This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

Secure and Energy Aware Routing (SEAR) in Wireless Sensor Networks

Di Tang[†*], Tingting Jiang[‡] and Jian Ren[†]
[†]Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824
Email: {ditony, renjian}@egr.msu.edu
[‡]Department of Computer Science, Virginia Tech, Blacksburg, VA 24061
Email: tvj@vt.edu
[*]National Key Laboratory of ISN & Information Science Institute, Xidian University, Xi'an 710071, China

***Abstract*—Lifetime optimization and security are two important design issues for multi-hop wireless sensor networks with non-replenishable energy resources. In this research, we propose a novel secure and energy aware (SEAR) routing protocol to address these two issues concurrently through balanced energy consumption and probabilistic random walking. SEAR is designed with two configurable parameters, energy balance control (EBC) and security level. EBC is used to enforce energy balance and increase the lifetime. Security level is designed to determine the probabilistic distribution of the random walking that provides routing security. The security level can be defined by the message source on a message level, or on a system level. Theoretical analysis and OPNET simulation results show that the proposed SEAR can provide excellent balance between routing efficiency and energy consumption while preventing routing traceback attacks.**

I. Introduction

The recent technological advances make wireless sensor networks (WSNs) technically and economically feasible to be widely used in both military and civilian applications, such as monitoring of ambient conditions related to the environment, precious species and critical infrastructures. A key feature of such networks is that each network consists of a large number of untethered and unattended sensor nodes. These nodes often have very limited and non-replenishable energy resources. Therefore, energy is an important design issue for these networks.

Routing is a very challenging design issue in wireless sensor networks due to several characteristics that distinguish WSNs from contemporary communication and wireless ad-hoc networks. A properly designed routing protocol should not only ensure high message deliver ratio and guarantee low energy consumption for packet delivery, but should also balance the entire sensor network energy consumption, and thereby extend the sensor network lifetime. However, this requirement makes routing in wireless sensor network even more complicated.

In addition to the aforementioned issues, WSNs rely on wireless communications, which is by nature a broadcast medium. It is more vulnerable to security attacks than its wired counterpart due to lack of a physical boundary. In particular, in the wireless sensor domain, anybody with an appropriate wireless receiver can monitor and intercept the sensor network communications. The adversaries may use expensive radio transceivers, powerful workstations and interact with the network from a distance since they are not restricted to using sensor network hardware. It is possible for the adversaries to perform jamming attacks and routing traceback attacks.

Motivated by the fact that sensor networks routing may often be geographically based, we design and evaluate a geographical-based secure and energy aware routing (SEAR) protocol for wireless sensor network. SEAR transmit messages to the appropriate geographical region without relying on flooding. It has three advantages: (i) SEAR ensures a balanced energy consumption of the entire sensor networks so that the lifetime of the WSNs can be maximized. (ii) SEAR dynamically selects routing paths based on the geographic information and the remaining energy of the neighboring grids. (iii) SEAR can seamlessly implement dynamic routing to prevent routing traceback attacks and malicious traffic jamming attacks in wireless sensor networks.

The rest of this paper is organized as follows. In Section II, the related works are reviewed. The system model is presented in Section III. The proposed scheme is described in Section IV. In Section V, security analysis of the proposed scheme is presented along with performance evaluation described in Section VI. We conclude in Section VII.

II. Related Works

Routing is a challenging task in wireless sensor networks due to high dynamics and limited resources. Geographic routing has been widely hailed as the most promising approach to generally scalable wireless routing. Geographic routing protocols utilize the geographic location information to route data packets hop by hop from the source to the destination. The source will choose the immediate neighboring node to forward the packet based on either the direction or the distance [1], [2].

While geographic routing algorithms offer the advantages that the nodes only need to maintain neighboring information and provide higher efficiency and better scalability for large scale WSNs, however, these algorithms may reach their local minimum, which result in dead end or loops.

The existing research on geographic routing focuses largely on routing efficiency and the dead end and loop issues through combined greedy and facing routing protocols [1], [3], [4] and local broadcast [5], [6]. Although there have

978-1-4244-5638-3/10/$26.00 ©2010 IEEE

been many research papers deal with the lifetime of wireless sensor networks, only a few of them are related to energy aware geographic routing [3], [7]–[9]. How to balance the energy consumption and thereby increase the network lifetime remains a problem for geographic routing protocols.

In addition, exposure of routing information presents significant security threats to sensor networks. By acquisition with the location and routing information, the adversaries may be able to traceback the source node easily. To solve this problem, several schemes have been proposed to provide source-location privacy through secure routing protocol design [10]–[13]. However, to the best of our knowledge, none of these schemes have considered energy balance.

In this paper, for the first time, we propose a secure and energy aware routing (SEAR) protocol that can address routing secure and energy balance concurrently. The main idea is that each sensor node needs to maintain the energy level of its immediate adjacent neighboring grids in addition to their relative locations. Using these information, each sensor node can create multiple filters based on the expected design tradeoff between security and efficiency. Our extensive OPNET simulation results show that SEAR can provide excellent energy balance and routing security with only very moderate routing overhead. It is also demonstrated that the proposed secure routing can increase the message delivery ratio due to reduced dead ends and loops.

III. Models and Assumptions

A. The System Model

We assume that the WSNs are composed of a large number of sensor nodes and a sink node. The sensor nodes are randomly deployed throughout the sensor domain. Each sensor node will have a very limited and non-replenishable energy resource. The sink node is the only destination that every sensor node will send message packets to through a multi-hop routing strategy. The information of the sink node is made public. For security management purpose, each sensor node may also be assigned a node ID corresponding to the location where this message is generated. To prevent adversaries from recovering the source location from the node ID, dynamic ID can be used. In addition, the content of each message can also be encrypted using the shared secret key between the node/grid and the sink node.

We also assume that each sensor node knows its relative location in the sensor domain and has knowledge of its immediate adjacent neighboring grids and their energy levels. The information about the relative location of the sensor domain may be broadcasted in the network for routing information update [14], [15].

The key management, including key generation, key distribution and key update, is beyond the scope of this paper. However, the interested readers are referred to reference such as [16] for more information.

B. The Adversarial Model

In WSNs, the adversary may try to recover the message source node or jam the packet from being delivered to the sink node. The adversaries would try their best to equip themselves with advanced equipments, which means they would have some technical advantages over the sensor nodes. In this paper, the adversaries are assumed to have the following characteristics:

- The adversaries will have sufficient energy resources, adequate computation capability and enough memory for data storage. On detecting an event, they could determine the immediate sender by analyzing the strength and direction of the signal they received. They can move to this sender's location without too much delay. The adversaries may also compromise some sensor nodes in the network. We assume that the adversaries will never miss any event close to them.
- The adversaries will not interfere with the proper functioning of the network, such as modifying packets, altering the routing path, or destroying sensor devices, since such activities can be easily identified. However, the adversaries may carry out passive attacks, such as eavesdropping of the communications.
- The adversaries are able to monitor the traffic in an area that is important to them and get all of the transmitted messages. However, we assume that the adversaries are unable to monitor the entire network. In fact, if the adversaries could monitor the entire wireless sensor networks, then they can monitor the events directly without relying on the sensor network.

C. Design Goals

Our design goal can be summarized as follows:

- To maximize the sensor network lifetime, we will ensure that the energy consumption of all sensor grids are balanced.
- To achieve high packet delivery ratio, our routing protocol should try to avoid packet dropping when alternative paths exist.
- The adversaries should not be able to get the source location information by analyzing the traffic pattern.
- The adversary should not be able to get the source location information if he is only able to monitor certain area of the WSNs and compromise a few sensor nodes.
- Only the sink node is able to identify the source location through the messages received. The recovery of the source location from the received message should be very efficient.
- The routing protocol should maximize the probability that the packet is being delivered to the sink node when adversaries are only able to jam a few sensor nodes [17].

D. Overview of the Proposed Scheme

In our scheme, the network is evenly divided into small grids. The formation of the grid and the head node selection in each grid have been studied in many literature works [18]–[20]. Each grid will have a relative location based on the grid information. The node in each grid with the highest energy level will be selected as the head node for packet

978-1-4244-5638-3/10/$26.00 ©2010 IEEE

forwarding. In addition, each node in the gird will maintain its own attributes, including location information, remaining energy level of its grid, as well as the attributes of its adjacent neighboring grids. The information maintained by each sensor node will be periodically updated. We assume that the sensor nodes in its direct neighboring grids are all within its direct communication range. We also assume that the whole network is fully connected through the multi-hop communications.

While maximizing message source location privacy and minimizing the traffic jamming for communications between the source and the destination nodes, we can optimize the sensor network lifetime through balanced energy consumption throughout the sensor networks.

In addition, through the maintained energy levels of its adjacent neighboring grids, it can be used to detect compromised nodes and filter them out of the active routing selection.

IV. The Proposed SEAR Scheme

We now describe the proposed SEAR algorithm. The algorithm consists of two methods for packet forwarding: shortest path forwarding based on the geographical information, and random forwarding, which is used to create routing unpredictability for source privacy and jamming prevention. As described in the introduction, we are interested in routing with energy balance.

A. SEAR Parameters and Design Tradeoff

In the SEAR algorithm, each node A maintains its relative location and the remaining energy level of its immediate adjacent neighboring grids. Denote the set of its immediate adjacent neighboring grids as $\mathcal{N}_A$ and the remaining energy of grid $i, i \in \mathcal{N}_A$, as $\mathcal{E}r_i$. Then node A can compute the average remaining energy of grids in $\mathcal{N}_A$ as $\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|}\sum_{i\in\mathcal{N}_A}\mathcal{E}r_i$.

In the multi-hop routing, the node A will only select its next hop grid from the set $\mathcal{N}_A$ according to our assumption. However, to achieve energy balance of the grids in $\mathcal{N}_A$, we should try to avoid draining energy from the grids with relatively low energy levels. Instead, node A should select only the grids from $\mathcal{N}_A$ with relative higher remaining energy levels as its next routing hop. More precisely, we first select a parameter $\alpha \in [0,1]$, called *energy balance control (EBC)*, and then define the candidate set as $\mathcal{N}_A^\alpha = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha\mathcal{E}_a(A)\}$ based on the EBC α.

It can be easily seen that the EBC α provides a tradeoff between energy balance and routing security. A larger α corresponds to a better energy balance, but less routing flexibility and security. In addition, α can be configured in a packet level, or a general network level based on the application scenarios.

SEAR algorithm contains two algorithms to select the grid for packet forwarding, one is a deterministic shortest path routing grid selection, and the other is a secure routing grid selection through random walking. In the deterministic routing algorithm, the next hop grid will be selected from $\mathcal{N}_A^\alpha$ based on the relative locations of the grids. The grid that is closet to the sink node will be selected for packet forwarding. In the secure routing algorithm, the next hop grid will be randomly selected from $\mathcal{N}_A^\alpha$ for packet forwarding. The distribution of these two algorithms is controlled by a *security level* $\beta \in [0,1]$ carried in each packet.

When a node needs to forward a packet, the node first selects two random numbers $\gamma, \delta \in [0,1]$, $\gamma \leq \beta$. If $\delta > \gamma$, then the node will select the next hop based on the deterministic algorithm, otherwise, the next hop node will be selected using the random walking. The security level β is an adjustable parameter, a smaller β will result in a routing path with fewer hops. Therefore, it is more energy efficient in packet forwarding. On the other hand, a larger β will provide more routing diversity and security.

B. SEAR Algorithm

Based on the previous description, the SEAR algorithm can be described as follows:

Algorithm 1 Node A find the next hop routing grid based on the given parameters $\alpha, \beta \in [0,1]$

1: Compute the average remaining energy of the adjacent neighboring grids: $\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|}\sum_{i\in\mathcal{N}_A}\mathcal{E}r_i$.
2: Determine the candidate grids for the next routing hop: $\mathcal{N}_A^\alpha = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha\mathcal{E}_a(A)\}$.
3: Select two random numbers $\gamma, \delta \in [0,1]$, $\gamma \leq \beta$.
4: **if** $\delta > \gamma$ **then**
5: Send the packet to the grid in the $\mathcal{N}_A^\alpha$ that is closet to the sink node based on its relative location.
6: **else**
7: Route the packet to a randomly selected grid in the set $\mathcal{N}_A^\alpha$.
8: **end if**

V. Security Analysis

In SEAR algorithm, through selection of the security level β and random parameter γ, δ, we create randomness and unpredictability for the routing path. This design is essentially a mixture of the random walking and the shortest path routing. The selection of these two routing strategies is controlled by the security level which may be determined in the message level. The security level can vary based on the security requirements of each packet. In addition, the security level only gives an average randomness of all the nodes. The individual value can vary significantly from node to node due to the random selection of δ.

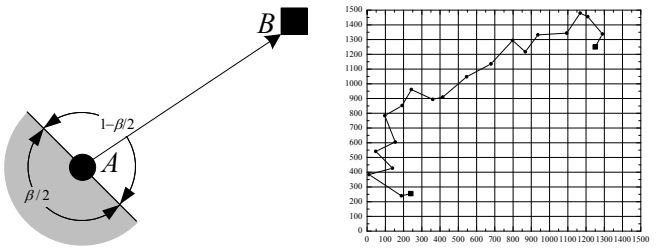
While random walking can provide excellent routing path randomness and security, it has poor routing performance [10], [12]. SEAR algorithm provides a balance between security and routing efficiency with a controllable security parameter β. We need to balance these two strategies in packet forwarding.

For security level β, the average probability of random walking can be calculated as:

$$\frac{1}{\beta}\int_0^\beta x dx = \frac{\beta}{2}. \quad (1)$$

This means that for the security level β to be 1, 0.75, 0.5 and 0, the probability for random walking can be calculated as 50%, 37.5%, 25% and 0%, respectively.

978-1-4244-5638-3/10/$26.00 ©2010 IEEE



(a) (b)

Fig. 1. Routing path distribution and trace back: (a) Routing direction distribution, (b) An example of routing path generated from OPNET

For a source node A to forward a packet, we can roughly split the area surrounding grids A into two equal size sections: the section that moves the packet forward towards B and backward away from B, shown in Fig. 1(a) & (b). As analyzed in equation (1), for security level β, the routing distribution density for the backward (shaded) area is $(\beta/2)/2\pi = \beta/4\pi$, while the density for the forward section is $(1-\beta/2)/\pi + \beta/4\pi = (4-\beta)/4\pi$. Therefore, the probability for the packet to be sent backward is $\beta/4$ and forward is $1-\beta/4$.

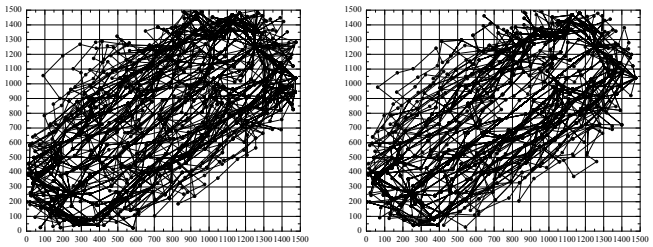
Based on this analysis, we can derive that when an adversary receives a packet in the sensor network, the immediate previous hop may be located at any direction. The probability that the previous hop is located between the current node and the sink node is $\beta/4$ and the probability that the node is away from the sink is $1-\beta/4$.

According to our assumption, regardless of where the previous sending node is located, when an adversary receives a packet, he is able to move to the previous node. Since we also assume that the adversary is only able to monitor a small section of the entire sensor network, once he moves to the very first node that he is able to monitor, he will not be able to further traceback to the actual source node.

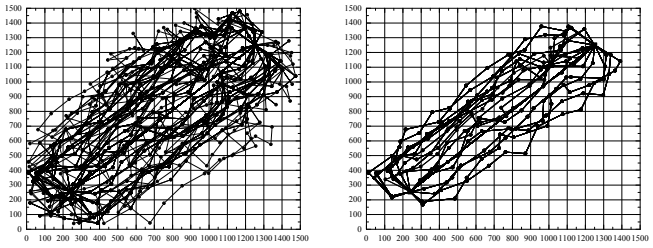
When a node transmit multiple messages, Fig. 2 gives the routing path distribution for different security levels using OPNET, where each line in the figure is a routing path of a message. It can be seen that the routing paths spread into a very wide area. A larger security level requires more effort to intercept a communication of a source since it triggers more random walking, and results in wider path distribution. Therefore, the adversary has to monitor a larger area in order to intercept a packet.

Since we assume that each node has the knowledge of the energy level of its adjacent neighboring grids, each sensor node can update the energy levels based on the detected energy usage. The actual energy will be updated periodically. For wireless sensor networks with non-replenishable energy resource, the energy level is a monotonically decreasing function. The updated energy level should never be higher than the predicated energy level since the predicted level is calculated based on only the detected usage. If the updated energy level is higher than the predicted level, the node must have be compromised and should be excluded from its adjacent neighboring grids.

In addition, for a node with low energy level that is caused by an excessive usage due to security attacks, according to our design these nodes will be filtered out of the pool for active routing selection. Therefore, this design can minimize the possibility for denial-of-service (DoS) attacks.



(a) (b)



(c) (d)

Fig. 2. Routing path statistics for different security parameters β for a target area of 1500×1500 with source node located at $(234, 255)$ and sink located at $(1250, 1250)$: (a) $\beta = 1$, (b) $\beta = 0.75$, (c) $\beta = 0.5$, (d) $\beta = 0$

VI. Performance Evaluation and Simulation Results

We will analyze the performance of the proposed SEAR algorithm for routing efficiency and energy balance. All our simulations were conducted in a targeted sensor area of size 1500×1500 meters. The targeted area is divided into grids of 15×15. We randomly spread 1000 sensor nodes in the this domain.

A. Routing Efficiency

Based on our design, we will first compute the number of packets that will be routed backward away from the sink. From Fig. 1(a), we can compute the number of packets that will be routed backward away from the sink as $\beta/4\pi \times \pi = \beta/4$ due to random walking. The redundancy that will be added to the routing path is estimated as $\beta/2$. In addition to random walking, the node may also be routed backward if the energy levels of the nodes in the direction towards the sink are all low. The percentage for this case is roughly 1.43%. Therefore, the average number of hops needed to forward a packet to the sink node can be calculated as $h_0 \times (1 + \beta/2 + 2 \times 0.0143)$, where h_0 is the required number of hops for security level $\beta = 0$.

We conduct simulation of the proposed SEAR using OPNET to measure the average number of hops for 4 different security levels. We assume that all sensor nodes will have equal amount initial energy and $\alpha = 0.5$. Table I shows the simulations results. The statistics of Table I was generated before any major section of the sensor node dies. We can see that the average number of hops in our simulation coincides with the theoretical analysis in the number of hops excellently.

From our simulation, we also see that as the energy level goes down, the routing path will be spread wider for better energy balance. This is exactly what we expect.

TABLE I
ROUTING HOPS FOR DIFFERENT SECURITY PARAMETERS

Security parameter	Average hops in simulations	Estimated SEAR hops
0	11.65	11.65
0.5	13.62	13.63
0.75	14.98	14.96
1	16.42	16.29

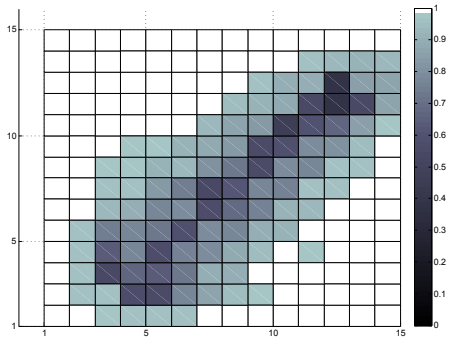


Fig. 3. Remaining energy distribution statistics for security parameter $\beta = 1$ after transmission of 300 packets

B. Energy Balance

SEAR algorithm is designed to balance the overall sensor network energy consumption in the grid and among the grids and thereby extend the lifetime of the sensor network. The ECB α is introduced to balance the overall energy usage by minimizing energy consumption of the sensor nodes with low energy levels. As α increases, better energy balance can be achieved. However, the number of routing hops may increase. So the overall energy consumption may go up. In fact, while the energy balance strategy can balance the overall network energy level, it may increase the number of routing hops and equivalently energy consumption.

In SEAR scheme, the parameter α can be adjusted to achieve the expected efficiency, routing security and energy balance. From a long run, we expect the number of routing hops to be comparable for all different α values. In our simulations, we set $\alpha = 0.5$ and there is only one source node. The energy consumption is spread over a large area between this node and the sink, see Fig. 3. Our simulations also demonstrate the SEAR can extend the lifetime of the sensor network and increase the number of messages that can be transmitted extensively.

C. Delivery Ratio

Our simulation results also show the proposed SEAR can ensure high message delivery ratio. It is also interesting to point out that while a larger security level requires more energy consumption, it also provides a higher message delivery ratio due to decrease of the number of dead end and loops. In our simulations, the message delivery ratio for security level 0 is only 94% for the first 1000 messages, while the delivery ratio for security level 1 is 97.2%.

VII. CONCLUSIONS

In this paper, we presented SEAR to balance energy consumption and increase the network lifetime. SEAR also has the flexibility to provide routing security and source privacy. Both theoretical analysis and simulation results show that SEAR has excellent routing performance in terms of energy balance and routing path distribution for routing path security.

ACKNOWLEDGEMENTS

The first author's research was partially supported by the China Scholarship Council. The second author's research was supported in part by the NSF under grants CNS-0845812 and CNS-0848569.

REFERENCES

[1] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *MobiCom'2000*, (New York, NY, USA), pp. 243 – 254, 2000.
[2] J. Li, J. Jannotti, D. S. J. D. C. David, R. Karger, and R. Morris, "A scalable location service fo geographic ad hoc routing," in *MobiCom'2000*, pp. 120 – 130, ACM, 2000.
[3] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy-aware routing: A recursive data dissemination protocol for wireless sensor networks," *UCLA Computer Science Department Technical Report, UCLA-CSD*, May 2001.
[4] T. Melodia, D. Pompili, and I. Akyildiz, "Optimal local topology knowledge for energy efficient geographical routing in sensor networks," in *Proc. IEEE INFOCOM*, vol. 3, pp. 1705 –1716 vol.3, March 2004.
[5] K. Yu and S. Bu, "Loop-free greedy routing in ad hoc or sensor networks using muti-hop geographic information," in *IEEE ICIS'2009*, vol. 3, pp. 328 –332, Nov. 2009.
[6] Q. Fang, J. Gao, and L. Guibas, "Locating and bypassing routing holes in sensor networks," in *Proc. IEEE INFOCOM*, vol. 4, pp. 2458 – 2468, march 2004.
[7] G. Zhao, J. Li, X. Liu, and A. Kumar, "Lifetime-aware geographic routing in wireless sensor networks," in *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery 2009*, pp. 355 –362, Oct. 2009.
[8] I. Stojmenovic and X. Lin, "Power-aware localized routing in wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 12, pp. 1122 –1133, Nov. 2001.
[9] J. Kuruvila, A. Nayak, and I. Stojmenovic, "Hop count optimal position-based packet routing algorithms for ad hoc wireless networks with a realistic physical layer," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 1267 – 1275, june 2005.
[10] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," *ICDCS*, pp. 599–608, June 2005.
[11] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *SASN*, pp. 88–93, ACM, 2004.
[12] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in *Proceedings of IEEE SECON 2009*, (Rome, Italy.), June 22-26, 2009.
[13] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in *to appear in the Proceedings of IEEE INFOCOM 2010*, (San Diego, USA.), March 15-19, 2010.
[14] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 829–835, April 2006.
[15] L. Hu and D. Evans, "Localization for mobile sensor networks," in *MobiCom'04*, (New York, NY, USA), pp. 45–57, ACM, 2004.
[16] H. Chan and A. Perrig, "Pike: peer intermediaries for key establishment in sensor networks," *Proceedings of IEEE INFOCOM*, vol. 1, pp. 524–535 vol. 1, March 2005.
[17] J. Hill, R. Szewczyk, S. H. A. Woo, D. Culler, and K. Pister, "System architecture directions for networked sensors," in *Proceedings of ACM ASPLOS IX*, November 2000.
[18] M. Ye, C. Li, G. Chen, and J. Wu, "EECS: an energy efficient clustering scheme in wireless sensor networks," in *IPCCC*, pp. 535–540, April 2005.
[19] J. Neander, E. Hansen, M. Nolin, and M. Bjorkman, "Asymmetric multi-hop communication in large sensor networks," in *2006 1st International Symposium on Wireless Pervasive Computing*, Jan. 2006.
[20] O. Younis and S. Fahmy, "Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, pp. 366–379, Oct.-Dec. 2004.