximate by dividing the field into a fine grid and assume that the intruder only moves along the line segments on this grid. Also, similar to the solution for the UT problem let m_l denote the probability of not detecting an intruder moving over a line segment l

1. **Generate** a suitably fine rectangular grid.
2. **For each** line segment l between adjacent grid points
3. **Compute** $|\log m_l|$ using Equation 2
4. **Assign** l a weight equal to $|\log m_l|$
5. **Endfor**
6. **For each** point x in the red zone
7. **Determine** least weight path P_x from x to the periphery using Dijkstra's algorithm.
8. **Let** w_x denote the total weight of P_x.
9. **If** $w_x <$ min_wx
10. min_x $= x$
11. min_wx $= w_x$
12. min_Px $= P_x$
13. **Endif**
14. **Endfor**
15. **Return** min_Px as the least exposure path with exposure equal to $10^{-\text{min\_wx}}$

Figure 4: Pseudo-code of the proposed solution for the UM problem.

on this grid. Then,

$$\log H(P) = 2 \sum_{l \in P} \log m_l + (T - 2 \cdot |R(P)|/v) \cdot \log(1 - D(x))$$

Note that, this expression is specific to the point x in the red zone. The problem is to find the point x and the associated path P_x from a suitable point in the periphery to x that results in the least exposure.

The algorithm to find path P which minimizes $|\log H(P)|$ is as follows. For each point x in the red zone determine the least weight path P_x to the field periphery using the Dijkstra's algorithm [8]. Given x and P_x one can compute $|\log H(P_x)|$. The desired least exposure path is obtained by choosing x in the red zone and the associated path P_x that minimizes $|\log H(P_x)|$. A pseudo-code of the overall algorithm is shown in Figure 4.

Example: Figure 5 shows a sensor field with eight sensors protecting an asset. The red zone is shaded. The noise process at each sensor is Additive White Gaussian with mean 0 and variance 1. Further assume that the sensors use value fusion to arrive at a consensus decision. Then, from Equation 1, we chose a threshold $\eta = 3.5$ to achieve a false alarm probability of 0.03%. The field has been divided into a 10×10 grid. The intruder emits energy $K = 12$ and the energy decay factor is 2. The figure shows the weight assigned to each line segment in the grid as described above. A least exposure path for the UM problem is highlighted. The probability of detecting an intruder who uses this path for unauthorized monitoring by spending 10 time units in the red zone is 0.677.

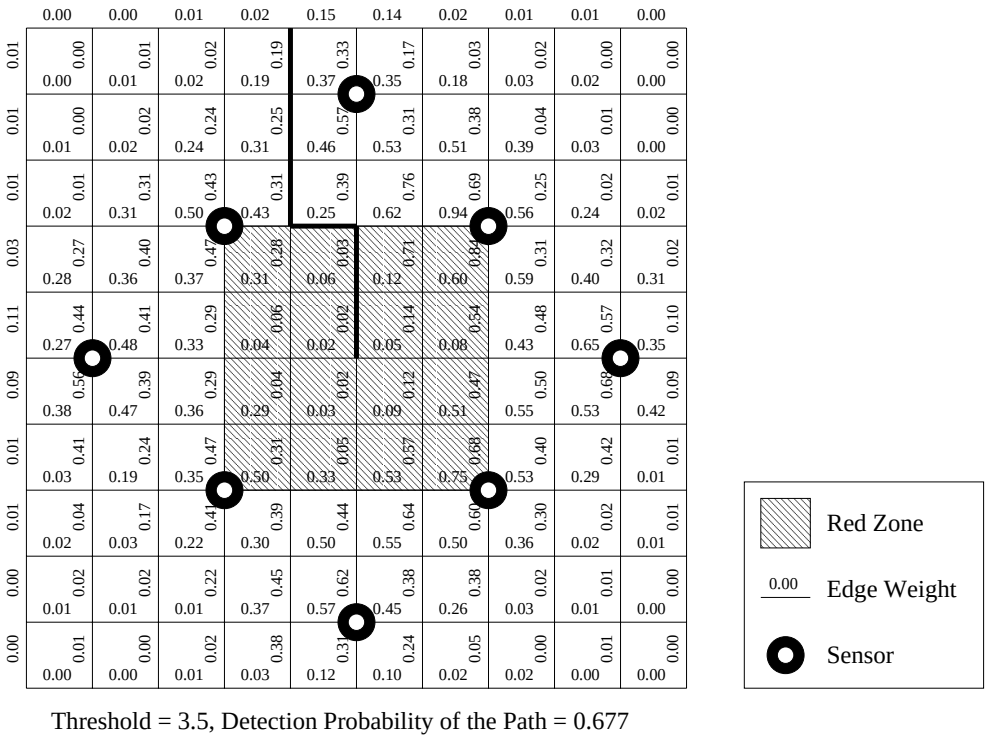


Figure 5: Illustration of the proposed solution for an example UM problem.

4 Tradeoff Between Exposure and False Alarm

The tolerable false alarm probability determines the detection threshold(s) which in turn, determines the exposure. As threshold increases, the false alarm probability decreases because the likelihood of noise energy exceeding the threshold decreases. Similarly, as the threshold increases, the total energy needed to detected an existing target is larger, and therefore, the probability of detecting a target decreases. Hence, the exposure also decreases with threshold.

In a good sensor deployment, the false alarm probability should be as small as possible. At the same time, the probability of detecting a target/intruder on the least exposure path should be as large as possible. Based on the above discussion these two requirements are in conflict with each other. That is, one must select a threshold that makes a good compromise between exposure and false alarm probability.

The tradeoff between exposure and false alarm probability is illustrated in Figures 6 and 7. The two curves in Figure 6 show the false alarm probability and the probability of detecting the target on the least exposure path as function of threshold for the UT problem. Similar curves for the UM problem are shown in Figure 7. The results are for the sensor deployments shown in Figures 1(a) and 1(b), respectively. The noise process at each sensor is Additive White Gaussian

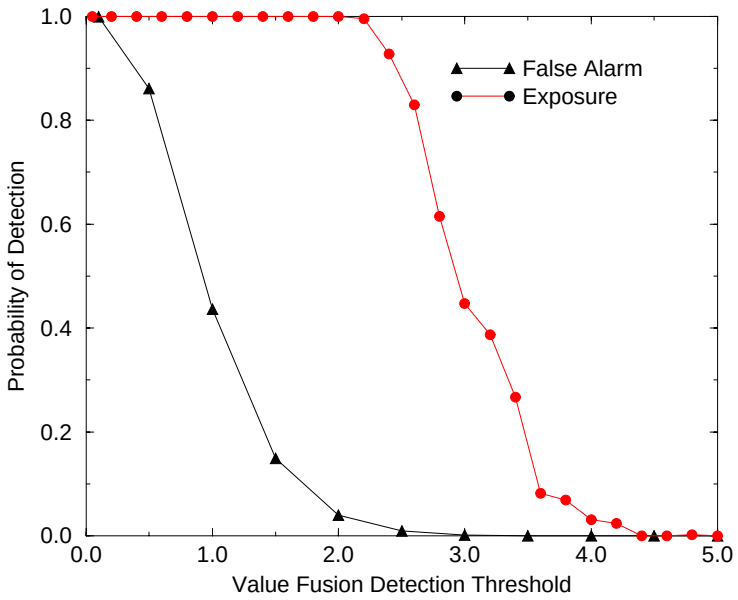


Figure 6: Tradeoff between exposure and false alarm in UT problem.

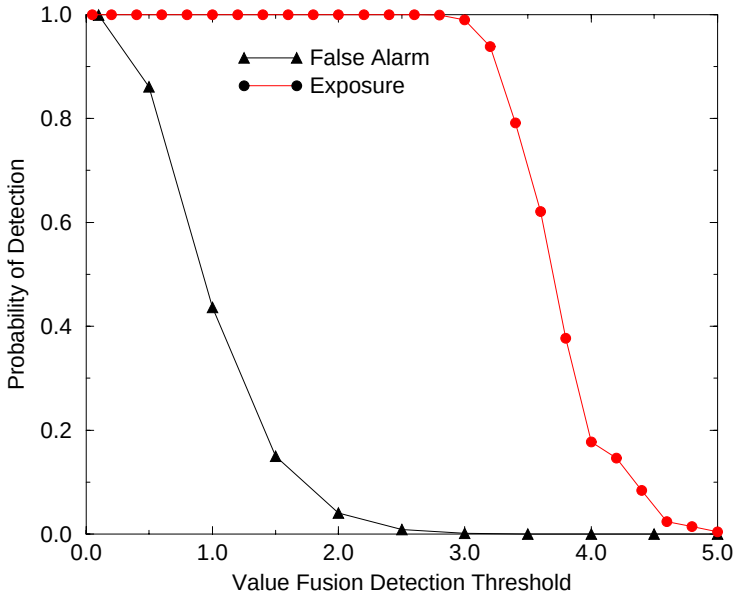


Figure 7: Tradeoff between exposure and false alarm in UM problem.

with mean 0 and variance 1. The noise process at the sensors are independent. The target and the intruder emit an energy $K = 12$ and the energy decay factor is 2. For each value of the threshold, the least exposure path is computed using the algorithms proposed in Section 3 using a 10×10 rectangular grid. The sensors use value fusion for arriving at the consensus decision. For Figure 7(b) the intruder spends 10 time units inside the red zone.

As expected, the false alarm probability and the probability of detection in the least exposure path decrease with threshold for both problems; demonstrating that the threshold must be carefully chosen to reach a good compromise between false alarm and exposure. For the scenarios corresponding to the figures, threshold values less than 2.0 result in unacceptably large false alarm probabilities while values greater than 4.0 leave the sensor field almost open to unauthorized traversal/monitoring. Threshold values between 2.0 and 4.0 seem to offer a good compromise; the exact value must be chosen based on the application.

5 Summary

In this paper, we considered two problems in wireless ad hoc sensor networks, namely unauthorized traversal and unauthorized monitoring. For both problems, we use probability of detecting a target carrying out the corresponding unauthorized activity as the measure of goodness of the deployment. We believe that this measure is better than the ones in literature. In addition to being more intuitive, this measure allows one to account for the presence of noise in sensor readings.

In the presence of noise, the paper shows that there is a tradeoff between probability of false alarm and the probability of detecting a target carrying out an unauthorized activity. The paper analytically characterizes this tradeoff and develops algorithms to find the most vulnerable paths for the unauthorized activity.

References

[1] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *Communications of the ACM*, vol. 43, pp. 51–66, May 2000.

[2] "DARPA SensIT Program." http://dtsn.darpa.mil/ixo/sensit.html.

[3] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava, "Coverage problems in wireless ad-hoc sensor networks," in *Proceedings of INFOCOM*, pp. 1380–1387, Apr. 2001.

[4] S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak, "Exposure in wireless ad-hoc sensor networks," in *Proceedings of MOBICOM*, pp. 139–150, July 2001.

[5] S. Meguerdichian, S. Slijepcevic, V. Karayan, and M. Potkonjak, "Localized algorithms in wireless ad-hoc networks: Location discovery and Sensor exposure," in *Proceedings of MOBIHOC*, pp. 106–116, October 2001.

[6] M. Hata, "Empirical formula for propagation loss in land mobile radio services," *IEEE Transactions on Vehicular Technology*, vol. 29, pp. 317–325, Aug. 1980.

[7] T. Clouqueur, P. Ramanathan, K. K. Saluja, and K.-C. Wang, "Value-fusion versus decision-fusion for fault-tolerance in collaborative target detection in sensor networks," in *Proceedings of Fourth International Conference on Information Fusion*, Aug. 2001.

[8] S. Baase and A. V. Gelder, *Computer algorithms: Introduction to design and analysis*. Addison-Wesley, 2000.