
Gerhard P. Hancke, C. Jaco Leuschner

Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Lynnwood Road, Pretoria, 0002.

ABSTRACT

The nature of wireless sensor networks necessitates specific design requirements, of which energy efficiency is paramount. In this paper we present SEER (Simple Energy Efficient Routing), a novel routing protocol for wireless sensor networks intended to optimise network lifetime. SEER uses a flat network structure for scalability and source initiated communication, along with event-driven reporting to reduce the number of message transmissions. Computational efficiency is achieved by using a relatively simple method for routing path selection. Routing decisions are based on the distance to the base station as well as on remaining battery energy levels of nodes on the path towards the base station. SEER minimizes the number of messages that are sent through the network and thus reduces the overall energy consumption. Simulation results show that SEER achieves significant energy savings for a set of specific conditions.

KEYWORDS: hierarchical routing, flat routing, wireless sensor networks, source initiated, destination initiated, energy consumption, energy efficiency, node lifetime, clustering, distributed sensing

1 INTRODUCTION

Wireless Sensor Networks was identified as one of the "21 ideas for the 21st century" [1] in 1999 and one of the "10 emerging technologies that will change the world" [2] in 2003. Such a network consists of wireless sensor nodes deployed in or close to the phenomenon that it has to monitor. Applications range from environmental monitoring to industrial sensing to military applications and far beyond. The development of this technology has been fuelled by advances in electronic miniaturisation (including micro electro-mechanical systems (MEMS) technology), wireless communication techniques and low-cost manufacturing.

Small, inexpensive, low-power, disposable sensors can be deployed in large numbers in environments ranging from the home to hostile and possibly inaccessible environments such as disaster areas or battlefields. They can be deployed manually or randomly by, for instance, dropping them from an aircraft. These sensor nodes are self-configuring and contain one or more sensors, embedded wireless communications and data processing components, but usually have a limited energy source. Due to the large number of nodes and the possibly very large number of sensing nodes, a WSN also has a base station. The sensing nodes (also known as a source node) have to route data from their environment to the base station (also known as a sink). The sink node collects and interprets the data from all the source nodes in the network. The sink node is usually connected to a wired network and does not have an energy limitation. The source nodes, on the other hand, are dependent on their limited batteries and drop out of the network when their batteries are depleted.

In this paper we present a routing protocol called Simple Energy Efficient Routing or SEER, designed to minimise complexity and maximise network lifetime.

In addition to the possibly very large number of sensing nodes, a WSN also has a base station. The sensing nodes (also known as a source node) have to route data from their environment to the base station (also known as a sink). The sink node collects and interprets the data from all the source nodes in the network. The sink node is usually connected to a wired network and does not have an energy limitation. The source nodes, on the other hand, are dependent on their limited batteries and drop out of the network when their batteries are depleted.

In this paper we present a routing protocol called Simple Energy Efficient Routing or SEER, designed to minimise complexity and maximise network lifetime.

The remainder of this paper is organized as follows: Section II presents existing routing protocol types for sensor networks with some of their advantages and disadvantages. SEER is presented in Section III and simulation results are shown in Section IV. Finally, Section V concludes this paper.

2 ROUTING PROTOCOLS OVERVIEW

The limited energy capacity of the sensor nodes necessitates energy efficient network design. Undoubtedly one of the most important tasks of a WSN routing protocol is to optimise the network lifetime. According to Intae et al. [3] the battery energy of a node is depleted by: (i) computational processing and (ii) transmission and reception of data to maintain the signal-to-noise ratio above a certain threshold. The latter is often the most energy intensive.

Many WSN protocols have been proposed ([4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], etc.). These protocols can be classified
as proactive, reactive or hybrid [32]. Proactive protocols compute all routes before they are needed, while reactive protocols compute routes on demand. Hybrid protocols make use of a combination of these two. Since a WSN can consist of thousands of nodes, the routing table that each node would have to keep could be huge and therefore proactive protocols are not suited to WSNs. Routing protocols can also be classified as direct communication, flat or clustered according to the way in which a node participates in the network. Direct communication is impractical in WSNs since it requires all the nodes to be able to communicate directly with the sink. In flat protocols, all the nodes in the network are equal and a node may find a route to the sink using multiple hops. Nodes close to the sink participate more than nodes further away. In clustering protocols, the network is subdivided into clusters of nodes with each cluster having a cluster head. The nodes within a cluster send messages only to the cluster head. The cluster head forwards all messages of its cluster towards the sink. The classification of WSN routing protocols is shown in Figure 1.

![Figure 1: Classification of WSN routing protocols.](image)

Although some authors, such as Jiang et al. [32], favour clustering, there are disadvantages that may impair network lifetime performance. In some clustering protocols, the cluster head or gateway is changed only at certain intervals. If the cluster head depletes its battery before another node becomes the cluster head, messages that are sent to the cluster head will be lost. The cluster head also depletes its energy faster than the other nodes. The clustering approach, therefore, depletes the energy of some nodes in the network much faster than other nodes. The disadvantage of having some nodes die faster than others is that the failure of one node might cause the network to become partitioned, which may lead to other nodes being cut off from the network.

Sensor nodes can be in one of four states, namely (i) transmit, (ii) receive, (iii) idle and (iv) sleep [24]. The largest part of a node’s energy is consumed while transmitting and receiving. Minimising the number of messages to be transmitted will therefore reduce the time spent in these states and subsequently increase the network lifetime.

Most protocols are destination initiated, which means that the sink node requests data from the sensor nodes and they in turn reply with data. One such protocol is Directed Diffusion [10], which has received a great deal of attention from the research community. A number of protocols have been derived from it, for example [12] and [19]. The problem with this approach is that the network is flooded with the request and the sink node needs to know the location of every sensor node in the network (location-based protocol). Source initiated protocols, on the other hand, send data to the sink at certain intervals or when certain events occur. This minimises the number of messages sent through the network.

The minimum cost forwarding algorithm (MCFA) [31] is an example of a source initiated protocol. It uses a flat network structure and proactive routing and assumes that the direction of routing is always known. One problem of MCFA is that nodes will deplete energy along certain paths if the minimum cost is not updated regularly. Another problem is that if hop count is used as the cost or if nodes are uniformly distributed and energy expenditure is used as the cost, multiple nodes will consider themselves on the minimum cost path and the protocol is reduced to flooding.

### 3 SIMPLE ENERGY-EFFICIENT ROUTING (SEER)

#### 3.1 Design Goals

There are many factors related to the inherent characteristics of WSNs that have to be considered in order to design an efficient WSN routing protocol. These factors include: node deployment, data reporting method, node and link heterogeneity, reliability, energy consumption, scalability, network dynamics, transmission media, connectivity, coverage, data aggregation and quality of service [33]. In this section we present SEER, designed to address some of the disadvantages described in the previous section. High level design goals are: scalability, energy efficiency, simplicity and practicality.

The following design choices were made towards achieving these goals:

1. The protocol is source initiated. This eliminates the need for the sink to flood an interest for data through the network and will therefore reduce the number of messages transmitted by individual nodes.

2. Nodes only transmit data when new data is observed. This condition will depend on the application, e.g., sensor nodes could be placed in an environment where sensed data below a certain threshold is not of importance, thereby only transmitting data above the specified threshold.

3. Data is routed along a single path, which is dynamically established. Every time a node needs to send data, it selects one neighbour to send the message to. This selection is based on the neighbour’s hop count and available energy.

4. The routing protocol is computationally simple. The method for selecting the next hop neighbour does not require complex rules or expressions to be evaluated.
3.2 Protocol Operation

The different steps involved in the routing of packets in a SEER network are discussed next. It is important to note that each node is required to keep a neighbour table, which contains an entry for each node within transmission distance.

3.2.1 STEP 1: Network setup and neighbour discovery

Once the network has been deployed in the area where it is to operate, the sink transmits a broadcast packet. The broadcast packet contains the header fields shown in Table 1.

Table 1: Fields contained in the network layer header of broadcast messages

<table>
<thead>
<tr>
<th>Field</th>
<th>Size (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source address</td>
<td>16</td>
</tr>
<tr>
<td>Destination address</td>
<td>16</td>
</tr>
<tr>
<td>Sequence number</td>
<td>8</td>
</tr>
<tr>
<td>Hop count</td>
<td>8</td>
</tr>
<tr>
<td>Energy level</td>
<td>16</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>64</strong></td>
</tr>
</tbody>
</table>

The source and destination addresses are 16 bit addresses enabling 65536 ($2^{16}$) unique addresses. Each node in the network is assumed to have a unique address within the network. The 8 bit sequence number is used to identify new broadcast messages. The sink increments the sequence number every time it sends a new broadcast message. Nodes store the sequence number locally and forward broadcast messages only if the sequence number of the message is different from the stored one. The sequence number uses 8 bits in order to ensure that latency in the network does not cause nodes to mistakenly forward old broadcast messages. An 8 bit hop count ensures that nodes can be up to 255 hops from the sink.

When a node receives this initial broadcast message, it checks whether it has an entry in its neighbour table for the node that transmitted the message. If not, it adds an entry that consists of the neighbour’s address, hop count and energy level. The node then increments the hop count stored in the message and stores this hop count as its own hop count. It then retransmits the broadcast, but changes the source address field to its address and the energy level field to its remaining energy level. Every node in the network retransmits the broadcast message once, to all of its neighbours. If a node receives a broadcast message with a lower hop count than the hop count it currently has, it updates its hop count. When this initial broadcast has flooded through the network, each node knows its hop count and has the address, hop count and energy level of each of its neighbours.

3.2.2 STEP 2: Transmitting new data

When a node observes new data, as defined earlier, it initiates the process of routing. Two types of data packets can be sent: normal data and critical data. If a message is considered critical, for example when the sensed temperature changes from 25°C to 100°C within a very short time, a flag is set in the message indicating that it is critical. A node that originates a critical message transmits it to two neighbours instead of only one. The fields contained in the network layer header of data messages are shown in Table 2.

Table 2: Fields contained in the network layer header of data messages

<table>
<thead>
<tr>
<th>Field</th>
<th>Size (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source address</td>
<td>16</td>
</tr>
<tr>
<td>Destination address</td>
<td>16</td>
</tr>
<tr>
<td>Creator address</td>
<td>16</td>
</tr>
<tr>
<td>Critical flag</td>
<td>1</td>
</tr>
<tr>
<td>Hop count</td>
<td>8</td>
</tr>
<tr>
<td>Energy level</td>
<td>16</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>73</strong></td>
</tr>
</tbody>
</table>

The creator address field is used to inform the sink of which node in the network originated the data message, since the source address is changed at every hop of the routing path. It is assumed that the sink knows where each node is in the network. If the sink does not know which node originated the data and where the node is located, the data is useless.

A node bases its routing decision on two metrics, namely hop count and remaining energy. A node searches its neighbour table for all its neighbours with smaller hop counts than itself. If there is only one such neighbour, that neighbour is selected as the destination for the message. If there is more than one neighbour with a smaller hop count, the node selects the neighbour who has the highest remaining energy entry in the neighbour table.

If a node does not have a neighbour with a smaller hop count, it searches for a neighbour with a hop count that is the same as its own. If there is only one such neighbour, that neighbour is selected. If more than one neighbour has the same hop count, the neighbour with the highest remaining energy is selected. If a node does not have any neighbours with hop counts smaller or equal to its own hop count, the message is discarded.

Before the message is sent, the remaining energy entry for the selected neighbour is decreased in the neighbour table. If the message is a critical message, the process of selecting a neighbour is repeated and the message is sent to a second neighbour. Using hop count as the routing metric ensures that the message is always sent in the direction of the sink.

3.2.3 STEP 3: Forwarding data

When nodes receive a data message they update the remaining energy value in the neighbour table for the neighbour that sent the message. Nodes that forward data messages follow the same process, except for minor differences, that the originating node uses to select the next neighbour in the routing path. The most important difference is that forwarding nodes take the creator address and source address into consideration when selecting the next hop neighbour. When searching the neighbour table for nodes with hop counts smaller or equal to its own, forwarding nodes also make sure that they do not select either the creator of the message, or the node from whom the
message was received as the next destination. This ensures that there are no routing loops in the network.

3.2.4 STEP 4: Energy updates

Nodes may be used by more than one neighbour for routing and therefore the energy value stored in the neighbour tables of both of the node’s neighbours will not be completely accurate. When a node’s remaining energy falls below a certain threshold, it transmits an energy message to all of its neighbours to inform them of its energy level. The fields contained in the header of an energy message are shown in Table 3. Energy messages do not contain any data.

Table 3: Fields contained in the network layer header of energy messages

<table>
<thead>
<tr>
<th>Field</th>
<th>Size (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source address</td>
<td>16</td>
</tr>
<tr>
<td>Destination address</td>
<td>16</td>
</tr>
<tr>
<td>Hop count</td>
<td>8</td>
</tr>
<tr>
<td>Energy level</td>
<td>16</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>56</strong></td>
</tr>
</tbody>
</table>

3.2.5 STEP 5: Network maintenance

The sink node periodically sends a broadcast message through the network so that nodes can add new neighbours that joined the network to neighbour tables and remove neighbours that have failed from the neighbour tables. Nodes also update remaining energy values stored in the neighbour tables. It is important to note that broadcast messages do not contain any data.

The operation of the protocol can be summarised as follows:

1. The sink initialises the network by flooding the network with a broadcast message.
2. Nodes add all their neighbours to their neighbour tables.
3. Nodes send new data along a single path for normal data and along two initial paths for critical data.
4. The neighbour with a hop count that is smaller than the sending node’s hop count is selected as the destination.
5. If multiple neighbours have smaller hop counts, the neighbour with the highest remaining energy is selected as the destination.
6. If a node does not have a neighbour with a smaller hop count, it selects the neighbour with the highest remaining energy from neighbours with an equal hop count to it.
7. If the node does not have a neighbour with an equal hop count to it, the message is discarded.
8. Nodes that forward messages select the next hop similarly to originating nodes, but also ensure that the message is not sent to the creator of the message or to the node from whom the message was received.
9. When a node’s energy falls below a certain threshold, it sends an energy message to notify its neighbours of its remaining energy.

10. The sink node periodically sends a broadcast message to update and maintain the neighbour tables of the nodes in the network.

4 PROTOCOL EVALUATION

4.1 Simulation Setup

Simulations of the developed routing protocol were done using the OMNeT++ Discrete Event Simulation System [34]. The simulator provides a framework for simulating discrete events in networks. Networks and protocols can be modelled using C++ and discrete events can be evaluated using the built-in graphical functionality.

The network was set up with the sink node in the centre of the network. Nodes were distributed uniformly with each node having up to eight neighbours. Non-uniformly distributed networks are left for future work. Figure 2 shows the network layout that was used for simulations.

![Figure 2: An example network of 25 nodes showing layout and connectivity.](image)

The radio model proposed by Heinzelman et al. [35] was used to calculate the energy consumed during transmission and reception of messages. According to this model, the energy consumed during transmission ($E_{Tx}$) is given by:

$$E_{Tx} = E_{Elec} \cdot k + \epsilon_{amp} \cdot k \cdot d^2$$  \hspace{1cm} (1)

and the energy consumed during reception ($E_{Rx}$) is given by:

$$E_{Rx} = E_{Elec} \cdot k$$  \hspace{1cm} (2)

where $E_{Elec}$ is the energy consumed by the transceiver electronics, $k$ is the size of the message in bits, $\epsilon_{amp}$ is the energy consumed by the transmitter amplifier and $d$ is the transmission distance in metres. The energy sources of nodes were initialised to 5mJ. This value was used to reduce the simulation time and the required processing by the desktop computer used for the simulations. As in [35], $E_{Elec}$ was taken to be 50nJ/bit and $\epsilon_{amp}$ 100pJ/bit. The distance between nodes was assumed to be 1m and nodes were uniformly distributed in the network.
SEER was evaluated against three other WSN routing protocols. These protocols were: flooding, directed diffusion and SPIN (Sensor Protocols for Information Negotiation). Flooding was chosen since it gives an indication of the worst case routing scenario. Directed diffusion was chosen due to the fact that it is very popular in the literature and many protocols have been based on it. SPIN was chosen since it is also a well-known source initiated protocol. The packet sizes for the different packets used are given in Table 4.

<table>
<thead>
<tr>
<th>Type of message</th>
<th>Size of message (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>105</td>
</tr>
<tr>
<td>Broadcast</td>
<td>64</td>
</tr>
<tr>
<td>Interest</td>
<td>64</td>
</tr>
<tr>
<td>Energy</td>
<td>56</td>
</tr>
<tr>
<td>Advertise</td>
<td>48</td>
</tr>
<tr>
<td>Request</td>
<td>48</td>
</tr>
</tbody>
</table>

The data message consisted of a 73 bit header and 32 bits of data and was used by all four protocols. The broadcast message was also used by all four protocols. The interest message was only used by directed diffusion, while the energy message was used only by SEER. The advertise and the request messages were used only by SPIN.

The simulation of the protocols started with a broadcast message at the start of the simulation. Every node in the network then sent a new data message every 15 minutes. For directed diffusion, the first data message, at 15 minutes, was sent along a single path since it was assumed in the simulation that the initial broadcast, at time 0, set up gradients. For subsequent data messages, nodes would flood the messages and upon receiving data messages from nodes, the sink would send a broadcast to set up gradients. Therefore nodes would alternate between flooding and sending along a single path every 15 minutes.

For SPIN, nodes would send an advertisement every 15 minutes and every neighbour would reply with a request message. The originator would then send a data message to every neighbour. These advertisement messages contained an 8 bit sequence number in order to ensure that nodes do not request the same data more than once.

4.2 Simulation Results

Simulations were performed to evaluate the network lifetime achieved by each protocol, as well as the number of messages generated by each protocol. The following results were achieved (all of the results, except for Test 6, were plotted using a logarithmic scale due to the large improvement achieved by SEER):

Test 1: The time until the first node fails.

The results from Test 1 (Figure 3) show that SEER achieves an improvement of several orders of magnitude better than the other protocols tested. This is due to the fact that messages are sent along a single routing path which eliminates energy consuming transmissions. The improvement in network lifetime for the network of 2000 nodes is only three times that of the other protocols, due to the fact that every node in the network sends its data through the nodes surrounding the sink. Therefore, 1999 messages are transmitted by eight nodes every fifteen minutes.

Test 2: The time until the sink is unreachable, due to all of its neighbours failing.

The results of Test 2 (Figure 4) add onto the results of Test 1, indicating that SEER can perform for longer period of time before the sink node becomes unreachable. As the network size increases, the number of messages that has to be routed by the eight nodes surrounding the sink increases and reduces their lifetime. The other protocols cause the network to fail after the first data messages are sent by the nodes at 15 minutes. This is due to the flooding used by all of the protocols.

Test 3: The time instant when the number of active nodes in the network reaches a selected percentage.

Test 3 (Figure 5) clearly shows that SEER prolongs the lifetime of the network much more than other flat routing protocols. This large improvement in network lifetime has to do with the fact that the initial energy of all the nodes was set to 5mJ and nodes use 5.1nJ for every message transmitted and 5nJ for every message received. The fact that nodes in the other protocols transmit to every neighbour dramatically increases the energy consumption and consequently reduces lifetime.
Figure 5: The time instant when the number of active nodes in a 2000 node network reaches a selected percentage.

Test 4: The average remaining energy of all the nodes in the network, at selected intervals.

Figure 6: The average remaining energy of all the nodes in a 2000 node network at selected intervals.

The average remaining energy of all of the nodes in the network is conserved for a much longer time in SEER than in the other protocols, as can be seen from the results of Test 4 (Figure 6). This is due to the reduced number of messages that are transmitted.

Test 5: The average number of data messages sent in the network at selected intervals.

Results from Test 5 (Figure 7) show that for the worst case, SEER nodes on average need to transmit only about a quarter of the number of messages that nodes in the best competitor have to transmit. The number of messages that SPIN transmits is much more than the other protocols due to the fact that each node broadcasts an advertisement and then sends data to all of its neighbours that sent a request.

Test 6: The number of data messages received by the sink at selected intervals.

Test 6 (Figure 8) indicates that the sink receives multiple instances of the same data message in the other protocols but only one message per node for SEER. The nodes surrounding the sink deplete their energy just after 30 minutes and therefore no more messages reach the sink after 45 minutes.

Figure 7: The average number of data messages sent in a 2000 node network at selected intervals.

Figure 8: The number of data messages received by the sink in a 2000 node network at selected intervals.

5 CONCLUSION

The results from the six tests confirm that SEER scales well and improves network lifetime by limiting the number of messages that are sent through the network. Overall, the routing protocol is novel and makes an important contribution to the literature by being simple enough to be physically implemented on a variety of existing WSN nodes while still achieving a very high level of energy efficiency.

The results also show that the node failure rate increases the closer nodes are to the sink. This causes a problem for a WSN since the nodes surrounding the sink fail much sooner than nodes far away from the sink. This means that data from the nodes that are still active cannot reach the sink. A possible solution to this problem is to increase the node density as the distance to the sink decreases. This is left for future research.

REFERENCES


