In Proceedings of 17th International IEEE Conference on Computer Communications and Networks, August 2008, pp. 1-6

A Power-Preserving Broadcast Protocol for WSNs With DoS Resistance

Chien-Chun Ni, Tien-Ruey Hsiang
National Taiwan University of
Science and Technology
Taipei, Taiwan 106
Email: (m9515066, trhsiang)@mail.ntust.edu.tw

J. D. Tygar
University of California, Berkeley
Berkeley, CA 94720
Email: tygar@cs.berkeley.edu

***Abstract*—Broadcast presents a special challenge for Wireless Sensor Networks (WSNs). In some situation such as time synchronization or building routing path, broadcasting messages must be securely transmitted to all nodes, but this process is subject to attack by adversaries. For example, an adversary may try to waste the battery power of intermediate nodes by forcing a compromised node to repeatedly rebroadcast, thus causing a Denial-of-Service (DoS) attack. One way to solve this problem is use only part of the nodes in the network as the intermediate nodes, limiting the effects of the attack. In this paper, we propose a novel broadcast protocol: BrOadcast Power Preserving (BOPP). In BOPP, a packet reception reliability metric of each network component is discovered. This reliability score gives the packet reception rate of each communication edge in the network. With the scoring metric, BOPP can judge the network reliability from time to time and adapt the network to provide maximum reliability while minimizing the energy cost. This enables the network to resist DoS attacks.**

***Index Terms*—broadcasting, dominating set, sensor networks, routing protocols.**

I. Introduction

This paper gives a protocol for assignment of resources in wireless sensor networks (WSNs). We give a broadcast protocol (BOPP, BrOadcast Power Preserving protocol) that involves some, but not all, intermediate nodes to achieve broadcast while balancing these two properties:

- reaching a large number of nodes with high probability; and
- using few resources, in terms of broadcasting packets (which requires and consumes power).

To achieve this tradeoff, we measure the reliability of internode direct communication, then use a greedy algorithm to select a subset of those nodes, and broadcast using the chosen subset as intermediate repeater nodes. We contrast our system with a flooding approach (involving *all* nodes) and with multipoint relays [1] and show that our system has substantially better results.

A Wireless Sensor Network (WSN) typically is a set of sensor nodes and base stations. A wireless sensor node often contain a low-cost processor, small amount of memory, limited battery power, limited wireless radio range, and appropriate built-in sensors for sensing the environment. These networks can be used to collect information in harsh environments.

Security issues need special attention in wireless sensor networks because of the strict hardware limitation. The limited radio range and battery power means that power for transmission is a scarce resource.

Denial-of-Service (DoS) attacks are a particular concern. If an adversary can cause a node to repeatedly broadcast messages [2], he can successfully drain power from that node. Worse, these messages will be rebroadcast by other intermediate nodes, draining their power. We need a broadcast protocol with a limited number of relay nodes to reduce the effect of DoS attacks.

The simplest broadcast method is *flooding*: every node in the network retransmits the first copy of every message it receives. This method is simple to implement and gives robust coverage of nodes. However, it uses a large amount of power. To increase the network lifetime, the most common solution is to choose a subset of nodes as *relay nodes*. One common method is to calculate the *Connected Dominating Set (CDS)*, or a *Multipoint Relay Set (MPR)* (these are discussed in the next section). Unfortunately, calculating a connected dominating set and finding a multipoint relay set with minimal size are both NP-hard [1], so only approximate solutions can be calculated.

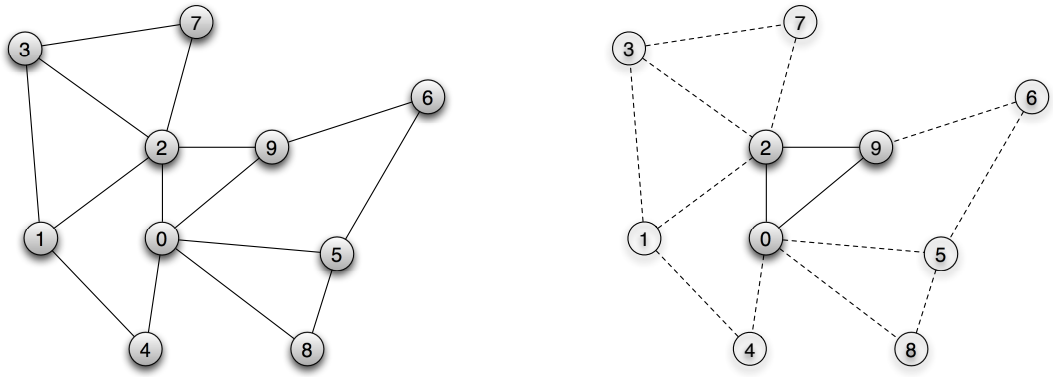
Unstable wireless signals subject to collisions, buffer overflows, and packet latencies may prevent broadcast messages from reaching all nodes. If there is only one route from the source node to the destination node, packet loss results in non-delivery of messages. Multi-path routing can alleviate the effect of packet loss.

In this paper we introduce a novel broadcasting protocol that can reduce the effect of packet loss in the network and decrease the size of the relay set. This protocol uses a reliability metric to compute a set of relaying nodes. By using smaller sets, network reliability is maintained.

II. Preliminaries

Various methods have been proposed for WSN broadcast. In [3], broadcasting protocols are categorized into four families: simple flooding, probability based methods, area based methods and neighbor knowledge methods. In simple flooding, each node immediately rebroadcasts the first instance of every packet [4]. The probability based method in [5] is similar to flooding, except that each node rebroadcasts with a certain

978-1-4244-2390-3/08/$25.00 ©2008 IEEE



(a) CDS: Before

(b) CDS: After

Fig. 1. An example of Connected Dominating Set (CDS). Fig. 1(a) shows every node as a relay node. Fig. 1(b) shows the CDS as the relay set; it needs only 3 nodes to transmit messages to the whole network.

probability. In area based methods [5], nodes are assumed to have a common transmission range. A node rebroadcasts only when reaching sufficient new coverage area. In neighbor knowledge methods [1, 6], the relay set is chosen using knowledge of each node's neighbor or child set.

Using neighbor knowledge to choose rebroadcasting nodes is a problem related to finding a *connected dominating set* (CDS): for a connected graph $G(V, E)$ where V is the vertex set and E is the edge set, a subset $R \subseteq V$ is called a *connected dominating set* if R is connected and any vertex in V is either in R or is adjacent to a node in R. Fig. 1 shows a CDS. If we let the minimal CDS be the relay set in broadcast, the transmission cost of broadcast will also be minimized. It is known that the problem of finding the smallest dominating set in a weighted graph is NP-hard [7]. Therefore, we must use an approximation algorithm for the minimal CDS problem. In [6, 8, 9], distributed algorithms are proposed to construct the dominating sets in the sensor network.

Qayyum et al. proposed *multipoint relays* (MPR) [1, 10] to reduce the size of relay sets. This method requires nodes have the knowledge of the network topology within a 2-hop radius. The nodes include the 1-hop neighbors in a greedy fashion to be the MPR that can reach the largest 2-hop neighborhood, until every node in the network can be reached by the MPR.

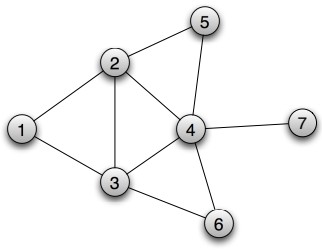


Fig. 2. Suppose node 1 is the base station. The MBR relay set is {2,3,4}; first consider 1-hop neighbors, choose node 2 to cover node 4 and node 5, then choose node 3 to cover node 6, and then choose node 4 to cover node 7. However, the minimal relay set is actually {2,4} or {3,4}.

The protocol is improved in [11]. In [12] a *tree based data collection scheme* (TBDCS) is proposed using vertex covers to choose covering nodes. Both MPR and TBDCS use neighbor knowledge based on the child set to decide the relay set. The links between the siblings are ignored. The ignored siblings problem is shown in Fig. 2.

To help address the ignored siblings problem, we can consider both the messages from *parent nodes* and from *neighbor nodes*. If a node has more broadcasting nodes near it, it has a higher probability of receiving the message and is more resilient to packet loss.

When multiple nodes broadcast in a compact region, the broadcast packets might interfere with each other and cause packet lost. These effects have been actually observed in Berkeley motes running broadcast; a number of instances are documented by Perrig and Tygar [13, 14]. Using part of the nodes in the network to be the relay node can decrease the node number within this compact region, also reduce the interference effects.

III. Broadcast Protocol

As mentioned earlier, multi-path routing reduces message loss. In multi-hop wireless networks, two nodes communicate over a (multi-hop) routing path. Let the packet reception rate be the weight of each edge. We can compute each node's packet reception rate. Using this data we can find a relay subset to broadcast messages to the whole network. Below we propose a novel, robust broadcast protocol that balances packet reception reliability and the size of relay sets.

A. Network Definition

A wireless sensor network is represented by a graph $G = (V, E)$ where V is the set of nodes, and $E \subseteq V^2$ is the edge set that gives available communication links between nodes. If an edge (u, v) belongs to E, then u and v can communicate to each other, and the packet reception rate of edge (u, v) is $p(u, v)$.

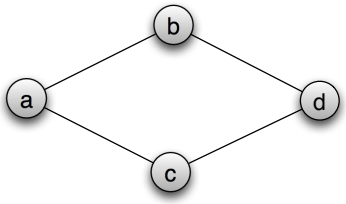


Fig. 3. A example of a network with parallel routing paths $a \to c \to d$ and $a \to b \to d$ from a to d. Every solid link between nodes is weighted with the packet reception rate between these two nodes.

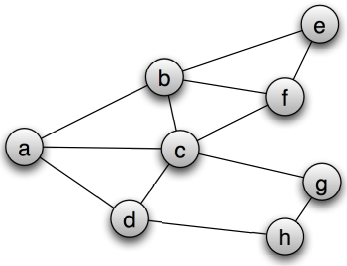


Fig. 4. An example of network communication where node a is the base station. There are multiple paths from node a to node f.

For all $x \in V$, $hop(x)$ is defined to be the shortest distance to the base station. With this definition, node x's parent set, child set, and neighbor set are defined as follows:

$$\begin{aligned} Parent(x) &= \{a \in V | hop(a) = hop(x) - 1, (a,x) \in E\} \\ Child(x) &= \{a \in V | hop(a) = hop(x) + 1, (a,x) \in E\} \\ Nbr(x) &= \{a \in V | hop(a) = hop(x), (a,x) \in E\} \end{aligned}$$

B. Node Reliability Score

In wireless communication some messages are lost during broadcast. If messages are redundantly routed over multiple paths then reliability increases. Given the packet reception rate r along every edge, we can compute the node's reliability score.

For every pair of nodes m and n that may communicate, we define the reliability score $s(n)$ as the packet reception rate of the node n. If there is only one path, $s(n) = r(m,n) \cdot s(m)$ where $s(m)$ is the score for node m. If there are multiple paths from parents, the score of the nodes in the parallel case can be defined as follows:

$$s(n) = 1 - \prod_{\forall x \in Parent(n)} (1 - s(x) \cdot r(x,n))$$

Suppose node a denotes the base station and there exist two routing paths $a \to b \to d$ and $a \to c \to d$, both of them capable broadcast the message to node d, as illustrated in Fig. 3. The reliability score of node d is

$$s(d) = 1 - (1 - s(b) \cdot r(b,d))(1 - s(c) \cdot r(c,d)).$$

This method can only handle the score with the shortest path to each node. In real network communications, the routing path of the broadcasting messages which transmitted with shortest paths are only parts of transmission. Fig. 4 shows one example. From the base station node a to node f, there are various paths such as $a \to b \to c \to f$, $a \to c \to b \to e \to f$, or $a \to c \to f$. Here is an approximation: for every route from node a to node b, we only consider the path length within $hop(b) + 1$. We use two scores to describe $hop(b) + 1$ and $hop(b)$. We denote the score that holds the shortest path (that is, $hop(b)$) as $s_d(b)$; we denote the route's combined scores with length $hop(b) + 1$ as $s_c(b,x)$, $\forall x \in Nbr(b)$. Then we can approximate the score

$$s(b) = 1 - (1 - s_d(b)) \prod_{\forall x \in Nbr(b)} (1 - s_c(b,x))$$

For the node b in Fig. 4, the routes under consideration are $a \to b$ and $a \to c \to b$. To compute the score of every node, we need to compute the score recursively.

In Fig. 4, we first consider the scores of the set $Child(a) = \{b, c, d\}$. For node b,

$$\begin{aligned} s_d(b) &= s(a) \cdot r(a,b) \\ s_c(b,c) &= s_d(c) \cdot r(c,b) \end{aligned}$$

hence

$$s(b) = 1 - (1 - s_d(b))(1 - s_c(b,c))$$

Similarly, we get

$$\begin{aligned} s(c) &= 1 - (1 - s_d(c))(1 - s_c(c,b))(1 - s_c(c,d)) \\ s(d) &= 1 - (1 - s_d(d))(1 - s_c(d,c)) \end{aligned}$$

For node f, $|Parent(f)|$ is greater than one, which means that there are multiple paths from parents, so the score s_c is

$$s_c(f) = 1 - (1 - s(b) \cdot r(b,f))(1 - s(c) \cdot r(c,f))$$

The combined score is

$$s_c(f) = s(e) \cdot r(f,e)$$

The remaining scores of every node is computed in a similar way. Fig. 5 shows a graph where nodes in the network are labeled with reliability scores, and the nodes with the same hop grouped in common shaded areas.

C. The Scoring Metric And The Broadcast Relay Set

We use the sum of all the scores of nodes to be a metric for the network, and we define the *maximal metric score* to be the score when every node in the network is a relay node (simple flooding). We use a greedy algorithm to minimize the size of the relay set.

Define $sum(N,U)$ to be the sum of all the nodes' reliability scores, where R is the relay set and $U = N \setminus R$ is the node set containing nodes not relaying messages. The scoring metric of the network $SM(N,U)$ is

$$SM(N,U) = \frac{sum(N,U)}{sum(N,\{\phi\})} \times 100\%.$$

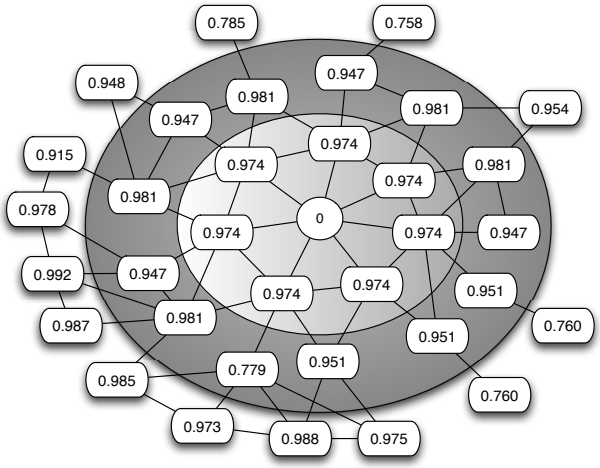


Fig. 5. A network graph where the nodes with the same hop count are grouped in colored bands.

When U is empty, every node in the network is in the relay set, and $SM(N, U) = 100\%$. As we remove nodes from the relay set, the score SM decreases. To prevent the network from being disconnected, SM becomes zero if there exists a node in the network whose reliability score is zero.

We use a greedy algorithm to choose U. At each step, the algorithm chooses a node to join U causing the smallest drop in SM. We do not drop below a threshold value. This acts as a parameter of broadcast reliability.

To maximize the life of the wireless sensor network, when the energy of a node drops below a threshold the node sends an alert to the base station. The low battery node is removed from the relay set and the relay set is rebuilt.

IV. Evaluation

A. Simulation Setup

In this section, we describe an experiment comparing BOPP and MPR in terms of the average size of the relay node set and the broadcast packet delivery rate. Our simulation randomly generated a network with sensor nodes within a two dimensional area of 400×400 units. Each node had a fixed transmission range of 10 units. To generate a network of fairly even distribution, no two nodes were allowed to be within 5 units of each other. The communication links between nodes have different packet delivery probabilities. We only considered connected networks.

The simulation considered both stable and unstable networks. In stable networks, the packet reception rate was randomly, uniformly set between 80% to 100%. In unstable networks, the rate was randomly, uniformly set between 20% to 100%. BOPP and MPR were tested on 100 stable networks and 100 unstable networks. The results were obtained by averaging the 100 simulations for both stable and unstable networks.

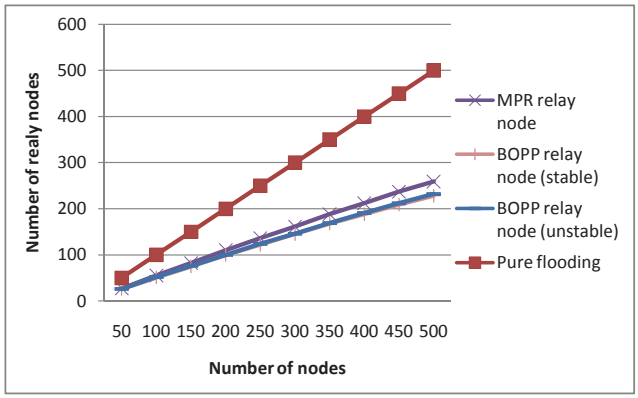


Fig. 6. A comparison of the average relay node set number required by pure flooding, MPR, and BOPP taken over 100 randomly generated stable networks (that is networks where neighboring node probability rate was set randomly, uniformly between 80% and 100%). We also show the average relay node set number required by BOPP taken over 100 randomly generated unstable networks (that is, networks where the neighboring node probability rate was set randomly, uniformly between 20% and 100%). The lower number of relay nodes, the lower amount of energy consumption.

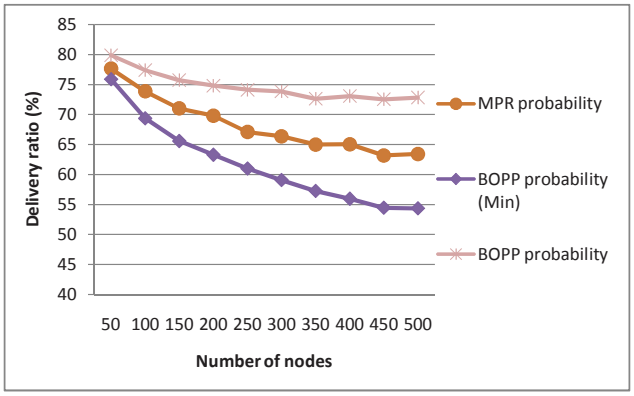


Fig. 7. A comparison of the average packet delivery rates associated with MPR and BOPP taken over 100 randomly generated, stable networks.

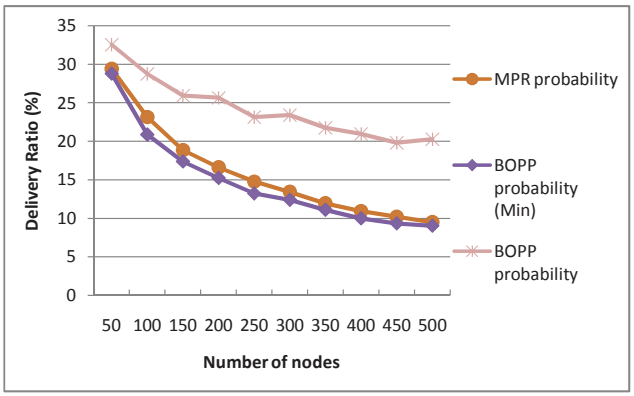


Fig. 8. A comparison of the average packet delivery rates associated with MPR and BOPP taken over 100 randomly generated, unstable networks.

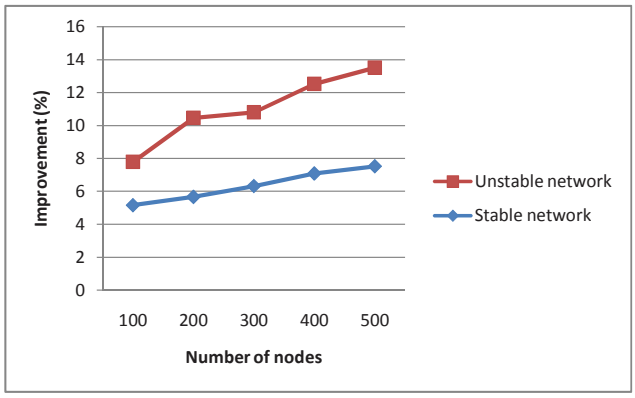


Fig. 9. Energy costs are reduced in BOPP, compared to MPR in both stable and unstable networks.

B. Simulation Result

Fig. 6 shows the simulation result for MPR and pure flooding in stable networks, and BOPP in both stable and unstable networks. BOPP needs about 10% fewer nodes than MPR. Since most of the energy consumption in WSNs comes from radio communication, the smaller the number of required relay nodes, the lower the amount of energy consumed.

Fig. 7 and 8 compare MPR and BOPP in terms of packet delivery rates in both stable and unstable networks respectively. In Fig. 7 and Fig. 8, there are two BOPP curves: one shows the delivery rate when BOPP is used with the same number of relay nodes as MPR; the other shows the rate when a minimal number of relay nodes are used in BOPP. When the same number of relay nodes is used by both MPR and BOPP, then BOPP has about 10% higher packet delivery rate than MPR, in both stable and unstable networks. Compared with MPR, the simulation results of both stable and unstable networks show that BOPP requires about 10% fewer relay nodes while maintaining the same delivery rate.

Since BOPP offers the desired packet delivery rate, we can also compare BOPP and MPR in terms of energy efficiency. Here we compare the energy efficiency of packet delivery rate that every relay node can provide. In our simulation, BOPP provided at least 5% improvement in energy consumption in stable networks (Fig. 9). As the network scales up, the improvement becomes greater and greater. For unstable networks, BOPP presented about a 10% energy improvement.

C. Resistance Against Denial-of-Service Attack

Denial-of-Service (DoS) attacks can be a serious problem for wireless sensor networks. If an adversary can flood a wireless sensor networks with messages, he can rapidly drain battery resources. Compared with a flooding protocol in which all of the nodes rebroadcast messages, BOPP use only 45% of resources. This provides resistance against DoS attacks. See Fig. 6.

V. Conclusions

We proposed a new broadcast algorithm providing maximum reliability while minimizing the energy cost. Compared with MPR, BOPP uses fewer relay nodes and provides the desired packet delivery rate. We also show that BOPP provides better performance in larger unstable networks, and the simulation result shows that BOPP saves more energy and is more resilient to DoS attacks. In future work, we will try to find out a lightweight method replacing the greedy algorithm to choose the relay nodes. In a longer presentation of this work, we will present a full analysis of our algorithm. We also plan to investigate nodes dynamically joining and leaving networks in the future.

Acknowledgment

This effort was partially supported by the International Collaboration for Advancing Security Technology (iCAST) and Taiwan Information Security Center (TWISC) projects, sponsored by National Science Council under the grants NSC 96-3114-P-001-002-Y and NSC96-2219-E-009-013 respectively.

This work was also supported in part by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), BT, Cisco, ESCHER, HP, IBM, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia, and United Technologies.

References

[1] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint relaying for flooding broadcast messages in mobile wireless networks," *HICSS '02: Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02)*, vol. 9, pp. 298–307, 2002.

[2] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer*, vol. 35, no. 10, pp. 54–62, 2002.

[3] B. Williams and T. Camp, "Comparison of broadcasting techniques for mobile ad hoc networks," *MobiHoc '02: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 194–205, 2002.

[4] C. Ho, K. Obraczka, G. Tsudik, and K. Viswanath, "Flooding for reliable multicast in multi-hop ad hoc networks," *DIALM '99: Proceedings of the 3rd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, pp. 64–71, 1999.

[5] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," *MobiCom '99: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 151–162, 1999.

[6] I. Stojmenovic, M. Seddigh, and J. Zunic, "Dominating sets and neighbor elimination-based broadcasting algorithms in wireless networks," *IEEE Transactions on Parallel Distributed Systems*, vol. 13, no. 1, pp. 14–25, 2002.

[7] S. Guha and S. Khuller, "Approximation algorithms for connected dominating sets," *European Symposium on Algorithms*, pp. 179–193, 1996.

[8] J. Wu and H. Li, "On calculating connected dominating set for efficient routing in ad hoc wireless networks," *DIALM '99: Proceedings of the 3rd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications*, pp. 7–14, 1999.

[9] M. Min, H. Du, X. Jia, X. Jia, C. X. Huang, S. C.-H. Huang, and W. Wu, "Improving construction for connected dominating set with steiner tree in wireless sensor networks," *Journal of Global Optimization*, vol. 35, no. 1, pp. 111–119, 2006.

[10] C. Adjih, P. Jacquet, and L. Viennot, "Computing connected dominated sets with multipoint relays," *Ad Hoc and Sensor Wireless Networks*, vol. 1, no. 1-2, pp. 27–39, 2005.

[11] F. Ingelrest and D. Simplot-Ryl, "Maximizing the probability of delivery of multipoint relay broadcast protocol in wireless ad hoc networks with a realistic physical layer," *ArXiv Computer Science e-prints*, January 2007.

[12] H. Li, H. Yu, and A. Liu, "A tree based data collection scheme for wireless sensor network," *ICNICONSMCL '06: Proceedings of the International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*, pp. 119–123, 2006.

[13] A. Perrig and J. D. Tygar, *Secure Broadcast Communication: In Wired and Wireless Networks*. Springer, 2002.

[14] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, "SPINS: security protocols for sensor networks," *ACM Journal of Wireless Networks*, vol. 8, no. 5, pp. 521–534, 2002.