A Power-Preserving Broadcast Protocol for Wireless Sensor Networks

C.C. Ni
Department of Computer Science and Information Engineering
National Taiwan University of Science and Technology, Taipei, Taiwan
E-mail: m9515066@mail.ntust.edu.tw

T.-R. Hsiang
Department of Computer Science and Information Engineering
National Taiwan University of Science and Technology, Taipei, Taiwan
E-mail: trhsiang@mail.ntust.edu.tw

J.D. Tygar
Department of Electrical Engineering and Computer Sciences
University of California, Berkeley, Berkeley, CA 94720
Email: tygar@cs.berkeley.edu

Abstract: Broadcast presents a special challenge for Wireless Sensor Networks (WSNs). In situations such as time synchronization or routing path establishment, broadcasted messages must be securely transmitted to all nodes, but this process is subject to attack launched by adversaries. For example, an adversary may attempt to waste the battery power of intermediate nodes by forcing a compromised node to repeatedly rebroadcast, thus forming a denial-of-service (DoS) attack. One solution to this problem is to limit the number of message-relaying nodes in the network, thus reduces the energy required to broadcast a message. In this paper, we present a power-preserving broadcast protocol (BOPP) that utilizes a packet reception reliability metric. The reliability score is computed for every communication link in the network. BOPP then selects a set of repeater nodes that most contributes to a broadcast. The selection process is repeated whenever the score distribution changes.

Keywords: broadcast; dominating set; sensor network; routing protocol.


1 Introduction

This paper presents 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 (Qayyum et al. (2002)) 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 often require special attention in wireless sensor networks because of the strict hardware limitation.

Copyright © 200x Inderscience Enterprises Ltd.
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 broadcast 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 select a set of relay nodes. While using smaller sets, network reliability is still maintained.

2 Preliminaries

Various methods have been proposed for WSN broadcast. In Williams and Camp (2002), broadcast protocols are categorized into four families: simple flooding, probability based methods, area based methods and neighbor knowledge methods. In simple flooding, every node immediately rebroadcasts the first instance of every packet (Ho et al. (1999)). The probability based method in Ni et al. (1999) is similar to flooding, except that every node now rebroadcasts with a certain probability. In area based methods by Ni et al. (1999), nodes are assumed to have a common transmission range. A node rebroadcasts only when reaching sufficient new coverage area. In neighbor knowledge methods by Qayyum et al. (2002) and Stojmenovic et al. (2002), 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). Fig. 1(b) shows every node as a relay node. Fig. 1(a) shows the CDS as the relay set; it needs only 3 nodes to transmit messages to the whole network.

(a) CDS: Before

(b) CDS: After

Figure 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.

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 (Wood and Stankovic (2002)), 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 consumes 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 shown NP-hard by Qayyum et al. (2002), so only approximate solutions can be calculated.
However, the minimal relay set is actually \{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\}.

sets are often unnecessarily larger. The ignored siblings problem is shown in Fig. 2.

To help address the ignored siblings problem, we consider the messages from parent nodes and from neighbor nodes. If one node can receive the messages from the neighbor nodes, its parents may not need to rebroadcast to save energy. On the opposite side, 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 may interfere with each other and cause packet loss. These effects have been actually observed in Berkeley motes running broadcast; a number of instances are documented by Perrig and Tygar (2002); Perrig et al. (2002). Using part of the nodes to be the relay nodes can decrease the node number within this compact region, also reduce the interference effects and packet loss.

To measure the packet transmission status between nodes, IEEE 802.15.4 protocol provided received signal strength index (RSSI) and link quality index (LQI) to estimate the radio signal strength and the radio signal quality. RSSI is a simple circuit to measure the strength of an incoming signal; LQI is a metric that measures the error in the incoming modulation of successfully received packets. Polastre et al. (2005) compared the relation of RSSI and LQI with packet reception rate. Their results showed that LQI represents a better correspondence to the packet reception rate than that of RSSI.

In terms of wireless sensor networks, LQI can be provided by CC2420, which is the radio transceiver used on the latest wireless sensor motes such as micaZ, Telos, and Intel Mote2. With LQI, we can easily collect the real-time approximated packet reception rate of each connection, and estimate the probability of successfully reception of each nodes. By knowing the packet reception rate between every link, a more reliable intermediate relay set can be provided for packet transmission.

### 3 Broadcast Protocol

As mentioned earlier, multi-path routing reduces message loss. In multi-hop wireless sensor networks, two nodes communicate over a (multi-hop) routing path. Let the packet reception rate be the weight of each edge, we can set up a mathematical model to estimate each node’s probability to get the broadcast messages. Using this calculated model, we can find a relay subset to broadcast messages to the whole network. In this section, we propose the robust broadcast protocol that balances packet reception reliability and the size of relay sets.

#### 3.1 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 with each other, and the packet reception rate of edge $(u, v)$ is $r(u, v)$.

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:

$$
\text{Parent}(x) = \{ a \in V | hop(a) = hop(x) - 1, (a, x) \in E \}
$$

$$
\text{Child}(x) = \{ a \in V | hop(a) = hop(x) + 1, (a, x) \in E \}
$$

$$
\text{Nbr}(x) = \{ a \in V | hop(a) = hop(x), (a, x) \in E \}
$$

#### 3.2 Node Reliability Score

In wireless communication some messages are lost during broadcast. If messages are redundantly routed over multiple paths, the reliability improves. 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 of node $m$ and $r(m, n)$ is the estimated packet reception rate of the connection between $m$ and $n$. If there are multiple paths from parents, the score of the nodes in the multiple sources can be defined as follows:

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

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

$$
s(d) = 1 - (1 - s(b) \cdot r(b, d))(1 - s(c) \cdot r(c, d)).
$$
The above method can only handle the score of the shortest path to each node. In real network communication, the routing path of the broadcasting messages transmitted with shortest paths are only parts of transmission. In Fig. 4 shows one example. From the base station node a to node f, there are multiple paths such as a → b → c → f, a → c → b → e → f, or a → c → f. Suppose 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). Let the score that holds the shortest path (that is, hop(b)) be $s_d$, and the route’s combined scores with length hop(b) + 1 be $s_c(b, x), \forall x \in Nbr(b)$. We can approximate the score

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

For node b in Fig. 4, the routes under consideration are $a \rightarrow b$ and $a \rightarrow c \rightarrow b$. To obtain 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,

$$s_d(b) = s(a) \cdot r(a, b)$$

$$s_c(b, c) = s_d(c) \cdot r(c, b)$$

hence

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

Similarly, we get

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

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

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

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

The remaining scores of every node are computed in a similar way. Fig. 5 shows a graph where nodes in the network are labeled with reliability scores, and nodes with the same hop grouped in common shaded areas. The algorithm of computing the score is shown in Alg. 1.

**Algorithm 1 Node Scoring**

1. $G = Child(\text{base station})$
2. while $|G| \neq 0$
3. \hspace{1em} $\forall a \in G$, compute $s_d(a)$
4. \hspace{2em} Compute $s_c(a)$
5. \hspace{2em} Compute $s(a)$
6. \hspace{1em} $G_{Child} = Child(G)$
7. \hspace{1em} $G = G_{Child}$
8. end while

### 3.3 The Scoring Metric And The Broadcast Relay Set

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

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

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

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 \( SM \), this step will be continuously until the network become disconnect. The algorithm is shown in Alg. 2.

**Algorithm 2 Node Selection**

Require: input graph \( G \)

1: \textbf{while} \( G \) is connected and \( SM \) is above the threshold \textbf{do}
2: \hspace{1em} try to remove each node from relay set
3: \hspace{1em} move the less score drop node to \( U \)
4: \textbf{end while}

Moreover, if we want to make the communication more robust, we can also set a fixed lower bound of \( SM \). This lower bound acted as a parameter of broadcast reliability. With this lower bound, we have flexibility in choosing a relay set that provides needed broadcast reliability.

To maximize the lifespan of the wireless sensor network, a node sends an alert message to the base station when its remaining energy is lower than a threshold. The low battery node is then removed from the relay set and the relay set is rebuilt.

**4 Evaluation**

**4.1 Simulation Setup**

In this section, we conduct experiments to compare BOPP and MPR in terms of the average size of the relay node set, the broadcast packet delivery rate, and the total transmission counts. Our simulation randomly generates a network of sensor nodes within a two dimensional area of \( 400 \times 400 \) units. Each node has a fixed transmission range of 10 units. We generate the network in fairly even distribution since it represents the worst case, a denser network topology will behave better in terms of broadcast. In the experiment setting, nodes are at least 5 units away from 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 set uniformly distributed between 80% to 100%. In unstable networks, the rate was set uniformly distributed between 20% to 100%. BOPP and MPR were tested on 100 stable networks and 100 unstable networks. The averaged results are used to represent the performance of BOPP and MPR.

To evaluate the delivery ratio of BOPP and MPR, testing message is broadcasted from the base station via relay nodes to every node. The delivery ratio defined as the proportion of nodes with successful reception.

We also count the total number of transmissions, which directly relates to the energy consumption, of BOPP and MPR. In every experiment, we let the base station broadcast 100 messages, then gather the total counts of retransmission in the network. To collect the average data, the results are also collected from 100 different network topology.

**4.2 Performance Comparison**

We compare the number of relay node and the delivery ratio under pure flooding, MPR, and BOPP. For the relay nodes, fewer relay nodes means lower amount of energy cost for each broadcast, while more unused node can save more energy for other applications. For the delivery ratio, higher delivery ratio represents that broadcast messages have higher reliability to be received by all the destina-
Fig. 6 shows the simulation result for MPR and pure flooding in stable networks, and BOPP in both stable and unstable networks. BOPP needs 10% less nodes than MPR. Since most energy consumption in WSNs comes from radio communication, the smaller the number of required relay nodes, the fewer energy is consumed. Fig. 7 shows the comparison of total transmission counts. Flooding need the most transmission counts (which implies the most energy consumption) since every node relays each messages exactly once. Due to BOPP has smaller relay sets, it generates fewer relay transmissions than MPR. In the case of a stable network with 500 nodes, BOPP only needs 75% of transmissions than that of MPR.

Fig. 8 and 9 compare MPR and BOPP in terms of packet delivery rates in both stable and unstable networks respectively. In Fig. 8 and Fig. 9, 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 delivery 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 shows a 10% improvement of packet delivery rate over MPR, in both stable and unstable networks. Compared with MPR, the simulation results of both stable and unstable networks show that BOPP requires 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. 10). As the network scales up, the improvement becomes greater. For unstable networks, BOPP performs even better at a 10% improvement.
4.3 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 uses only 45% of resources. This provides resistance against DoS attacks. See Fig. 6.

5 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, the simulation result shows that BOPP saves more energy and is more resilient to DoS attacks. In future work, we will try to develop a fully distributed relay node selection mechanism based on BOPP. We also plan to investigate the case where nodes dynamically join and leave 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


