Blocking Vulnerable Paths of Wireless Sensor Networks

Shu Zhou
The University of New Mexico
Albuquerque, USA

Min-You Wu
Shanghai Jiao Tong University
Shanghai, China

Wei Shu
The University of New Mexico
Albuquerque, USA

***Abstract*— In this work, we study the topology enhancement problem of wireless sensor networks. Our research focuses on reducing the path-based vulnerability. The objective is to get as much information as possible for any target moving out of the surveillance area. We study intelligent targets that have the knowledge of existing sensor distribution. Under such assumption, we find the vulnerable paths that rational targets would like to take and block these paths to enhance the network detection performance. Simulation shows that by adding only a few numbers of new sensors on specific positions, we can greatly decrease the vulnerability of a randomly deployed sensor network.**

I. INTRODUCTION

Recent advancement in wireless communications and electronics has enabled the development of low-cost wireless sensor networks. It also presents us many new challenging practical and theoretical problems.

In the physical layer, sensor placement models study location of sensors and its impacts on the network. Currently, researches are focused on power consumption, transmission, network coverage, and exposure [9], [8], [7], [14]. Several models [3], [4], [11], [15], [16], [17] were proposed in recent years, to adjust sensor distribution, in order to get better network performances.

Three metrics are frequently used in these researches: *coverage*, *detection probability* and *exposure*.

Coverage is the measurement of how much of the surveillance area is under the detection of sensors. It is generally based on the 0-1 detection model. Detection probability is similar to coverage, but based on a more accurate model.

Exposure is a special path-based metric [8], [9], [14]. It focuses on the sensor field intensity along paths. Unlike coverage and detection probability, which are more suitable for discrete and independent events, exposure works best in a mobile target detection scenario.

In a path-based sensing model, the path of a target is essential to the sensor network performance. If a target is intelligent, and has the knowledge of existing sensor distribution (we call it rational target), it will move along the path that has a minimum exposure [9], [8], [7]. Otherwise, its moving trace should be random walks. In the first scenario, the selected minimum exposure paths expose the vulnerability of the sensor network.

Most previous researches on exposure only studied how to calculate, or how to use the path. A few works have touched the area of fixing it. However, the path-based rational mobile target detection problem is still wide open.

Above discussions motivate our research on detecting rational mobile targets. As a native path-based metric, exposure is used to measure the network vulnerability. To decrease the exposed vulnerabilities and to prevent mobile targets from escaping, we first find out the most vulnerable paths using Voronoi diagram [1] and Dijkstra's [2] shortest path algorithm. Additional sensors are deployed to blocking these paths. Data show that by deploying only a small number of additional sensors, we can greatly decrease the vulnerability of network.

The remainder of this paper is organized as follows. We define the problem in Section II. Section III presents our framework and algorithms. Simulation and case studies are presented in Section IV. Section V lists related works. Finally, we conclude this paper in Section VI.

II. PROBLEM DEFINITION

In this work, we use the Euclidean plane to model the surveillance area. An edge between two points x and y is defined as a straight line connecting them together, denoted by e_{xy}. A path P_{ab} is defined as a sequence of edges connected one by one from point a to point b.

Define the distance from a sensor s_i to a point x as $d(i,x)$, and the sensing ability of s_i at x as $m(i,x)$. $m(i,x)$ generally diminishes as $d(i,x)$ increases. The specific function of $m(i,x)$ depends on the type of s_i.

$$m(i,x) = \frac{\alpha}{d(i,x)^k} \tag{1}$$

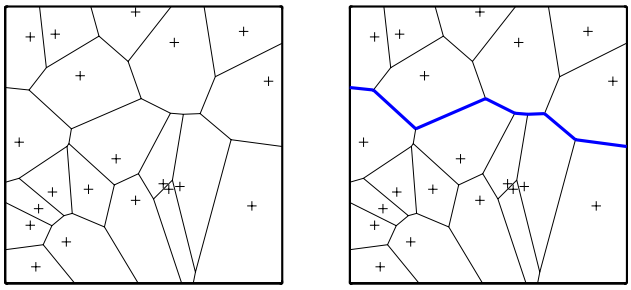
where α is a manufactory-dependent parameter, and k depends on the communication scenarios. Generally, $k \in (2,4)$. From this equation, the further a target is away from a sensor, the less likely it could be detected.

Based on this detection model, a rational target attempts to find a path that is far away from sensors as much as possible. We call this path the *Most Vulnerable Path (MVP)*. *Voronoi Diagram (VD)* and Dijkstra's shortest path algorithm are used as tools to find this path and calculate it vulnerability.

By *VD*'s definition, for each sensor s_i in a given sensor set S, a boundary enclosing all the intermediate points lying closer to s_i than to other sensors is called a *Voronoi Polygon (VP)*, and the set of all *VP* is called a Voronoi Diagram.

For any point on an edge of a *VD*, the distance to the nearest sensor is maximized. Figure 1(a) demonstrates this property,

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.



(a) A Voronoi Diagram **(b)** The Most Vulnerable Path

Fig. 1. Voronoi Diagram and the Most Vulnerable Path

where plus signs and lines denote the sensors and edges of *VD*, respectively.

The vulnerability is a measurement of the unawareness of the sensor network when a target is sneaking along some path. By definition, *MVP* exposed the most vulnerability among all possible paths.

The goal of this anti rational target research is to block the most vulnerable paths. We define the problem as:

Given a randomly deployed sensor network,

1) *find the most vulnerable paths that a rational mobile target would take to sneak out of the surveillance area.*
2) *find the best locations to place additional sensors, subject to minimize the network vulnerability.*

III. METHODOLOGY

A. Exposure

In this work, we use *exposure* to measure vulnerability. By definition, exposure is the measurement of the sensor field intensity at a certain point or along a path.

Denoted as $I_A(x)$, the sensor field intensity at point x is defined as:

$$I_A(x) = \sum_{s_i \in S} m(i, x) \tag{2}$$

where S denotes the set of existing sensors.

From Equation (1), sensing ability drops fast when the distance increases, especially for a large k value. Without loosing accuracy, Equation (2) can be simplified by considering only the closest sensors, as shown in Equation (3)

$$I_c(x) = m(j, x) \tag{3}$$

where j denotes the closest sensor s_j to point x.

Based on this definition, we define the exposure of an edge e_{xy} as:

$$R_{xy} = \int_x^y I_c(t)dt \tag{4}$$

And the exposure of a path P_{ab} is:

$$R_{ab} = \sum_{e_{xy} \in P_{ab}} R_{xy} \tag{5}$$

Apparently, minimum exposure represents maximum vulnerability, because of the minimum sensor field intensity. In the following of this paper, we select the path with minimum exposure as the *MVP*.

B. Rational target's Path

The sneaking path of a rational target is selected to be as far from nearby sensors as possible. Thus, each edge of this path should be an edge of the *VD*. Figure 1(b) draws an ideal path of a rational target that moves horizontally cross the surveillance area. It is plotted by the bold line segments.

An *MVP* between two vertices can be found by using Dijkstra's shortest path algorithm. In this process, *VD* serves as the input graph, and the weight of each edge is calculated by Equation (4). On the other hand, Dijkstra's algorithm cumulates each edge's weight in each step, which also satisfies Equation (5). This ensures a cumulative exposure of an entire path. For an input graph $VD = (V, E)$, an individual single source Dijkstra's shortest path calculation spends $O(|E|log|V|)$ time.

In our research, we want to find out the *MVP* across the surveillance area, i.e., between two parallel borders. So calculating each shortest path between each pair of vertices on the borders could be more efficient than an all-pair Dijkstra's algorithm, which consumes $O(|V|^3)$ time. Buffers can also be introduced to record partial path information.

C. Blocking the Vulnerable Paths

Finding out the *MVP* allows us to know the path that needs to be blocked. However, we do not have large bulk of sensors to jam the whole path. A specific point needs to be identified as the location of a new sensor. We call this point *blocking point (BP)*.

To block a path with fixed end points is trivial. Just putting an additional sensor on the start or end point can totally cancel the existing and future *MVP*. However, for a rational sensor that attempts to cross the surveillance area, the situation is more complicated. It can choose another start or end point along the borders. We propose four *BP* selection algorithms, and compare their performances in Section IV.

Obviously, to maximize the efficiency of new sensors, the *BP* should be chosen from the points along the current *MVP*. From the blocking point of view, deploying a sensor on any point along *MVP* is sufficient. However, the points with extremum sensor field intensity are of special interests to this research. A large intensity value represents a dense sensor distribution, while a small one indicates an uncovered area. As the *Point-based* approach, selecting extremum intensity points as *BP* allows us to emphasize on some special areas.

Edge-based BP selection is another approach. It first selects a particular edge, then deploy a new sensor at the center of this edge.

Combine these two factors together, our four *BP* selection algorithms are: *Best Blocking Effort (BBE)*, *Maximum Side Effect (MSE)*, *Center of Maximum Exposure Edge (CXE)* and *Center of Minimum Exposure Edge (CIE)*.

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

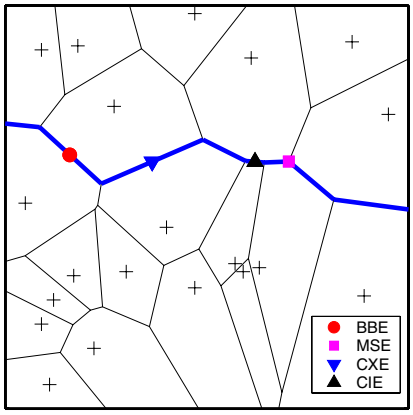


Fig. 2. Demonstration of BP Selection Algorithms

1) BBE: In this algorithm, we select the position that jams the *MVP* most, in another words, to create an area that has the most dense sensor distribution. From all points along the *MVP*, we choose x with maximum $I_c(x)$ in Equation (3) as BP. It is an extreme approach focusing on local maximum, with minimum side effect on other areas.

2) MSE: If we consider blocking not only the current, but also the next potential *MVP*, the *BP*'s location should allow the new sensor to cover sparse area as much as possible. On the contrary to *BBE*, BP is the point x with minimum $I_c(x)$. It is a method that focuses on the global performance.

3) CXE: Among all edges in the *MVP*, *CXE* selects the center of e_{xy} with maximum exposure R_{xy} in Equation (4) as *BP*. Similar to *BBE*, *CXE* is also an algorithm that targets on thoroughly blocking a path by jam the most exposed edge.

4) CIE: On the contrary to *CXE*, *CIE* selects the center of edge e_{xy} with minimum exposure R_{xy} as *BP*. An edge with small exposure is a weak link in the sensor network. It can be used by multiple *MVP*. Putting an additional sensor there can potentially block multiple *MVP*.

Figure 2 demonstrates these four approaches, where the plus sign, solid line and bold line represent the existing sensors, original *VD* edges and original *MVP*, respectively.

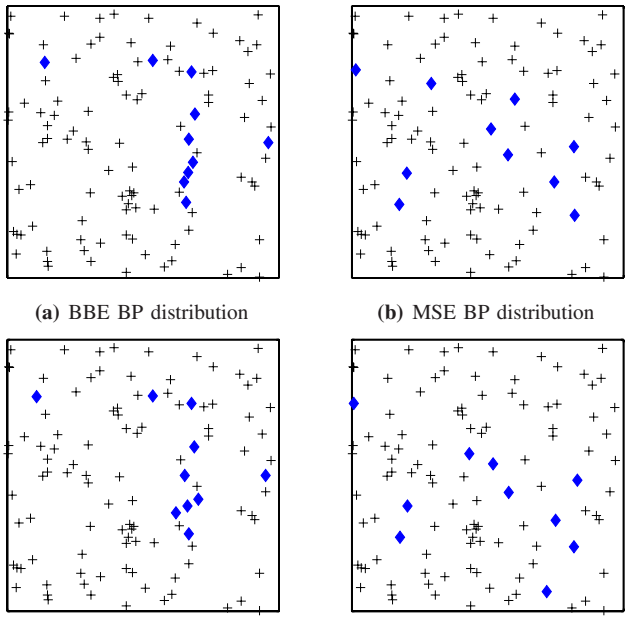
D. New Sensor Deployment

There are two ways to facilitate the calculated *BP*. We can either manually deploy sensors exactly on those spots, or use mobile sensors. The detailed moving scheme is beyond the coverage of this paper. Please refer to works of S. Zhou *et al.* [12] and G. Wang *et al.* [15] for detailed information.

IV. SIMULATION

To test the performance of this work, we simulate a wireless sensor network composed of 100 stationary sensors. They are randomly deployed in a square region A, following uniform distribution. In the sensing model, we select $\alpha = 1$ and $k = 2$.

To simulate different paths of the rational targets, we design two test cases: *Escaping* and *Crossing*. In escaping case, the target tries to go out of the surveillance area from the center. It can escape by any direction. In crossing case, it crosses the surveillance area from one border to the parallel one. We do not know whether it is moving horizontally or vertically. So we calculate two *MVP*, one for each direction.



(a) BBE BP distribution **(b)** MSE BP distribution

(c) CXE BP distribution **(d)** CIE BP distribution

Fig. 3. Blocking Point Distribution in Escaping Scenario

Figure 3 shows a sample distribution of sensors in escaping case, after 10 new sensors are added. Plus signs and large solid diamonds represent original sensors and newly added sensors, respectively. We notice that, *BBE* puts most new sensors on one direction of the escaping path, and blocks that path thoroughly. At the same time, it also consumes too many sensors on one direction and has not enough sensors left to take care of other directions. *CXE* is similar to *BBE*. *MSE*'s performance is much better, where all new sensors are placed in sparse areas. There is hardly any easy path left. *CIE* performances closely to *MSE*.

Figure 4 is the sample of sensor distribution in crossing case. The result is similar to that of escaping case.

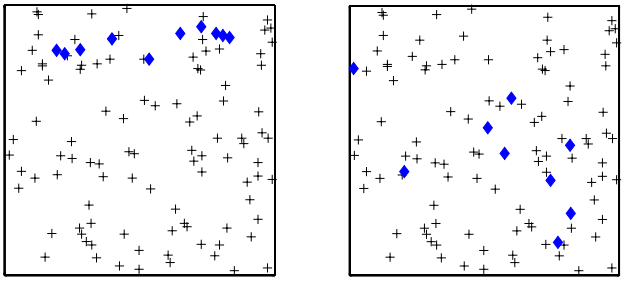
For more accurate numerical results, we generate 10 randomly deployed sensor networks, using the same setting as described in the beginning of this section. All following test results are averaged over these 10 testbeds.

Figure 5 plots the performances of our algorithms in escaping case. It further proves the result of Figure 3. Four *BP* selection algorithms are notably divided into two groups. *MSE* and *CIE* remarkably outperform *BBE* and *CXE*, especially when the number of additional sensors increase.

Figure 6 plots the performances in crossing case. No matter the average or the minimum exposure of horizontal and vertical *MVP*, *MSE* and *CIE* again have better performances than the other two. Same as Figure 5, *MSE* performs best.

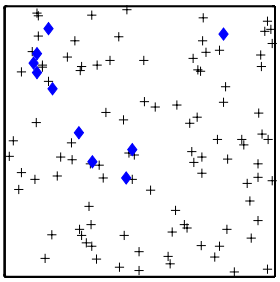
Together with Figure 4, the results of crossing case confirm the results of escaping case. We can also conclude that, *minimum extremum* based approaches outperform *maximum extremum* based approaches.

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.

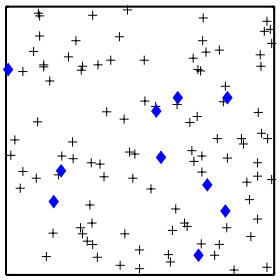


(a) BBE BP distribution

(b) MSE BP distribution



(c) CXE BP distribution



(d) CIE BP distribution

Fig. 4. Blocking Point Distribution in Crossing Scenario

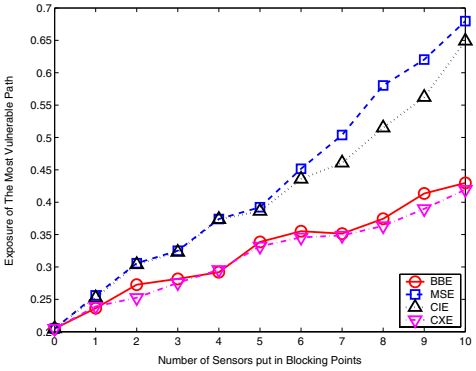
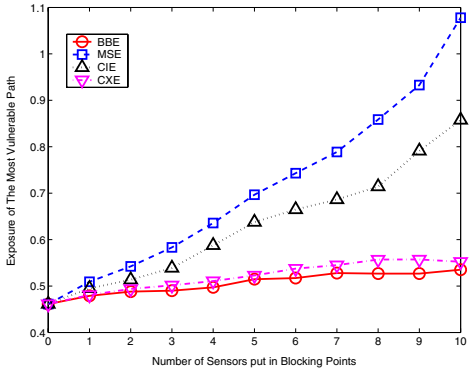


Fig. 5. Performance In Escaping Scenario

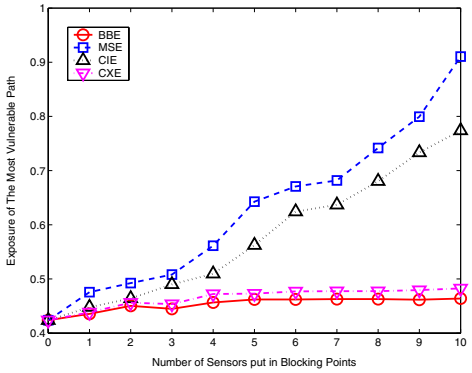
The major difference between this work and traditional coverage problem is that, the targets are rational. They know how to avoid existing sensors. Here we present tests on the performance of coverage-based sensor deployment on this rational targets detecting scenario. Same as the tests discussed above, we consider both escaping and crossing cases. The results are averaged over 10 test cases.

Figure 7 compares the performance of coverage-based approach with our *BP*-selection algorithms. Obviously, it cannot handle rational targets properly. In escaping case, rational mobile targets can escape from any direction, so the coverage-based sensor deployment can hardly block all potential sneaking paths. Thus the line of coverage-based algorithm in Figure 7 (a) lies in the bottom. We consider both horizontal and vertical path in crossing case. Under this condition, coverage-based approach performs closely to *BBE* and *CXE*, as shown in Figure 7 (b) and (c). However, it is still not comparable to *MSE* and *CIE*.

Summarily, a proper vulnerability blocking approach can



(a) Average Exposure of Horizontal and Vertical MVP



(b) Minimum Exposure of Horizontal and Vertical MVP

Fig. 6. Performances in Crossing Scenario

perform well in both escaping and crossing cases. The algorithms selecting minimum intensity locations as *BP* are better than those selecting maximum intensity. In this work, *MSE* has the best performance in both cases. It takes care of both current and potential *MVP*, and deploys sensors on the most needed spots.

Comparison with coverage-based approach further proves the necessity of path-based method for detecting rational mobile targets.

V. RELATED WORK

Early researches on sensor placement are for metric measurements. S. Meguerdichian *et al.* [9], [8] studied exposure. G. Veltri *et al.* [14] discussed the minimal and maximal exposure path.

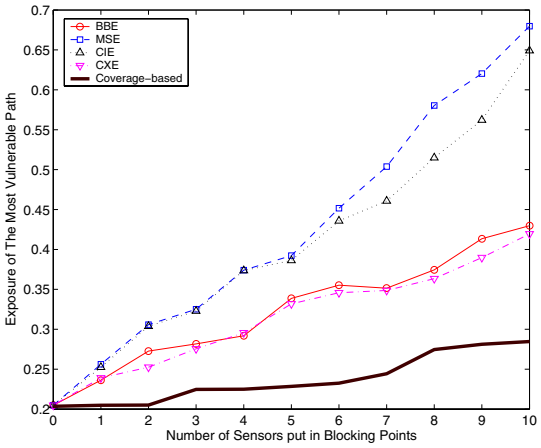
Soon, researches expanded to a much broader scope, studying the relationship between placement and other network metrics, such as power consumption [13], network lifetime [5] and communication channel [10], etc.

Researchers also worked on adjusting the existing sensor placement. S. Meguerdichian *et al.* [7] mentioned the path blocking on a path with fixed end points. B. Liu *et al.* [6] discussed the improvement on coverage by introducing mobility.

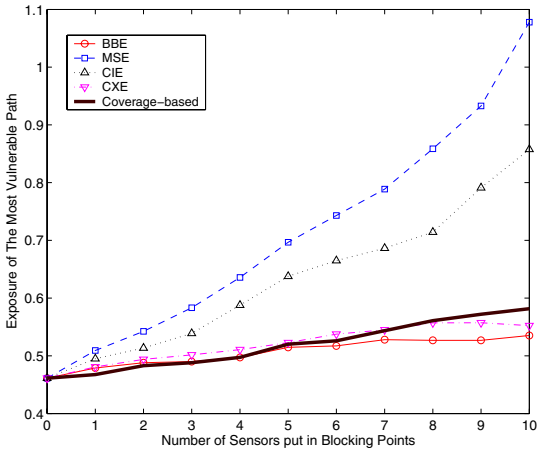
VI. CONCLUSION AND FUTURE WORK

This work presents a new method of decreasing sensor network vulnerability. We use exposure as the metric to

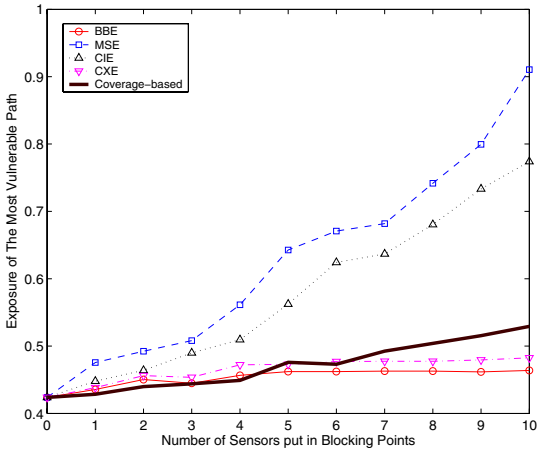
1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.



(a) Exposure of MVP (Escaping)



(b) Average Exposure of Horizontal and Vertical MVP (Crossing)



(c) Minimum Exposure of Horizontal and Vertical MVP (Crossing)

Fig. 7. Performances of Coverage-based Sensor Deployment

represent network vulnerability, and find out the paths that expose it mostly. We select a few points from the most vulnerable paths and place additional sensors there to block them. Several blocking point selection algorithms are studied. Simulation results in both escaping and crossing cases demonstrate a significant exposure increase. It is the first work that concentrates on path-based rational mobile targets detection and sensor network vulnerability.

This research also points out new topics on the path-based network topology study, such as the relationship between exposure and coverage, detection probability, exposure's impact on irrational targets, etc. A probability-based exposure should also be able to provide more accurate results on these topics.

Acknowledgments

This research was supported partially by Natural Science Foundation of China grant # 60573138.

REFERENCES

[1] F. Aurenhammer. Voronoi diagrams - a survey of a fundamental geometric data structure. *ACM Computing Surveys*, 23(3):345–405, September 1999.

[2] E. W. Dijkstra. A note on two problems in connection with graphs. In *Numerische Math. 1*, pages 269–271, 1959.

[3] D. K. Goldenberg, J. Lin, and A. S. Morse. Towards mobility as a network control primitive. In *The Fifth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '04)*, pages 163–174, May 2004.

[4] A. Howard, M. J. Mataric, and G. S. Sukhatme. Mobile sensor network deployment using potential fields: A distributed scalable solution to the area coverage problem. In *the 6th International Conference on Distributed Autonomous Robotic Systems (DARS 02)*, pages 299–308, June 2002.

[5] E. Jain and Q. Liang. Sensor placement and lifetime of wireless sensor networks: Theory and performance analysis. In *IEEE Globecom 2005*, November 2005.

[6] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley. Mobility improves coverage of sensor networks. In *ACM MobiHoc 2005*, May 2005.

[7] S. Megerian, F. Koushanfar, M. Potkonjak, and M. Srivastava. Worst and best-case coverage in sensor networks. *IEEE Transactions on Mobile Computing*, 4(1):84–91, December 2004.

[8] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. Srivastava. Coverage problems in wireless ad-hoc sensor networks. In *IEEE InfoCom 2001*, April 2001.

[9] S. Meguerdichian, F. Koushanfar, G. Qu, and M. Potkonjak. Exposure in wireless ad-hoc sensor networks. In *ACM Mobile Computing and Networking*, July 2001.

[10] D. Miorandi and E. Altman. Coverage and connectivity of ad hoc networks in presence of channel randomness. In *IEEE InfoCom 2005*, March 2005.

[11] S. Zhou, M-Y. Wu and W. Shu. Finding optimal placements for mobile sensors: Wireless sensor network topology adjustment. In *IEEE 6th CAS Symposium on Emerging Technologies*, May 2004.

[12] S. Zhou, M-Y. Wu and W. Shu. Terrain-constrained mobile sensor networks. In *IEEE Globecom 2005*, November 2005.

[13] T. Shu, M. Krunz, and S. Vrudhula. Power balanced coverage-time optimization for clustered wireless sensor networks. In *ACM MobiHoc 2005*, May 2005.

[14] G. Veltri, Q. Huang, G. Qu, and M. Potkonjak. Minimal and maximal exposure path algorithms for wireless embedded sensor networks. In *1st ACM International Conference on Embedded Networked Sensor Systems*, November 2003.

[15] G. Wang, G. Cao, and T. L. Porta. A bidding protocol for deploying mobile sensors. In *11th IEEE International Conference on Network Protocols*, November 2003.

[16] G. Wang, G. Cao, and T. L. Porta. Movement-assisted sensor deployment. In *IEEE InfoCom 2004*, March 2004.

[17] Y. Zou and K. Chakrabarty. Sensor deployment and target localization based on virtual forces. In *IEEE InfoCom 2003*, April 2003.

1-4244-0357-X/06/$20.00 ©2006 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2006 proceedings.