This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

Optimizing Sensor Communication Exposure in Target Detection Applications

Zhengzheng Xu[†], Jia-liang Lu[† ‡], Min-You Wu[†], Charles-Francois Curis[‡], Wei Shu[♯]

[†]Dept. of Computer Science & Engineering, Shanghai JiaoTong University, Shanghai, China
[‡]CITI Lab, INSA Lyon, University of Lyon, France
[♯]Dept. of Electrical & Computer Engineering, University of New Mexico, USA
[†]{zhengzheng,jialiang.lu, mwu}@sjtu.edu.cn, [‡]charles-francois.curis@insa-lyon.fr, [♯]shu@ece.unm.edu

***Abstract*—In a target detection application, rational adversary targets that are conscious of the deployed location of sensor nodes are capable of planning a path in order to avoid being detected by sensor nodes. Probing sensor communication is one of the means that are used by adversary targets to get the necessary information. Therefore, this paper investigates how to reduce the sensor communication exposure. We introduce target bypassing routing methods applied to omnidirectional and directional sensor communication models to achieve the goal of reducing the possibilities for targets to probe the sensor communication. The simulation results show that our bypassing methods can decrease the possibility of communication exposure to a large extent. We also implement a prototype system with Iris motes to verify our solution.**

I. Introduction

Target detection applications built on Wireless Sensor Networks (WSNs) are envisioned to ensure real-time detection of adversary targets. The role of the WSNs is to detect and report potential targets and suspect events that can pose a threat on deployed field. Most existing researches emphasize the intelligence of sensors and have developed different mechanisms to promote detection and monitoring abilities of WSNs. Huang et al. discussed the coverage problem in wireless sensor networks with 2D and 3D models [1]. Kumar et al. [2] discussed barrier coverage problem, in which sensor nodes cooperatively form a barrier of the surveillance area to detect targets.

In [3], mobile targets are categorized into two classes: free linear-moving targets and rational targets. Unlike free linear-moving targets, rational targets are able to collect information of sensors such as sensor placement. Such information can be utilized to design an optimal path to maximize the distance from sensors and minimize the chances of being detected [4]. To our best knowledge, there are two approaches for sensor network to deal with rational targets. The first one is to identify critical positions and add a few sensors to enhance the coverage [3]. The second one as we introduce in this work is to reduce the sensor exposure so as to prevent rational targets from getting necessary information for planning smart paths. Works on geographic routing [5], [6] have investigate bypassing techniques, but they can not be used to optimize sensor exposure. The most important reason is that their communication model is edge-based. However, in sensor communication exposure problem, a sensor exposes when its communication signal is captured by a target. Therefore, the radiation pattern cannot be simply modeled as an edge.

We develop Target Bypass Routing(TBPR) for both omnidirectional and directional communication models. For omnidirectional model, we adopt a radius assignment scheme to reduce communication exposure in multi-hop routing. For directional model, a Virtual Potential Field (VPF) method is used to orient the directional communication and minimize exposure to the targets.

The rest of the paper is organized as follows: Section II formulates the SCE problem and categorizes the problem into omnidirectional and directional communication models. In Section III, we propose a radius assignment based TBPR and set up an experimental test-bed with Iris Motes using omnidirectional communication. Section IV proposes orientation assignment based TBPR using directional communication. Both TBPRs are evaluated in Section V.

II. Sensor Communication Exposure Problem

Two sensor communication models are defined–one for sensors with omnidirectional antenna and the other for sensors with directional antenna, and both are considered as 2-D communication models.

In the omnidirectional communication model, the communication area of a sensor node can be represented as a circular range denoted by a 2-tuple (X_i, r). Here X_i denotes the location of the sensor node n_i and r is the maximum communication radius. A communication link exists for node pair (n_i, n_j) if $\|n_i - n_j\| \leq r$.

In the directional communication model, we assume that the antenna of sensors is featured by adjustable orientation and fixed beam-width which is supported by beam-forming technique [7]. Communication area is modeled as a sector denoted by a 4-tuple $(X_i, r, \mathcal{K}, \Theta)$. $\mathcal{K}$, which varies from $[0, 2\pi)$, is the adjustable orientation vector, and Θ represents the beam-width (beam angle). The directional antenna radiates at $\left[\mathcal{K} - \frac{\Theta}{2}, \mathcal{K} + \frac{\Theta}{2}\right]$.

The *Exposure Area* $EA(n_s)$ of each one-hop sensor communication from n_s to n_d is defined as the point set covered by the communication area from n_s in a given communication model. Given multi-hop sensor communication from node n_s to node n_d via path $P = \{n_s, ..., n_j, ..., n_d\}$, *Exposure Area*

978-1-61284-233-2/11/$26.00 ©2011 IEEE

$EA(n_s, n_d)$ is the union of the exposure areas caused by all one-hop sensor communication on the path:

$$EA(n_s, n_d) = \bigcup_{n_j \in P, n_j \neq n_d} EA(n_j). \quad (1)$$

A rational target possesses probing ability to capture communication among sensor nodes and perceive their existence. We denote $U_T(L_j)$ as the target T's probing intensity at L_j:

$$U_T(L_j) = k_T \cdot |L_j - L_T|^{\alpha}. \quad (2)$$

where k_T is a constant proportional to the probing ability of the rational target, $|L_j - L_T|$ denotes the distance from the location L_j to the target, and $\alpha \in [-1, -4]$ depends on the radio channel model. For multiple targets, $T_1, T_2, ...$, $\Theta_{\{T\}}(L_j)$ is the sum of probing intensity of all targets:

$$\Theta_{\{T\}}(L_j) = \sum_{T \in \{T_1, T_2, ...\}} U_T(L_j). \quad (3)$$

The exposure of sensor communication (n_s, n_d) is measured by the maximum probing intensity $\Theta_{\{T\}}(h)$ on point h, where $h \in EA(n_s, n_d)$, which is denoted as $\psi(n_s, n_d)$:

$$\psi_{\{T\}}(n_s, n_d) = \text{MAX}(\Theta_{\{T\}}(EA(n_s, n_d))). \quad (4)$$

According to (2), it is obvious that the possibility of communication exposure is inversely proportional to the distance to adversary targets. However, in practice sensor communication is also subject to other constraints, such as path length and power consumption. To this end, we incorporate the concern of path length and power consumption in SCE problem.

For any message routing algorithm Y in WSNs, we define a normalized metric $\xi_Y(n_s, n_d)$ for path length from n_s to n_d:

$$\xi_Y(n_s, n_d) = \frac{\text{PL}_Y(n_s, n_d)}{\text{PL}_{\text{GR}}(n_s, n_d)} \quad (5)$$

$\text{PL}_X(n_s, n_d)$ represents the number of hops in the routing path when routing algorithm X is applied. $\text{PL}_{\text{GR}}(n_s, n_d)$ is a baseline metric representing the hops of a geographic routing path from node n_s to n_d without considering the targets. The metric $\xi_Y(n_s, n_d)$ hence describes the additional cost on routing path due to the optimization on sensor communication exposure. If there is no rational target in a WSN, $\xi_Y(n_s, n_d)$ will be a unit. Otherwise, it is greater than one.

The power consumption of a one-hop communication from node n_s is characterized by the radiation power of the transmitter: $P(n_s)$, which is proportional to the square of the radiation radius. For any routing algorithm Y in WSNs, the power consumption is the sum of the transmission powers for every one-hop communication n_s to n_d as $E_Y(n_s, n_d)$:

$$E_Y(n_s, n_d) = \sum_{n_j \in P, n_j \neq n_d} P(n_j) \quad (6)$$

DEFINITION 1: (**SCE Problem**): For a wireless sensor network, given a set of targets, find out a routing algorithm Y to route messages from n_s to n_d as to minimize exposure $\psi_{\{I\}}(n_s, n_d)$ while optimizing $\xi_Y(n_s, n_d)$ and $E_Y(n_s, n_d)$.

As for omnidirectional communication model, a sensor node can only adjust its transmission radius to minimize the exposure. Thus the key concern of SCE problem is to find the next hop node with a radius assignment $\{p_i\}$ for each node i in path $P(n_s, n_d)$. In the directional communication model, the transmission radius is fixed and a sensor node can only vary its antenna's orientation when selecting a next routing node. The SCE can be resolved by providing an orientation assignment $\{\mathcal{K}_i\}$ for each node i in path $P(n_s, n_d)$. In both cases, SCE is a multi-objective optimization problem. We propose two Target Bypass Routing (TBPR) algorithms to solve the SCE problem with omnidirectional communication and directional communication in Sections III and IV, respectively.

III. TBPR FOR OMNIDIRECTIONAL COMMUNICATION

A. Radius Assignment based TBPR

As SCE problem is considered in circumstance where sensor nodes are deployed in adversary environment, a deployed sensor node will generate a local alert once it detects an adversary target. We assume that alerts are multi-broadcast to all of its neighboring sensor nodes between a certain interval. However, the alert broadcast mechanism may bring about an increase of traffic load. To make a trade off, only sensor nodes within two-hop communication range from targets(insecure nodes) are notified with the alerts while other sensor nodes outside that range(secure nodes) are blind to them. To be more specific, insecure nodes will compute according to (3) the probing intensity of targets that either have been detected by itself or reported by neighboring sensors, while secure nodes just keep probing intensity zero.

A threshold φ_U is used as a variable parameter to quantify the probing ability of targets. When a sensor node encounters a routing demand, it compares its current probing intensity with the threshold φ_U. These are two possible cases as a result of the comparison:

1) If current probing intensity is larger than φ_U, the sensor node will select the closest among its neighbors which have smaller probing intensity to forward the message. This transmission is assigned with the minimal necessary communication radius.
2) Otherwise, the sensor node sorts the neighbors by their residual distance to the destination (as in geographic routing). It selects the first qualified node in the list.

Fig. 1 illustrates a multi-hop communication path generated by radius assignment TBPR, which successfully circumvents the regions within intruders' probing capability.

B. Experimental Test

We deploy a testbed with 16 Iris motes [8], one of which acts as a target denoted as $T.1$ and the rest are used to form a WSN as shown in Fig. 2. All Iris motes use 2.4GHz Zigbee omnidirectional antenna with the same transmission power.

Nodes n_0 and n_{12} are selected as source and destination nodes, respectively, of a multi-hop sensor communication. By default, nodes use GPSR [9] geographic routing protocol. Each node records its previous and next hop node. The first part of

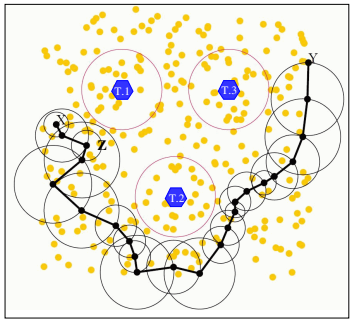


Fig. 1. TBPR path from X to Y in omnidirectional communication model

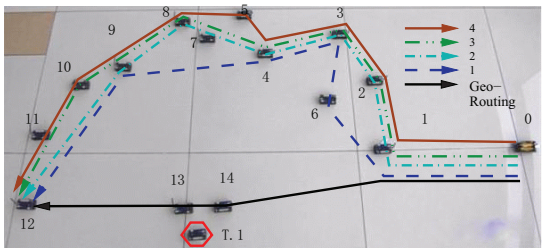


Fig. 2. TBPR directs the message to reduce exposure.

our experiment demonstrates that sensor nodes can effectively choose a path with less exposure. After that, we alter the value of parameter k_T in (2) to study its impact on TBPR's path selection. Without consideration of the presence of target, the message follows the geographic routing and takes the path $\{n_0, n_1, n_{14}, n_{12}\}$ as shown in Fig. 2. When TBPR is applied, message is routed along longer paths in order to meet the security demand.

Furthermore, multiple paths from n_0 to n_{12} (four TBPR paths as shown in Fig. 2) are the results of different values of parameter k_T. Fig. 3 illustrates the TBPR path selection. As k_T varies from 180 to 290, the path length $\xi_{\text{TBPR}}(n_0, n_{12})$ increases. Therefore, we can see an inversely proportional relation between k_T and the necessary path length for bypassing the threatened area.

IV. TBPR for Directional Communication

A. Orientation Assignment based TBPR

Sensor nodes equipped with directional antennas is somewhat different. They are able to adjust the communication beam orientation, which grants them bigger chances to bypass intruders' probing region. In [10], virtual coordinates are used to develop a directional multi-path geographic routing for video communication over restrained bandwidth. Here we use potential field as a tool to solve the SCE problem, which is a commonly used and well understood method in robotics and is often applied for tasks such as navigation [11].

The potential field used here is similar to an electric field. We can imagine that the message currently carried by one of the sensor nodes possesses a positive charge. We let the targets also carry positive charge thus having a repulsive force on the

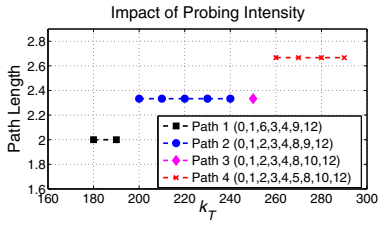


Fig. 3. Relation between probing intensity and path length

message. And we let the sink node have a positive charge which imposes an attractive force on the message. This is consistent with the routing requirement that message should be sent toward the sink node and meanwhile avoid intruders' probing region. Moreover, avoiding loops is also an important consideration in routing. Therefore, we let the last routing node carry a positive charge, which imposes a repulsive force on the message as they carry the same charge. The potential field method can be described as follow. The message is subject to a force that is the gradient of a potential field U.

$$F = -\nabla U \tag{7}$$

The potential field U can be divided into three components: the field $\Theta_{\{T\}}$ due to the targets, the field U_d due to the destination and the field U_s due to the last routing node. These fields generate repulsive forces $F_{\{T\}}$, F_d and attractive force F_s. Thus we have $U = \Theta_{\{T\}} + U_d + U_s$ and $F = F_{\{T\}} + F_d + F_s$.

According to (2), (3) and (7), the force $F_{\{T\}}$ can be rewritten as:

$$F_{\{T\}}(L_j) = \sum -\frac{d(U_T)}{d\vec{x}} = \sum k_T \cdot |r_j|^{\alpha-1} \cdot \frac{\vec{r}_j}{|r_j|} \tag{8}$$

where $r_j = L_j - L_T$, the distance between a certain intruder and the evaluated point.

We formulate U_d and U_s as below and therefore F_d and F_s are forces with constant strength. This is out of the consideration that attractive force from the destination and repulsive force from the last routing node should be constant everywhere. We have

$$U_d(L_j) = k_d \cdot |L_j - L_d| \tag{9}$$

$$U_s(L_j) = k_s \cdot |L_j - L_s| \tag{10}$$

and

$$F_d(L_j) = -\frac{d(U_d)}{d\vec{x}} = -\frac{d(U_d)}{dr_j} \cdot \frac{dr_j}{d\vec{x}} = k_d \cdot \frac{\vec{r}_j}{|r_j|} \tag{11}$$

$$F_s(L_j) = -\frac{d(U_s)}{d\vec{x}} = -\frac{d(U_s)}{dr_j} \cdot \frac{dr_j}{d\vec{x}} = k_s \cdot \frac{\vec{r}_j}{|r_j|} \tag{12}$$

where k_d and k_s are constants representing the attractive intensity on the message and the repulsive intensity respectively. Relative position vector $r_j = L_j - L_d/L_s$ allows sensor nodes

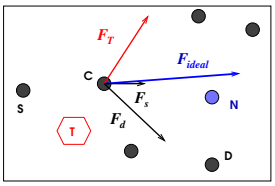


Fig. 4. Computation of ideal orientation. C, current node; S, previous hop node; D, destination node; node N, next hop node.

to compute the force directly without the assistance of global localization system.

An intermediate node in one multi-hop sensor communication computes the F_{ideal} based on $F_{\{T\}}$, F_d and F_s. The direction of F_{ideal} is considered the ideal orientation of the next transmission. Fig. 4 gives an illustration of how F_{ideal} is constituted. Note that for the first communication, the sender does not need to consider the repulsive force F_s from the last routing node. The direction of F_{ideal} optimizes the exposure of communication while still considering both path length and power objectives.

Having obtained the ideal orientation, the current routing node compares its neighbors by the angle between two orientations–the orientation from the current routing node to the neighbor and the ideal orientation. Then we ensure the security of the next routing node candidate by comparing the probing intensity of a candidate $\Theta_{\{T\}}$ with the threshold value φ_U as we do in the radius assignment TBPR. Finally, the current routing node selects a secure routing node with the smallest angle between the two orientations.

Fig. 5 gives an example of TBPR path from node X to Y applying orientation assignment based TBPR. Compared to Fig. 1 with the same configuration, the routing path generated by orientation assignment based TBPR elegantly travels through the three targets without being probed and meanwhile achieving shorter path length.

V. Performance Evaluation

We simulate TBPRs for both omnidirectional and directional communication models and analyze their performance on a variety of network topologies. We also compare the performance of TBPRs with that of geographic routing which has been carefully altered to fit into the adversary settings in our problem definition. The results show that TBPR definitely meets our design goal of minimizing communication exposure while still maintaining high successful delivery ratios.

In order to make geographic routing fit into the adversary scenarios, some changes are made to it:

1) The sensor nodes within the intruders' probing region are excluded from candidates for routing nodes.
2) Prospective routing nodes are checked to ensure that the communication range is not exposed to intruders.

Network topologies containing 300 sensor nodes are randomly generated on a fixed area of sensor field. We set the parameter α in 2 as -1, therefore $U_T(L_j) = k_T \cdot |L_j - L_T|^{-1}$. We assume that the maximum communication range is 0.2 in

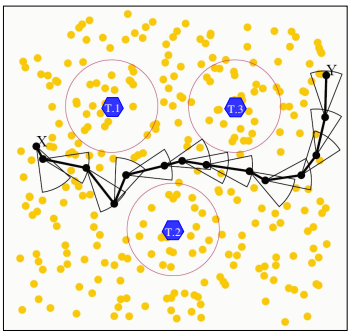


Fig. 5. TBPR path from X to Y in directional communication model

all routing methods. The *Exposure Distance* is related to the probing intensity parameter k_T, which quantifies the intruders' probing ability. In each simulation, every routing method is simulated under the same network configuration and routing demand. Each result is shown with a 95% confidence interval. We study delivery ratio, path length and power consumption under different number and probing ability of targets.

Fig. 6(a) shows that TBPRs achieve overwhelmingly higher successful delivery rate than the modified geographic routing. Moreover, TBPR with smaller beam-width performs better than its counterpart with larger beam-width.

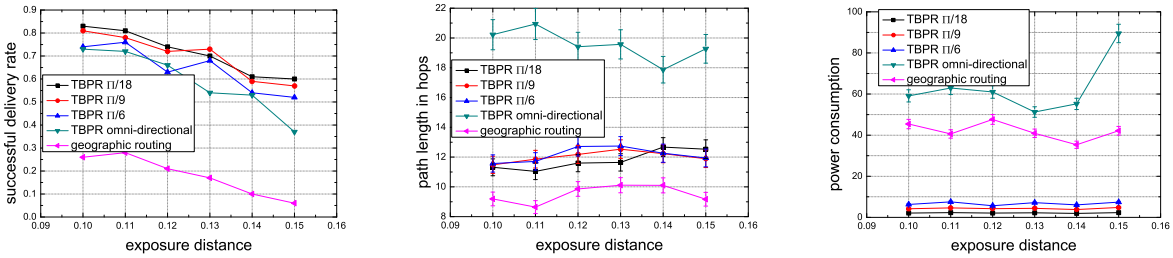
In fig. 6(b) directional TBPR shows great performance in maintaining appropriate path lengths while achieving high successful delivery rate. Omnidirectional TBPR has to extend the path length in order to cautiously bypass intruders. The short path length of geographic routing is chiefly caused by the fact that routing demands with longer path length are often failed and are not taken into statistics.

Fig. 6(c) evaluates and compares the power consumption in those routing scenarios that all routing methods can succeed. It shows that directional TBPR is great power saver with approximately 85% of power saved. Meanwhile, omnidirectional TBPR inevitably consumes more power as cost of bypassing.

Fig. 7(a) shows that directional TBPR is well adaptive to the increase of intruder population, and omnidirectional TBPR also has similar performance in a certain range of intruder population. Moreover, with increased number of targets, TBPRs for both communication model demonstrate better successful delivery rate than geographic routing.

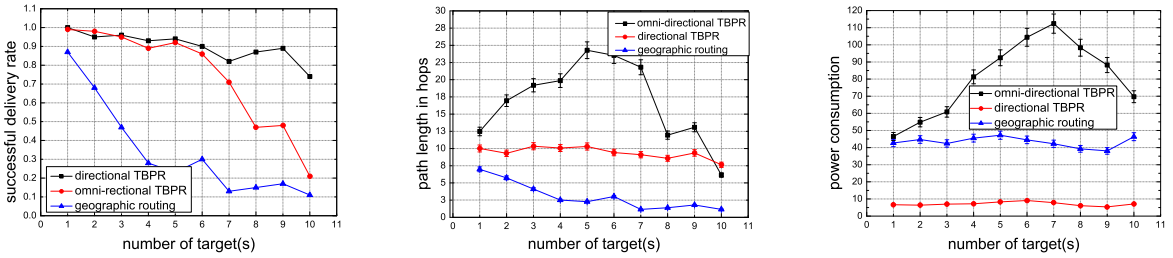
Fig. 7(b) compares the average path length of those successfully-met routing demands. Directional TBPR maintains effective length of routing path with increased intruder population. In omnidirectional TBPR, path length increases before successful delivery rate drops in order to meet the routing demands. Note that the drop of path length for geographic routing does not mean that routing effectiveness is increased, instead it means that only routing demands that require fewer hops can be successfully met.

From fig. 7(c), we can see that TBPRs have higher power consumption due to the longer path length necessary for bypassing the intruder. And specially, directional TBPR elegantly maintains a relatively similar power consumption under differ-



(a) Successful delivery rate (b) Path length (c) Power consumption

Fig. 6. Performance evaluation under different intruder probing ability.



(a) Successful delivery rate (b) Path length (c) Power consumption

Fig. 7. Performance evaluation with presence of different number of targets.

ent intruder population and meanwhile has nice performance in both successful delivery rate and path length. Note that the obvious drop in power consumption of omnidirectional TBPR is due to the drop of path length.

VI. Conclusion

In a target detection application, rational targets may be conscious of the location of sensor nodes, so they can plan a path to traverse the sensor field without being detected. Instead of enhancing surveillance ability by deploying more sensors as traditional solution does, we propose a new approach which prevents information leakage to adversary targets and thus disables them from selecting smart paths. This approach aims to optimize the sensor communication exposure. Two target bypass routing schemes are proposed to deal with omnidirectional and directional communication. The simulation results confirm that both of them can greatly reduce the exposure of sensor communication to targets. Particularly, orientation assignment TBPR applying for directional communication achieves a stable and better performance on exposure, path length as well as power consumption. We also set up a primary experimental testbed to verify radius assignment based TBPR, and we are currently conducting experiments with sensor nodes equipped with beam-forming directional antennas to verify potential based TBPR.

Acknowledgement

This research was supported by NSF of China under grant No.60773091, No.61073158 and Shanghai Post-Doc grant No.09R21413700.

References

[1] C.F. Huang, Y.C. Tseng, and L.C. Lo. The coverage problem in three-dimensional wireless sensor networks. *IEEE Globecom*, 2004.

[2] S. Kumar, T. Lai, and A. Arora. Barrier coverage with wireless sensors. *Proc. of the 11th annual int'l conference on Mobile computing and networking (Mobicom)*, pages 284–298, 2005.

[3] S. Zhou, M.Y. Wu, and W. Shu. Improving mobile target detection on randomly deployed sensor networks. *Int'l Journal of Sensor Networks*, 6(2):115–128, 2009.

[4] C. Zhang, Y. Zhang, and Y. Fang. Localized coverage boundary detection for wireless sensor networks. *Proc. of the 3rd International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks, Waterloo, Canada*, 2006.

[5] M. Chen, V. Leung, S. Mao, Y. Xiao, and I. Chlamtac. Hybrid geographical routing for flexible energy-delay trade-offs. *IEEE Transactions on Vehicular Technology*, 58(9):4976–4988, 2009.

[6] F. Yu, S. Park, Y. TIan, M. Jin, and S. Kim. Efficient hole detour scheme for geographic routing in wireless sensor networks. *Proc. of the IEEE Vehicular Technology Conference, VTC Spring, Marina Bay, Singapore*, pages 153–157, May 2008.

[7] S. Roy, C. Hu, D. Peroulis, and X. Li. Minimum-energy broadcast using practical directional antennas in all-wireless networks. *Proc. of the 25th Annual IEEE Conference on Computer Communications (INFOCOM), Barcelone, Spain*, pages 1–12, April 2006.

[8] Iris Motes. http://www.xbow.com/Products/productdetails.aspx?sid=264.

[9] B. Karp and H. Kung. GPSR: Greedy perimeter stateless routing for wireless networks. *Proc. of the Sixth ACM/IEEE Int'l Conference on Mobile Computing and Networking (MobiCom), Boston, USA*, pages 243–253, 2000.

[10] M. Chen, V. Leung, S. Mao, and Y. Yuan. Directional geographical routing for real-time video communications in wireless sensor networks. *Elsevier Computer Communications*, 30(17):3368–3383, 2007.

[11] A. Howard, M. Mataric, and G. Sukhatme. Mobile sensor network deployment using potential fields: a distributed, scalable solution to the area coverage problem. *Proc. of the 6th International Symposium on Distributed Autonomous Robotics Systems (DARS02) Fukuoka, Japan*, June 2002.