09 Aug 2010

Defending Wireless Sensor Networks Against Adversarial Localization

Neelanjana Dutta

Abhinav Saxena

Sriram Chellappan
Missouri University of Science and Technology, chellaps@mst.edu

Recommended Citation

N. Dutta et al., "Defending Wireless Sensor Networks Against Adversarial Localization," *Proceedings - IEEE International Conference on Mobile Data Management*, pp. 336 - 341, article no. 5489711, Institute of Electrical and Electronics Engineers, Aug 2010.
The definitive version is available at https://doi.org/10.1109/MDM.2010.75

Defending Wireless Sensor Networks Against Adversarial Localization

Neelanjana Dutta, Abhinav Saxena and Sriram Chellappan

Department of Computer Science
Missouri University of Science and Technology
Rolla, MO 65401, U.S.A.
Email: {nd2n8, arsnt7, chellaps}@mst.edu

Abstract

In this paper, we study the issue of defending against adversarial localization in wireless sensor networks. Adversarial localization refers to attacks where an adversary attempts to disclose physical locations of sensors in the network. The adversary accomplishes this by physically moving in the network while eavesdropping on communication messages exchanged by sensors, and measuring raw physical properties of messages like Angle of Arrival, Signal Strength of the detected signal. In this paper, we aim to defend sensor networks against such kinds of adversarial localization. The core challenge comes from the sensors performing two conflicting objectives simultaneously: localize the adversary, and hide from the adversary. The principle of our approach and the subsequent defense protocol is to allow sensors intelligently predict their own importance as a measure of these two conflicting requirements. Only a few important sensors will participate in any message exchanges. This ensures high degree of adversary localization, while also protecting location privacy of many sensors. Extensive simulations are conducted to demonstrate the performance of our protocol.

I. Introduction

Recently, a critical component of research in the networking arena has been Wireless Sensor Networks (WSNs). Numerous civilian and military applications are possible with wireless sensor networks. Towards this extent, a vast amount of theory in the realm of sensor deployment, data dissemination, sensor mobility, localization, tracking, security [1], [2], [3], [4], [5] etc. have been developed by researchers. In parallel, many wireless sensor network test-beds have also been successfully deployed, tested and validated [6], [7]. The conclusions from these efforts serve to demonstrate the significant promise WSNs have to impact humans in a variety of applications.

In this paper, we focus on an important security threat in WSNs, called *adversarial localization*. Adversarial location refers to attacks wherein an adversary aims to discover positions of sensors in a network. We claim that under such attacks *location privacy* of sensors is compromised. A host of benefits are patent to adversaries when sensor location privacy is compromised. For instance, the number of sensor nodes in the network can be estimated which can help gauge network strength; optimal intrusion paths involving minimal detection through the network can be determined, physical destruction of sensors can be accomplished to compromise network functionality etc. Protecting location privacy of sensors against adversarial localization is hence a critical security requirement.

There are two intuitive approaches to protect location privacy in WSNs. The first is to encrypt all sensor messages [5], [8], [9]. Adversaries will hence not be able to decrypt messages, and hence the identities of sensors are preserved. Unfortunately, this technique fails since the adversary can measure raw physical (and location specific) properties of the wireless signals like Angle of Arrival (AoA) and Receive Signal Strength Indicator (RSSI). Repeated messages from the same sensors naturally leak more location information until eventually sensors are localized. The second approach is to let all sensors sleep, and so no information of sensors positions is leaked. Unfortunately, the sensors do not accomplish the WSN mission in this case, and the network is rendered useless. Preserving location privacy of sensors while still maintaining sufficient network performance is very challenging.

In this paper, we make the following contributions:

Attack and Network Model: In this paper, we define a representative adversarial localization attack model. A physically mobile adversary (typically a robot) will move in the network while simultaneously listening for sensor

978-0-7695-4048-1/10 $26.00 © 2010 IEEE
DOI 10.1109/MDM.2010.75

communication signals. To maintain stealthiness, the adversary will be *passive*, that is, it will not attempt to physically tamper with sensors. As such, the adversary will not be able to infer any information privy to sensors like identities, stored keys, message content etc. However, since the nature of the medium is wireless, the adversary will be able to detect wireless signals and measure their physical properties like Angle of Arrival (AoA) and Receive Signal Strength Indicator (RSSI) and localize sensor positions using existing techniques in [10], [11], [12]. Clearly, more the number of messages sent by a sensor, the more location information its leaks to the adversary. The sensor network on the other hand is deployed to localize such an adversary. However, the sensors are also aware that the adversary will attempt to locate sensor positions. The goal of the sensor network is to localize the adversary, while simultaneously preserving its location privacy from the adversary.

A light-wight and distributed protocol: In this paper, we design a light-weight and purely distributed protocol for preserving sensor location privacy against adversarial localization. The core challenge comes from the sensors performing two conflicting objectives simultaneously: localize the adversary, and hide from the adversary. The principle of our approach is to allow sensors intelligently predict their own *importance* as a measure of these two conflicting requirements. Only a few important sensors will participate in any message exchanges. This ensures high degree of adversary localization, while also protecting locations of many sensors. We then design a localized light weight and purely distributed protocol based on this approach. Extensive simulations are conducted to demonstrate the performance of our protocol from the perspective both adversary localization and sensor location privacy.

The rest of the paper is organized as follows. In Section II, we present the system model and problem definition. In Section III, we present our defense protocol against adversarial localization. Performance Evaluations are presented in Section IV, and the paper is concluded in Section V.

II. System Model and Problem Definition

In this section, we will first define the system model, from the perspective of both the sensor network and the adversary. The formal problem definition is presented next

A. System Model

Sensor Network Model: In this paper, we consider a sensor network where the deployment field is clustered into multiple grids. Clustering a sensor network has been widely adopted in practice [13], [14], [4]. Advantages of clustering include better network scalability, decreased routing complexity, improved power efficiency etc. We assume that sensors know their positions in the network, which can be accomplished using localization techniques in [15], [16]. We also assume that sensors encrypt their messages using light weight techniques like [5], [8].

The mission of the sensors is to localize adversaries physically moving in the network. To do so, sensors are equipped with ranging hardware that they use to determine distances from the adversary (can be accomplished by typical vibration or infrared sensors). For a grid of size r, the sensing range is assumed to be $\geq \sqrt{(2)}r$, and the radio transmission range is assumed to be $\geq \sqrt{(5)}r$. The localizing accuracy is expected to be grid level, i.e., the adversary is considered to be *localized* at all times when sensors are correctly aware of the grid where the adversary is physically present, and *lost* at other times. In this paper, we initially assume (for ease of elucidation) that the deployment field is fully covered, i.e., every point in the field is within the sensing range of one or more sensors [1]. Note that in order to localize any adversary in the network, sensors will have to exchange communication messages on adversary position. Since multiple sensors will likely be sensing the adversary at any point in time, there may be multiple messages exchanged. Clearly there is a tradeoff between accuracy of localizing the adversary and number of messages exchanged by sensors.

Adversary model: In this paper, we consider an adversary that is physically moving in the network like a programmable robot. The adversary's movement is either random or controlled. While the adversary can have any objective in its mobility, it also has the objective of localizing sensor positions passively. By passive, we mean the adversary will not launch any active attack on the network like breaking into sensors to determine their positions, or disclose encryption keys. Rather the adversary will discover sensor positions based on information leakage of wireless signals which sensors exchange in the network. The adversary will accomplish this by passively intercepting communication messages, and measuring its raw physical properties like Received Signal Strength or Angle of Arrival or both. Any number of existing techniques for sensor localization [3], [17], [10] with subtle modifications can then be applied to localize sensors. Clearly, more the number of messages from the sensors, more is the information leaked to the adversary, and better is the adversary's estimate of the sensor positions.

B. Problem Definition

We model our problem as a game played between two opposing entities - the sensors in the network and the adversary. The goal of the sensors is to localize the adversary, while simultaneously minimizing information leakage in terms of communication messages. The adversary's goal is to physically move in the network, while

[1]However, the proposed scheme will work without modification even if this assumption does not hold in practice.

simultaneously attempting to localize sensors. The success of the sensors is measured by means of a metric called *Adversary Location Certainty*, which denotes the degree of accuracy of adversary localization by sensors. The success of the adversary is measured by a metric called *Sensor Location Leakage*, which is defined as a function of number of message sent out by a sensor within the radio range of the adversary. In simple terms, our problem is to design a protocol to be executed by sensors at runtime that maximizes *Adversary Location Certainty*, while simultaneously minimizing *Sensor Location Leakage*.

III. Our Protocol

In this section, we present a light-weight and distributed protocol for defending wireless sensor networks against adversarial localization. As indicated in Section II, the goal is to maximize the accuracy of adversary tracking by the sensors (i.e., *Adversary Location Certainty*), while simultaneously protecting location privacy of sensors from the adversary (i.e., *Sensor Location Leakage*).

A. Preliminaries

Before discussing the protocol, we first discuss and define important definitions used later in the paper.

1) Fixed Parameters: In this section, we discuss definitions for Fixed Parameters, which are those parameters in our protocol whose values are unchanged during the entire network mission.

Neighboring Grids: For each grid in the network, we divide their neighboring grids into two classes Regular Neighbors and Corner Neighbors. Regular Neighbors of a Grid g are those neighboring grids which are in the immediate Up, Down, Left and Right position of Grid g. Corner Neighbors of a Grid g are those neighboring grids which are in the immediate diagonal positions of Grid g.

d^i_{max}: For each grid in the network, d^i_{max} is the minimum Euclidian distance between the sensor i in the grid and the adversary, beyond which the sensor i can deterministically assume that the adversary is not in the same grid as itself. In other words, it is the distance between a sensor and the furthest boundary point of that grid in which the sensor is present. We consider every grid has a vertical axis passing through its center, and clockwise angle is measured to be positive. Consider a sensor i (represented as a dot) in Figure 1 (a). Let the angle made by a straight line drawn between the center of the grid and the sensor i, and the vertical axis be θ. Let the distance between the center of the grid and the sensor be ϵ. Considering that the sensor might be included in any of the four quadrants,

$$d^i_{max} = \sqrt{(}2r^2 + (-1)^n 2r\epsilon(sin\theta + (-1)^k Cos\theta) + \epsilon^2), \quad (1)$$

where $n = \lfloor \frac{\theta}{180} \rfloor$ and $k = \lfloor \frac{\theta}{90} \rfloor$.

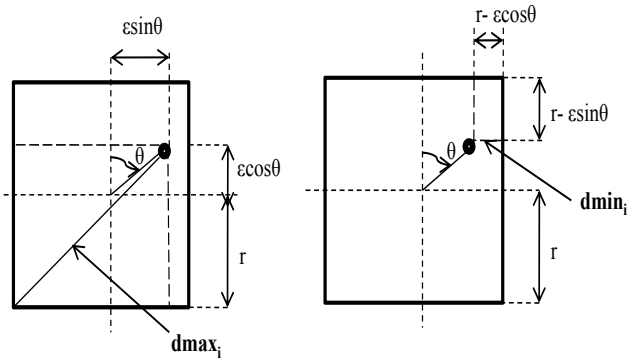

Fig. 1. Determination of d^i_{min} and d^i_{min} for Sensor i in A Grid

d^i_{min}: For each grid in the network, d^i_{min} is the maximum Euclidian distance between the sensor i in the grid and the adversary, within which a sensor can deterministically assume that the adversary is in the same grid as itself. That is, it is the distance between a sensor and the closest boundary point of that grid in which the sensor is present, as shown in Figure 1 (b), and given by,

$$d^i_{min} = min[(r + (-1)^n \epsilon sin\theta), (r + (-1)^m \epsilon cos\theta)] \quad (2)$$

where $n = \lceil \frac{\theta}{180} \rceil$ and $m = \lceil \frac{\theta+90}{180} \rceil$.

d_{max} and d_{min} sensor: For each grid, the sensor with the minimum value of d^i_{max} among all sensors in that grid is the d_{max} sensor of the grid. Similarly, the sensor with the maximum value of d^i_{min} among all sensors in that grid is the d_{max} sensor. We also define the d_{max} and d_{min} circles as the circles whose centers are the positions of the d_{max} and d_{min} sensors, and whose radii are d_{max} and d_{min} respectively for each grid.

We wish to point out that each sensor can calculate the above parameters independently with knowledge of other sensor positions in the grid. The parameters once determined are fixed, and do not change subsequently.

2) Dynamic Parameters: We now discuss the parameters in our protocol whose values are dynamically altered as a function of where the adversary is currently located. For all subsequent discussions in this section, consider that the adversary is currently localized in Grid g.

$\bar{d}^i_{max}$: For each sensor i in a corner neighbor of grid g, we define its $\bar{d}^i_{max}$ as the distance between sensor i and the edge of the corner neighbor, closest to the adversary.

$\bar{d}^i_{min}$: For each sensor i in the neighboring grids (both regular and corner neighbors) of grid g, we define its $\bar{d}^i_{min}$

as the distance between sensor i and the perpendicular distance between sensor i and the boundary of Grid g.

$\bar{d}_{max}$ sensor: Recall that there can be different values for $\bar{d}^i_{max}$ for each sensor i in the neighboring grids of grid g. For each sensor in a neighboring grid, we define its $\bar{d}^i_{max}$ circle as a circle of radius $\bar{d}^i_{max}$ centered at the location of sensor i. Among all such sensors, the one whose $\bar{d}^i_{max}$ circle overlaps the most with its neighboring grids is considered to be $\bar{d}^i_{max}$ sensor of Grid g.

$\bar{d}_{min}$ sensor: Recall that there can be different values for $\bar{d}^i_{min}$ for each sensor i in the corner neighbors of grid g. For each sensor in a particular corner neighbor, we define its $\bar{d}^i_{min}$ circle as a circle of radius $\bar{d}^i_{min}$ centered at the location of sensor i. Among all such sensors, the one whose $\bar{d}^i_{min}$ circle covers the most area in its grid is considered to be $\bar{d}^i_{min}$ sensor of Grid g.

We wish to point out here that the values for these parameters can change based on which grid the adversary is currently localized. However, irrespective of where the adversary is localized, depending on the current position of the adversary, each sensor can calculate each of the above parameters independently assuming each sensor knows the positions of other sensors in the grid.

B. Defense Protocol Description

Pseudocode 1 presents the pseudocode of our defense protocol, which is divided into two phases: Initialization Phase, and Post Initialization Phase as discussed below.

Initialization Phase: Initially when the adversary first enters the network, the first three sensors sensing the adversary will perform simple message exchanges and triangulation to localize the adversary to a grid. This is the initialization phase, which notifies all sensors to execute the protocol for adversary localization and sensor location privacy preservation as discussed below.

Post Initialization Phase: With this start of the protocol, the sensors in neighboring grid of the adversary calculates $\bar{d}_{min}$ and $\bar{d}_{max}$ sensors and updates them with each new grid location of the adversary. We define adversary-sensing circle of a sensor S_x to be the circle with S_x at center and radius equal to the distance between adversary and sensor S_x.

The aim of this paper being grid level localization, the protocol allows message exchange among sensors only when a grid switch by the adversary is detected. At different steps the protocol uses four different types of messages m_1, m_2, m_3 and m_4. Each message contains a unique message key to indicate its own type. Either one of the four different cases discussed below would take place in case of a detected grid switch.

Case 1 - Grid Switch Detection by d_{min} sensor: When a d_{min} sensor of a neighboring grid, say g^*, starts sensing

Pseudocode 1 Pseudocode of the Defense Protocol

```
1:  Initialization Phase
2:  while When Adversary is first sensed by three sensors do
3:      Triangulate Adversary to a Grid
4:  end while
5:  End Initialization Phase

6:  Post Initialization Phase
7:  for Each Step of Adversary do
8:      while Adversary position is in Grid g do
9:          if Adversary enters d_min circle of Grid g* then
10:             Refer to Section III-B Case 1.
11:         else if Adversary enters d̄_min circle of Grid g* then
12:             Refer to Section III-B Case 2.
13:         else if Adversary leaves d_max circle of Grid g then
14:             Refer to Section III-B Case 3.
15:         else if Adversary enters d̄_max circle of Corner Neigh-
            bor g** of Grid g then
16:             Refer to Section III-B Case 4.
17:         end if
18:     end while
19: end for
```

the adversary, It indicates the adversary's movement into the d_{min} circle, which is possible only in case of a grid switch to g^*. The d_{min} sensor broadcasts message m_1 updating current position of adversary to be g^* and adversary's distance from it. As a grid switch is detected, all the sensors receiving m_1 update the set of neighbors of current grid, $\bar{d}_{min}$ and $\bar{d}_{max}$ sensors. In this case, only a single message is exchanged to update sensors in vicinity of the adversary about its grid switch.

Case 2 - Grid Switch Detection by $\bar{d}_{min}$ sensor: Another case of identifying and broadcasting adversary's grid switch using only one message is possible when $\bar{d}_{min}$ sensor of a neighboring grid g^* starts sensing the adversary, indicating adversary's grid switch to g^*. Similar to case 1, the $\bar{d}_{min}$ sensor of g^* updates the location information and its distance from adversary by broadcasting message m_1.

Case 3 - Grid Switch Detection by d_{max} sensor:

Step 1: Before Case 1 or Case 2 occurs for a particular grid switch of the adversary, the grid switch can be detected when the d_{max} sensor of current grid stops sensing the adversary. Although it signifies adversary's movement outside the current grid, it cannot be determined by the d_{max} sensor which neighboring grid it has moved to. So the d_{max} sensor will broadcast message m_2 to initiate the Localization() procedure.

Step 2: Upon receiving message m_2, every sensor S_i sensing the adversary computes the two points of intersection of the sensing circles of the sender of the m_2 and itself. The adversary should be present in either of these two points. Based on the location of these points, the sensors intelligently try to localize the adversary. The next steps of the protocol can be divided into two cases based on the location of the intersection points.

a) If the two points are included in a single grid, say g^{**}, the adversary has clearly moved to grid g^{**}. Otherwise, if only one of the intersection points falls in a neighboring grid (say g^{**}) of last known adversary grid, g^{**} is the new location of the adversary, as the adversary can move only to neighboring grids in a single step. After concluding about adversary's new location, S_i waits for a time t, (t = distance of the adversary from S_i), to avoid any redundant message expenditure. If no other sensor has sent m_1 in this interval of time t, then S_i broadcasts m_1 updating the grid location of adversary and its distance from S_i. In this case, two messages are sent out among the sensors to determine and update the new grid location of the adversary.

b) If both the points of intersection fall into different neighboring grids, it is possible that the adversary has moved to any of the two grids. So after wait time t, if no other sensor has sent m_1 or m_3 in that time, S_i broadcasts message m_3. Every sensor S_j receiving m_3 and sensing the adversary computes point of intersection of sensing circle of sender of m_2 and m_3 and itself. The grid containing this point is recognized by S_j as the new location of the adversary. Sensor S_j waits for time t^* (t^* = distance of the adversary from S_i + a constant c) to avoid conflict. The constant c is chosen large enough to ensure that the value of t^* is most likely greater than the value of t, so that if any sensor can satisfy the criteria mentioned in a), it can send message before S_j, and thus only two messages will be required to perform the localization. If no other sensor has sent message m_4 in that time t^*, S_j broadcasts m_4 updating new position of the adversary. In this case, three messages are required to locate the adversary.

Case 4 - Grid Switch Detection by $\bar{d}_{max}$ sensor: Before any of the previous cases detects a grid switch, $\bar{d}_{max}$ sensor of a corner neighbor of the current grid might start sensing the adversary. It signifies that the adversary has moved to a new grid, but this information is insufficient to determine exactly which grid the adversary has moved to. The $\bar{d}_{max}$ sensor broadcasts message m_2 and the localization procedure begins (discussed in the next paragraph). The successive steps in this case is exactly similar to the Step 2 in Case 3. Even in this case, either two or three messages are required to locate the adversary.

The proposed solution localizes the adversary by intelligently using the its previous location. But as we trade location certainty against location privacy, in some of the cases the adversary cannot be deterministically or correctly located due to its movement into the uncertainty region. However, using simulations, we show in section IV that our protocol assures location certainty in most of the time while majority of the sensors in the network do not send any message or sends negligible number of messages throughout.

IV. Performance Evaluations

In this section, we evaluate the performance of our defense protocol via simulations. We consider a sensor network clustered into 15×15 grids, where the sensors are uniformly and randomly deployed. The adversary randomly moves in the network and is equipped with unlimited memory to store and process messages exchanged by sensors. We assume that the radio range of the adversary is unlimited (i.e., the adversary can eavesdrop on any message sent by any sensor in the network). We have two key performance metrics: *Adversary Location Certainty*, which is the percentage of time that the adversary's position is correctly localized to a grid, and *Sensor Location Leakage*, which is quantified by the number of messages sent by each sensor within the radio range of the adversary.

Evaluating *Adversary Location Certainty*: In Figure 2 (a), we plot the *Adversary Location Certainty* as a function of number of time units spent by the adversary in the network for a network density of 10 sensors per grid. As we can see close to 90% of the time the sensors are able to correctly localize the adversary in our protocol. The loss of about 10% in localization certainty comes from the trade-off is minimizing message exchanges (which is evaluated subsequently). In Figure 2 (b), we plot *Adversary Location Certainty* as a function of number of sensors per grid when the time spent by the adversary is $12,000$ time units. As we can see, even for very low sensor densities of 3 sensors per grid, the *Adversary Location Certainty* is 75%. When the density increases, the success of localizing the adversary dramatically increases. Interestingly, the success rate begins to flatten at around 95% beyond when the number of sensors per grid is 15. This is because, the uncertainty regions in the network tends to stay constant even for further increases in number of sensors per grid beyond 15.

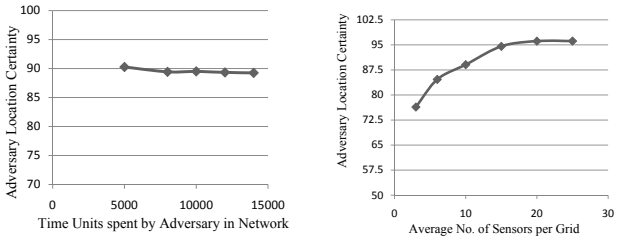

Fig. 2. Adversary Location Certainty vs. Time spent by Adversary (a) and Sensor Density (b)

Evaluating *Sensor Location Leakage*: In Figure 3, we study the sensor location privacy as a function of *Sensor Location Leakage* when the density of the sensors is 10 per grid. Clearly, more the number of messages sent by

a sensor, more is the information leaked, and less is the location privacy of sensors. As we can see from Figure 3, a vast majority of the sensors in the network (more than 90%) send less than three messages. This coupled with the fact that *Adversary Location Certainty* is also quite high demonstrates that our protocol is effective in localizing adversaries while keeping the information leakage from sensors quite low. Due to space limitations, we do not study *Sensor Location Leakage* as a function of varying sensor densities. Nevertheless, the trend remains the same.

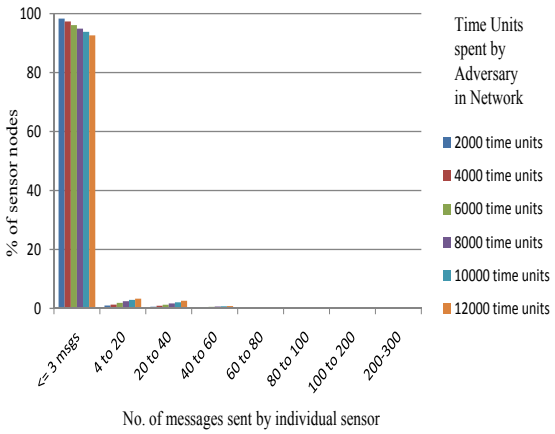

Fig. 3. Sensor Location Leakage with Varying Times Spent by Adversary in the Network

V. Conclusions

In this paper, we addressed an important problem, namely the defense of sensor networks against adversarial localizations. The problem spanned the three critical dimensions of target tracking, sensor localization and privacy in sensor networks, which to the best of our knowledge is unique. The principle of our defense is to allow sensors to intelligently predict their own importance as a measure of the two conflicting requirements of adversary localization and sensor location privacy. Only a few such important sensors will participate in any message exchanges. This ensures high degree of adversary localization, while also protecting location privacy of many sensors. We then design a localized light weight and purely distributed protocol based on this approach. Extensive simulations conducted demonstrate the performance of our protocol.

Acknowledgment

This work was supported in part by a grant from University of Missouri Research Board. All opinions, findings, and conclusions are those of the authors and do not necessarily reflect the views of the funding agency.

References

[1] X. Bai, S. Kumar, D. Xuan, Z. Yun, and T.H. Lai, "Deploying wireless sensors to achieve both coverage and connectivity", in *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing(MobiHoc)*, Florence, May 2006.

[2] F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, "A two-tier data dissemination model for large-scalewireless sensor networks", in *Proceedings of ACM International Conference on Mobile Computing and Networking (MOBICOM)*, Atlanta, September 2002.

[3] T. He, C. Huang, B.M. Blum, J.A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks", in *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom)*, San Diego, August 2003.

[4] T. Abdelzaher, B. Blum, Q. Cao, D. Evans, J. George, S. George, T. He, L. Luo, S. Son, R. Stoleru, J. Stankovic, and A. Wood, "Envirotrack: An environmental programming model for tracking applications in distributed sensor networks", in *Proceedings of International Conference on Distributed Computing Systems (ICDCS)*, Tokyo, March 2004.

[5] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", in *Proceedings of the ACM Conference on Computer and Communication Security (CCS)*, November 2002, pp. 41–47.

[6] Prashant Shenoy Purushottam Kulkarni, Deepak Ganesan and Qifeng Lu, "Senseye: A multi-tier camera sensor network", in *Proceedings of ACM Multimedia*, Singapore, November 2005.

[7] S. Bapat, V. Kulathumani, and A. Arora, "Analyzing the yield of exscal, a large-scale wireless sensor network experiment", in *Proceedings of the 13th IEEE International Conference on Network Protocols (ICNP)*, 2005, pp. 53–62.

[8] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks", in *Proceedings of IEEE Symposium on Research in Security and Privacy*, May 2003.

[9] D. Liu and P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks", in *Network and Distributed System Security Symposium (NDSS)*, San Diego, February 2003.

[10] S. Chellappan, V. Paruchuri, D. McDonald, and A. Durresi, "Localizing sensor networks in un-friendly environments", in *IEEE Military Communications Conference (MILCOM)*, San Diego, November 2008.

[11] Z. Yang, E. Ekici, and D. Xuan, "A localization-based anti-sensor network system", in *Proceedings of IEEE INFOCOM 2007 Symposia*, Anchorage, May 2007.

[12] X. Wang, S. Chellappan, W. Gu, W. Yu, and D. Xuan, "Search-based physical attacks in sensor networks", in *Proceedings of IEEE ICCCN*, October 2005.

[13] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing", in *Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom)*, Rome, July 2001.

[14] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks", in *Proceedings of Hawaii International Conference on System Sciences (HICSS)*, Maui, January 2000.

[15] N. Bulusu, J. Heidemann, and D. Estrin, "Adaptive beacon placement", in *Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS)*, Phoenix, AZ, April 2001.

[16] A. Howard, M. J. Mataric, and G. S. Sukhatme, "Relaxation on a mesh: a formation for generalized localization", in *Proceedings of IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, Maui, November 2001.

[17] Andreas Savvides, Chih-Chieh Han, and Mani B. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors,", in *Proceedings of ACM MobiCom*, 2001.