Why Flooding is Unreliable in Multi-hop, Wireless Networks

Rachel Cardell-Oliver

School of Computer Science & Software Engineering
The University of Western Australia
Crawley WA 6009 Australia
email: rachel@csse.uwa.edu.au
tel: +61 8 6488 2231
fax: +61 8 6488 1089

Abstract

This paper examines the unreliability of the flooding protocol - a simple broadcast protocol for delivering a message to all nodes in a multi-hop, wireless network. The protocol is unreliable in that there exist protocol runs in which some network nodes fail to receive the message. A formal specification of the behaviour of a multi-hop network is used to characterize configurations that lead to failure, and to prove unreliability. The specification is also used for simulation, to analyse the percentage of runs that fail to reach all nodes, and the cost and efficiency of flooding. The protocol’s performance is examined for different network topologies, radio transmission properties and protocol retransmission rules. Our results establish a fundamental limit on the reliability of protocols such as flooding, and show how networks can be configured to optimise reliability, cost and efficiency. The formal specification provides a basis for future simulation and verification studies of a wide range of protocols for multi-hop, wireless networks and for modelling energy use, node mobility, and other interactions between nodes and their environment.

Key words: Flooding Protocol, Multi-hop Network, Ad-hoc Network, Formal Verification, Protocol Reliability
1 Introduction

Multi-hop, wireless networks are being used today in a growing range of applications from environmental monitoring with sensor networks [1], to pervasive computing applications in man-made environments [2]. Flooding is a simple broadcast protocol for delivering a message to all nodes in a multi-hop network. The flooding protocol has been widely studied because,

- it is simple to describe and implement,
- it is robust with a high level of redundancy but not 100% reliable,
- its behaviour is strongly affected by transmission interference between nodes,
- and it is used within many more complex application protocols.

This paper extends previous work by proving how certain configurations can lead to failure, and examining the extent of unreliability for different network configurations. Our formal specification and simulation results on the reliability of flooding, in different network configurations, are a step towards building more robust and scalable multi-hop network applications.

Flooding is initiated by a source node broadcasting a message to all nodes within its transmission range. In turn, each node which receives the message then broadcasts it. Having done this, the node goes to sleep, neither sending nor receiving further messages. More generally, the node may wake up again on reception of a new flood message. In this paper we consider only single floods: the flood is complete once every node that has received the message has also broadcast it.

The main advantage of the flooding protocol is its simplicity. It requires no tables to be set up or be managed in order to deliver a message to all network nodes. The main disadvantage of the protocol is its inefficiency, because the flood message is typically broadcast to each node many times. Flood inefficiency, known as the broadcast storm problem, has been widely studied [3,4] and many modifications to the basic flooding protocol have been proposed to improve its efficiency.

However, despite broadcast storm redundancies, the flooding protocol is also unreliable. That is, there exist protocol runs in which some nodes in the network do not receive the flood message. The potential for losing messages was first shown in 1975 by Tobagi and Kleinrock: messages are lost in multi-hop networks because of signal interference as a result of the hidden terminal problem [5]. Tobagi and Kleinrock also studied the problems of nodes competing for a wireless transmission channel and the effectiveness of carrier sense multiple access [6]. Both these analyses were for probabilistic models of traffic load, rather than for specific protocol conditions. In this paper we quantify which sequences of actions and network constraints can lead to a node missing the
flood, and so prove that there exist unreliable runs in which the flood fails to reach all network nodes. We then use simulation experiments to analyse the likelihood of failure under different network topologies, radio footprint types and transmission rules. By characterising these causes and effects, we enable trade-offs to be made to optimise the reliability and efficiency of flooding for a given network configuration.

Our assumptions about how a wireless, multi-hop network behaves are made explicit in a formal specification, presented in full in this paper. A wireless network is defined as a set of network nodes positioned in a landscape. Nodes interact via their landscape by sending and receiving radio broadcast messages. Each node’s specification defines the operations that the node can perform: physical layer broadcast and receive, MAC layer CSMA and the network layer send and receive rules which define the flooding protocol. We quantify three conditions sufficient for flooding failure: a disconnected network topology, transmission noise, and a topology in which some nodes may repeatedly be hidden terminals.

The network specification provides a basis for future simulation and verification studies. An advantage of our approach is that the specification makes visible all assumptions about network behaviour. This is particularly important for comparing protocol performance since minor changes in protocol parameters can result in significant changes in their performance [7].

The theoretical possibility of failure need not be a problem in a wireless network so long as the probability of failure is sufficiently low. After all, wired networks also suffer from potential communication failure because a node can never guarantee that its neighbour has received a message, even with acknowledgements. In this paper, the probability of flooding failure is measured by simulating hundreds of protocol runs for different network configurations, and analysing the measured reliability and efficiency of these runs. These results are of practical benefit for protocol designers, because the scarce power resources available to battery powered nodes are a significant design problem for most wireless networks. Thus, being able to predict the potential trade-offs between increasing reliability and efficiency and reducing cost is critical for achieving scalability, robustness and maximum lifetime of wireless network applications.

The network specification presented in this paper is particularly suited for analysis of wireless sensor networks because there are many new applications in this area [1], and the performance of sensor networks has proved difficult to predict [8,16]. Sensor network characteristics include large scale networks of hundreds of nodes, dynamic and lossy wireless communication, low power radio, and significant interaction between physical, MAC and network layer behaviours [9]. Our specification and its executable version can be extended
to model energy use, node mobility, and the behaviour of the landscape in which network nodes reside. We focus here on the flooding protocol in a static multi-hop network, but using the same specification we plan to specify and study a range of protocols for multi-hop, wireless networks including routing, data collection, and network management in static and mobile networks.

The main contributions of this paper are

- an abstract, formal model for the behaviour of wireless, multi-hop network protocols, and in particular of flooding in these networks,
- a proof that flooding is unreliable in multi-hop, wireless networks, and quantification of the properties which lead to unreliable flooding,
- an analysis by simulation experiments of the probability of unreliable flooding given different network topologies, radio transmission properties, and protocol retransmission rules.

In Section 2 we define a new formal model for wireless, multi-hop networks. The simple flooding protocol is defined within this model. In Section 3 we prove that flooding is unreliable, and make explicit the conditions under which this occurs. The formal model is also used in Section 4 for simulation experiments to quantify the effect of network topologies, transmission footprints and flood retransmission rules on flooding reliability and efficiency. Related work is discussed in Section 5 and conclusions and future work in Section 6.

2 Specification of Multi-hop, Wireless Network Behaviour

This section specifies the behaviour of wireless, multi-hop networks in terms of the actions that can be performed by each node, and the order in which these actions occur in the full network. We view a network as a set of nodes that inhabit a shared landscape in which radio broadcast messages are sent and received. Our model is based on applications such as wireless sensor networks, which have autonomous nodes, each constrained by limited memory, processing and radio transmission power, and by limited node lifetime from battery power. Both mobile and static networks can be described in our model, but in this paper only static networks without lost nodes will be analysed.

The behaviour of a network is defined by the set of its possible behaviours, each a sequence of global states that assign values to variables. A complete behaviour is an infinite sequence of states $\sigma = \langle s_0, s_1, \ldots \rangle$. Each pair of states $(s_i, s_{i+1})$ is a step whose relation is defined by an action predicate. This is a standard and widely used model for concurrent systems similar to the Temporal Logic of Actions [10]. The behaviour of a network is specified by a constraint on the initial states of the system, and a set of actions defining possible steps.
There are both actions for individual nodes (e.g. to send or receive a message) and actions for the global network (e.g. to clear the landscape). Actions of individual nodes are interleaved in the global sequence, abstracting from the precise timing of each node’s actions. The states of this model have variables for the status of individual nodes in the network and the status of the landscape in which the nodes are situated. All state variables have finite domains, and so the transition system defined by the network’s actions is also a finite state machine. This finite state machine specification is executable and so can be readily used for simulation as well as deductive analysis. The model is, however, highly non-deterministic, and so is not suitable for exhaustive model checking for any but the smallest network configurations.

2.1 Topology: Network Nodes and their Landscape

A wireless network node is a micro-computer located in a physical landscape and communicating with other nodes by local radio broadcast. A wireless network is a collection of such nodes co-operating, for example, to monitor and control their environment. A multi-hop wireless network is a wireless network in which more than one broadcast is required to reach all nodes in the network. Each wireless node is characterised by

- its physical position in the landscape,
- the protocol it follows: its programmed behaviour,
- its physical capabilities such as the sensors attached, transmission power, memory and battery power.

The landscape in which these nodes reside is modelled by a 2-dimensional, rectangular grid of cells. Each landscape cell is characterised by

- its x-y co-ordinates in 2-dimensional space,
- physical wireless transmission phenomena such as the presence or absence of radio signal at that location, and
- for some applications by environmental phenomena such as the temperature or soil moisture at that location

In general, wireless nodes sparsely populate their landscape. That is, there are many more landscape cells than there are nodes. The topology of a multi-hop wireless network and its landscape is characterised by the following natural number constants.
This model describes a *static* wireless sensor network, which means that nodes do not change their position in the landscape over time. A static model is suitable for the applications we are developing in which nodes are positioned in an agricultural landscape, and each node is connected to a soil moisture probe in the ground. For future applications we are experimenting with two extensions of this model that capture the dynamics of node position: energy and mobility.

In the *energy* sensor network model, nodes may fail by running out of energy and thus become unavailable for message transmission or reception in the network. In this way, the network topology changes over time.

In the *mobile* sensor network model, nodes may move about their landscape, as for example when the nodes are attached to animals in a natural habitat. Mobile nodes can be modelled by defining the node location function \( \text{NodePos} \) as a state variable (which changes over time) rather than a constant function as used in this paper (where node position does not change over time). The literature on mobile networks contains several models for node movement such as the random waypoint model [11] which can be described within the model introduced in this paper.

### 2.2 Physical Layer: Wireless Transmission and Reception

Packets in a sensor network are transmitted by radio broadcast. When a node broadcasts a packet, bit by bit, each bit propagates like the ripples in a pond to cover a roughly circular region whose radius is proportional to the transmission power of the node. In this way, a packet is transmitted to every location in the sending node’s *footprint*: the set of landscape cells reached by the signal.

The values of a footprint cell or a landscape cell are members of the set \( \text{Signal} \) which contains a finite set \( \text{Data} \) representing the valid messages of the network.
2.2.1 Footprints

In its most general form, a node’s footprint is a function from landscape cells to the signal content of each cell when that node transmits. In this paper we use two types of footprint model:

**analytic:** an idealised transmission model of a circular disk without noise [3,12], and

**empirical:** based on experimental results for wireless sensor networks [13,8,14].

In the analytic model, transmitted messages reach all cells within a disk of Cartesian distance radius $R$ centred on the transmitter’s landscape cell. $R$ is proportional to the transmission power used: the higher the transmission power, the more cells around the transmitter are reached. In this model, there is no noise and the probability of reception is 1 for all cells within the disk, and 0 for all landscape cells outside the disk. The definition is shown in Figure 1.

The analytic model is convenient for analysis, but unfortunately it is not a good representation of the transmission behaviour of real network nodes. Experiments show that the transmission footprint of sensor network nodes is highly probabilistic, and includes significant transmission noise. Furthermore, footprints are irregular in shape (not circular), and probabilities of reception vary over time, even in controlled environments [8,13,15,16,12].

The empirical footprint model specified in Figure 2 is an approximation based on existing experimental results of over 48,000 packet reception experiments using Mica1 motes [13,14]. The model uses a reception probability profile. For a landscape cell at (natural number) distance $d \in 1..\maxD$ from the sending node, $\text{RecvP}[d]$ is the probability that cell correctly receives the transmitted message. There is a different probability profile for each transmission power.
setting used by network nodes, and this can be used to calculate a set of cells of a footprint that contain good data. The probability of reaching a given footprint cell is calculated each time there is a transmission to that cell.

The experiments tell us about good reception, but what happens in cells which do not receive data? Xu, Gerla and Bae [12] propose that wireless transmissions are characterised by three ranges: a transmission range (our reception probabilities), an interference range (distance within which receiving nodes will experience signal interference by an unrelated transmitter) and a carrier sense range (distance within which a transmitter detects another node’s transmission). They argue that interference range and carrier sense range are larger than transmission range: signal at greater distances from the transmitter can interfere with other signals, and be detected by carrier sense even though they are too noisy to be decoded as a good signal. We also adopt this model defining an interference radius, \( \text{maxI} \), selected to cover the area around a transmitter where the probability of reception is at least 5%. Within a disk of radius \( \text{maxI} \), any cell which does not contain a good data signal is assumed to contain corrupted signal \( \text{NOISE} \). At distances greater than \( \text{maxI} \) from the sender a non-receiving cell is \( \text{EMPTY} \). This model allows for the outlier reception cells observed by Ganesan \textit{et al} which lie beyond the interference radius. As well as corruption as a result of colliding transmission signals, the reception of radio signals is noisy because of interference from other objects in the area, radio antennae differences and so on. These sources of noise are reflected in the observed reception probabilities and so modelled implicitly by our reception probability profiles.
2.2.2 Broadcasting

We can now define the effect of a node \( n \) broadcasting a message \( m \) in its landscape. The landscape in which nodes are placed is a state variable that changes over time as different nodes transmit and receive, and radio signals fade away. A transition of the finite state machine model is defined in the standard way as a predicate on primed and un-primed state variables \([10]\). The prime superscript on a state variable denotes the value of that variable in the successor state of the transition and un-primed state variables denote their value in the source state of the transition. Any state variable that does not appear in primed form in the definition of a transition, is assumed to have the same value in the successor state as in the current state.

Variables

\[
\text{landscape} : \text{Xcells} \times \text{Ycells} \rightarrow \text{Signal}
\]

Transitions

\[
\text{broadcast}[n][m] \stackrel{def}{=} \forall x,y. \text{landscape}[x][y]' = \text{landscape}[x][y] \oplus \text{footprint}[n][m][x][y]
\]

The constant \( \oplus : \text{Signal} \times \text{Signal} \rightarrow \text{Signal} \) defines the effect of transmitting signal \( s \) onto a landscape cell. \( \oplus \) is commutative and total.

Constants

\[
\forall s \in \text{Signal}. \ s \oplus \text{EMPTY} = s \quad \text{EMPTY} \oplus s = s
\]

\[
\forall d_1, d_2 \in \text{Data}. \ d_1 \oplus d_2 = \text{NOISE}
\]

\[
\forall s \in \text{Signal}. \ s \oplus \text{NOISE} = \text{NOISE} \quad \text{NOISE} \oplus s = \text{NOISE}
\]

2.3 MAC Layer Protocols

MAC protocols for wireless networks are designed to achieve fair and efficient transmission and reception for autonomous network nodes in the face of signal interference. Figure 3 specifies a standard carrier sense multiple access [6] protocol with a random backoff in the range \( 0 \ldots \text{maxB} \).

2.4 Network Protocols: Flooding

A network protocol is the set of rules followed by each network node for sending and receiving messages. In this paper we define the rules for a simple flooding protocol. Many other protocols can be specified using the same approach,
Fig. 3. MAC layer Send and Receive operations in a Wireless Network including protocols for routing, data collection, and network management protocols.

The control flow of the protocol executed by each network node is remembered by the state variable \texttt{nstate}. The flooding protocol considered in this paper requires no other state information except the MAC layer state variables \texttt{nmessage} and \texttt{nbackoff}. When modelling other protocols, additional historical state information, such as the amount of energy remaining for each node, can be captured in exactly the same way: using a state variable which maps node identifiers to the current value of the variable a given node.

Initially, one node, \texttt{Source} ∈ Nodes is selected as the source of the flood, a default message \texttt{FloodMsg} ∈ Data is placed in its message buffer and its control state is \texttt{TRYSEND} meaning the node is ready to send. All remaining
Fig. 4. Sequence of Actions for each Non-source Network Node

---

TRANSITIONS

\[
\text{init\_node} (n:\text{Node}) = \text{def} \\
\quad \left( (n=\text{Source} \land \text{nstate}[n]=\text{TRYSEND} \land \text{nmessage}[n]=\text{FloodMsg}) \lor \right) \\
\quad \left( n \neq \text{Source} \land \text{nstate}[n]=\text{WAIT} \right) \land \\
\quad \text{MAC\_init}(n)
\]

\[
\text{recv\_wait} (n:\text{Node}) = \text{def} \\
\quad \text{nstate}[n]=\text{WAIT} \land \text{MAC\_recv\_wait}(n)
\]

\[
\text{recv\_done} (n:\text{Node}) = \text{def} \\
\quad \text{nstate}[n]=\text{WAIT} \land \text{MAC\_recv\_done}(n) \land \text{nstate}'[n] = \text{TRYSEND}
\]

\[
\text{transmit\_wait} (n:\text{Node}) = \text{def} \\
\quad \text{nstate}[n]=\text{TRYSEND} \land (\text{MAC\_carrier\_busy}(n) \lor \text{MAC\_backoff}(n))
\]

\[
\text{transmit\_done} (n:\text{Node}) = \text{def} \\
\quad \text{nstate}[n]=\text{TRYSEND} \land \text{MAC\_send}(n) \land \text{nstate}'[n]=\text{DONE}
\]

---

nodes are initially in state \text{WAIT}, waiting to receive the flood. When the network starts up, the source node transmits the default data packet by broadcasting it to all nodes within its radio transmission range. Every non-source node, \( n \), in the network follows the same protocol: first wait to receive a packet (with \text{nstate}[n]=\text{WAIT}) and then broadcast a copy of that packet to all neighbouring nodes (with \text{nstate}[n]=\text{TRYSEND}). Finally the node sleeps (with \text{nstate}[n]=\text{DONE}) neither receiving nor sending any further messages. The sequence in which these protocol operations will be taken by individual nodes is illustrated in Figure 4.

A single run of the protocol is from the initiation of the flood by the source node until there are no nodes left that are able to transmit. Each node’s flooding protocol operations are defined in Figure 5.
2.5 Global Network Behaviour

When we observe a multi-hop, wireless network over an interval of time, three types of activity can be seen: some nodes are broadcasting a message, or attempting to do so and finding the carrier busy; another set of nodes are waiting to receive a message, and a third set are sleeping, possibly performing internal processing. The landscape itself contains transmitted radio signals, which eventually fade, leaving the landscape ready for another round of processing. Specifying the physical timing of these different activities is complex because each network node is autonomous, follows its own clock, and may send or try to receive at any time. Physical factors affect the time for signal decay, propagation time of radio signal and interference between signals in the landscape. Thus the global behaviour of a multi-hop wireless network is potentially chaotic, since the number of possible scenarios grows exponentially with the number of nodes in the network, which is expected to be in the hundreds or thousands. Fortunately, although the fine-grained timing of actions is highly non-deterministic, there are also strong causal orderings in this system. First, a message must be transmitted in order to be received, and both these actions occur within a time interval just longer than the time to transmit a packet; second, carrier sense prevents two nodes within one interference radius of each other from transmitting during the same round. Thus we can abstract from the micro-second details of physical time, and consider global network behaviour in logical rounds. During each round, the landscape clears all signal, then all nodes wishing to send attempt to do so. Finally all nodes wishing to receive attempt to do so, reading the signals which have just been transmitted into the landscape. Logically (although not in fine-grained physical time), the set of nodes waiting to transmit do so in sequence, one after the other, and then all reception events only occur after all transmitting node have attempted to transmit.

Our abstraction of modelling network activity in its logical phases is reasonable for a significant class of multi-hop, wireless networks. For example, in sensor network applications we are developing using Mica Motes [17] and the TinyOS operating system [18] all packets are the same size (typically 38 bytes), and the distance between nodes is typically 1 to 100 metres. Thus the propagation time of less than 0.00333 milliseconds [19] is insignificant in relation to transmission time (30.4 milliseconds per packet).

In order to specify formally the global behaviour of a sensor network we introduce three auxiliary state variables: senders, receivers, alldone. Each variable is a set of nodes. The three sets partition the nodes of the network at each round. A control variable phase ∈ {SEND, RECV, CLEAR} is used to identify the current activity within a round, and rounds are identified by a state variable thisround which is incremented for each new clear-send-receive cycle.
During the transmission phase, nodes that are ready to send may do so in any order. This captures the non-determinism inherent in a network of autonomous nodes. The fine-grained time order in which nodes send is significant, because the node which sends first gets access where there is competition for the carrier. The full finite state machine specification for flooding in a wireless sensor network is given in Figure 7. The sequence in which these operations occur in the global system is shown in Figure 6.

3 The Flooding Protocol is Not Reliable

The flooding protocol is reliable if it ensures that all nodes in the network receive the message broadcast by the source. In this section we prove that flood protocol is not reliable in multi-hop wireless networks. That is, there are runs of the protocol (infinite sequences of states) in which some nodes never receive the flood message. We have identified three properties of a network configuration that can lead to unreliable flooding:

(1) the network node topology includes one or more nodes that are not connected to the source node,
(2) noisy transmission footprints are allowed, or
(3) the network node topology includes nodes whose neighbours can be partitioned into subsets each containing two or more nodes able to transmit simultaneously.

We now define an unreliable flood formally in terms of the MHWflood specification and prove that each of the conditions above can lead to unreliable flooding.

Definition 1 A run of the protocol MHWflood is an infinite sequence of states \( \sigma = (s_0, s_1, \ldots) \) for which (init_network)\( s_0 \) and for each step \((s_i, s_{i+1})\) in \( \sigma \) the action predicate \((\text{new\_phase} \lor \text{transmit\_all} \lor \text{receive\_all})(s_i, s_{i+1})\) is satisfied for unprimed state \(s_i\) and primed state \(s_{i+1}\).

Definition 2 The protocol MHWflood is unreliable if and only if there exists
Transitions

\[ \text{init\_network} = \text{def} \]
\[ \begin{align*} 
\text{phase} &= \text{CLEAR} \land \text{thisround}=0 \land \\
\forall n: \text{Nodes}. \text{init\_node} (n) \land \\
\forall x,y. \text{landscape}[x][y] &= \text{EMPTY} \land \\
\text{senders} &=\{\text{Source}\} \land \text{receivers}=\text{Nodes}−\{\text{Source}\} \land \text{alldone}=\emptyset
\end{align*} \]

\[ \text{new\_phase} = \text{def} \]
\[ \begin{align*} 
\text{phase} &= \text{CLEAR} \land \\
\text{thisround}' &= \text{thisround}+1 \land \\
\forall x,y. \text{landscape}'[x][y] &= \text{EMPTY} \land \\
\text{senders}' &= \{ n: \text{Nodes} \mid \text{nstate}[n] = \text{TRYSEND} \} \land \\
\text{receivers}' &= \{ n: \text{Nodes} \mid \text{nstate}[n] = \text{WAIT} \} \land \\
\text{alldone}' &= \{ n: \text{Nodes} \mid \text{nstate}[n] = \text{DONE} \} \land \\
\text{phase}' &= \text{SEND}
\end{align*} \]

\[ \text{transmit\_success} = \text{def} \]
\[ \begin{align*} 
\text{phase} &= \text{SEND} \land \\
\exists s \in \text{senders} \land \text{transmit\_done} (s) \land \\
\text{senders}' &= \text{senders}−\{s\}
\end{align*} \]

\[ \text{transmit\_delay} = \text{def} \]
\[ \begin{align*} 
\text{phase} &= \text{SEND} \land \\
\exists s \in \text{senders} \land \text{transmit\_wait} (s) \land \\
\text{senders}' &= \text{senders}−\{s\}
\end{align*} \]

\[ \text{transmit\_final} = \text{def} \]
\[ \begin{align*} 
\text{phase} &= \text{SEND} \land \text{senders}=\emptyset \land \text{phase}'=\text{RECV}
\end{align*} \]

\[ \text{transmit\_all} = \text{def} \]
\[ \text{transmit\_success} \lor \text{transmit\_delay} \lor \text{transmit\_final} \]

\[ \text{receive\_all} = \text{def} \]
\[ \begin{align*} 
\text{phase} &= \text{RECV} \land \\
\forall r \in \text{receivers}. \text{recv\_done}(r) \lor \text{recv\_wait}(r) \land \\
\text{phase}' &= \text{CLEAR}
\end{align*} \]

Specification

\[ \text{MHW\_flood} = \text{def} \]
\[ \text{init\_network} \land \text{ALWAYS}(\text{new\_phase} \lor \text{transmit\_all} \lor \text{receive\_all}) \]

Fig. 7. Formal Specification of Flooding in a multi-hop, Wireless Network
at least one (non-source) node \( n \) and run \( \sigma \) of WSNflood in which node \( n \) fails to receive the flood message in all states \( s_i \) of \( \sigma \):

\[
\exists n, \sigma. \forall s_i \in \sigma. (nstate[n] = \text{WAIT})s_i
\]

It follows directly from this definition and the specification MHWflood that a flood run is unreliable exactly when there is never good data available to receive at \( n \)'s landscape position.

**Lemma 3 Unreliable Landscape**

MHWflood is unreliable for run \( \sigma \) and node \( n \) \( \iff \)

\[
\forall s_i \in \sigma. (\text{phase} = \text{RECV} \implies \text{landscape}[n_x][n_y] \notin \text{Data})s_i
\]

**PROOF.**

**Case** \( \implies \)

If MHWflood is unreliable for run \( \sigma \) and node \( n \) then by definition \( (nstate[n] = \text{WAIT})s \) and so also \( (n \in \text{receivers})s \) for any state of that run. Consider any step \( (s_i, s_{i+1}) \in \sigma \) where \( (\text{phase} = \text{RECV})s_i \) Since \( n \in \text{receivers} \) we know either the recv\_done\( (n) \) or recv\_wait\( (n) \) action is taken. But recv\_done\( (n) \) can not be taken since it would change nstate\[n\]. Therefore recv\_wait\( (n) \) must be taken, and since MAC.recv\_wait\( (n) \) we have \( (\text{phase} = \text{RECV})s_i \) and \( (\text{landscape}[n_x][n_y] \notin \text{Data})s_i \) as required.

**Case** \( \impliedby \)

Assume that in run \( \sigma \) the landscape at \( n \) never contains data when \( \text{phase} = \text{RECV} \). Let the induction hypothesis over states be \( P(s) = (nstate[s] = \text{WAIT})s \).

For state \( s_0 \in \sigma \) we have \( \text{phase} \neq \text{RECV} \), landscape\[n_x][n_y] \notin \text{Data} \) and \( nstate[n] = \text{WAIT} \) since \( n \) is not the source node. Thus \( P(s_0) \) is trivially satisfied.

Assume the induction hypothesis, \( P(s_i) \) for \( s_i \in \sigma \), that is \( (nstate[n] = \text{WAIT})s_i \).

If \( (\text{phase} = \text{RECV})s_i \), then \( (\text{recv\_wait}(n))(s_i, s_{i+1}) \) since there is no data in the landscape so recv\_done\( (n) \) is disabled. Thus in \( s_{i+1} \) we also have \( nstate[n] = \text{WAIT} \) which is \( P(s_{i+1}) \) as required.

If \( (\text{phase} \neq \text{RECV})s_i \), then since \( n \in \text{receivers} \), there are no actions which can change \( nstate[n] = \text{WAIT} \) and so \( P(s_{i+1}) \) as required.

\( \Box \)
In order to reason about the state of a network node, we consider the transmissions of its neighbours: those nodes whose transmissions reach the node.

**Definition 4** *Node m is a neighbour of n if at least some of m’s footprints contain a data cell at n’s location nx, ny. That is, NodePos(n) = (x, y) and for some rand ∈ Percent we have footprint[m][msg][x][y] ≠ EMPTY. The set of all nodes which are neighbours of n is denoted neighbourhood(n).*

For analytic footprints, neighbours are any nodes within transmission radius d of one another. For empirical footprints, m is a neighbour of n if m reaches node n in at least some footprints. That is that the distance from m to n is d ≤ maxD and RecvP[d] > 0. In the probabilistic, analytic model of footprints, m’s transmission may reach n but not vice versa at different times. Thus in the analytic model the neighbourhood relation is not commutative in a given protocol run. However, for our purposes, both nodes have the possibility of reaching one another, and so the possible-neighbour relation is commutative.

**Definition 5** *A network contains a broadcast path from node n0 to node nk with k hops iff there exist nodes n1, …nk−1 such that ∀i ∈ 0 … k − 1 we have ni ∈ neighbourhood(ni+1).*

**Definition 6** *A set of nodes n1 to nk is reachable at thisround = r iff there exists a run of MHWflood for which there is a state si such that

\[
\{n_1, \ldots n_k\} \subseteq \text{senders} \land \text{thisround} = r) s_i
\]

A reachable set of nodes for any round r can be constructed by applying the flood protocol rules of MHWflood for r rounds. The resulting set, senders, at the beginning of the send phase of round r is a reachable set of nodes for the given configuration. This set is the maximal reachable set of nodes for that round. But, because of carrier sensing, usually not every node in senders actually transmits in round r. We define the set transmitters(r, σ) as all reachable nodes which also transmit during round r of run σ.

**Definition 7** \(\text{transmitters}(r, \sigma) = \{n : \text{Nodes} \mid \exists s_i, s_{i+1} \in \sigma. (\text{thisround} = r)s_i \land (\text{phase} = \text{SEND})s_i \land \text{MAC\_send}(n)(s_i, s_{i+1})\}\)

**Definition 8** *A multi-hop network is one containing at least one pair of nodes whose shortest broadcast path has at least two hops*

**Definition 9** *A node in a multi-hop network is fully connected with respect to node Source if and only if there is a broadcast path from Source to every network node.*
Connectivity is a property of the node topology and the neighbourhood relation defined by footprint spread. It is independent of any protocol rules governing network behaviour. If a network is not fully connected then flooding will necessarily fail to reach any nodes which are disconnected from the source. Since a disconnected network is a trivial case for flood failure, we omit the proof in this paper. For details see [20]. In the remaining sections we assume multi-hop networks in which all nodes are connected to the source.

3.1 Noisy Transmission

From the Unreliable Landscape lemma, we know that a run is unreliable if a landscape cell for node \( n \) is always empty or contains noise when \( n \) is ready to receive. We now characterise how the value of each cell is built up during the sending phase: as the sum of all footprint cells of the transmitting nodes of that phase. Since \( \oplus \) is commutative, the order in which the transmissions occur does not matter for this lemma.

**Lemma 10 Landscape Cell Values**

For all runs, \( \sigma \), and states \( s \in \sigma \), nodes \( n \) and rounds \( r \), and flood message \( m \),

\[
(\text{phase} = \text{RECV} \land \text{thisround} = r \land \text{transmitters}(r, \sigma) = \{m_1, \ldots, m_k\}) s
\]

\[
\Rightarrow (\text{landscape}[n_x][n_y] = \text{footprint}[m_1][msg][n_x][n_y] \oplus \ldots \oplus \text{footprint}[m_k][msg][n_x][n_y]) s
\]

**PROOF.**

By definition, for each \( m_i \in \text{transmitters}(r, \sigma) \) we have \( \text{MAC} \_ \text{send}(m_i) \) and for \( \text{msg} = \text{nmessage}[m_i] \) that broadcast \( [m_i][msg] \) at some step in round \( r \). Therefore, \( \forall x, y. \text{landscape}'[x][y] = \text{landscape}[x][y] \oplus \text{footprint}[m_i][msg][x][y] \) In particular, at node \( n \)'s location, \( n_x, n_y \) the footprint cell of node \( m_i \) is added to the landscape cell. After all transmitting nodes have sent, phase is set to \( \text{RECV} \) and

\[
\text{landscape}[n_x][n_y] = \text{footprint}[m_1][msg][n_x][n_y] \oplus \ldots \oplus \text{footprint}[m_k][msg][n_x][n_y]
\]

\( \square \)

**Theorem 11 Noise Theorem**

*If the footprints of each node \( m \in \text{neighbourhood}(n) \) are able to transmit noise to \( n \)'s landscape cell \( n_x, n_y \), then flooding is unreliable.*
PROOF.

For each round of the flooding protocol, either there are no neighbours of node \( n \) transmitting, or there are one or more neighbours. In the former case, \( \text{landscape}[n_i][n_j] = \text{EMPTY} \oplus \ldots \oplus \text{EMPTY} \) and so \( \text{nstate}[n]' = \text{WAIT} \) in such rounds. In the latter case, since the neighbours may transmit noise, we can construct a run in which \( \text{landscape}[n_i][n_j] = \text{NOISE} \) since \( \text{NOISE} \oplus s = \text{NOISE} \) for any signal \( s \). Thus node \( n \) does not receive the flood message in the receive phase of any round and so flooding is unreliable in a network with noisy transmission.

\[ \square \]

3.2 Multi-neighbour Transmissions

Given the significant transmission redundancy in the flooding protocol, it is surprising that even if the network is fully connected, and there is no transmission noise, then flooding is still unreliable. The problem in this case is that a node may receive only corrupted signals when its neighbours’ transmissions interfere with one another.

A collision set for some node is any set of nodes able to transmit during the same round whose signals could interfere at that node’s landscape cell.

**Definition 12** A set of nodes \( \{n_1, \ldots, n_k\} \) is a collision set for node \( n \) iff

\[ \exists r, \sigma, \{n_1, \ldots, n_k\} \subseteq \text{transmitters}(r, \sigma) \land \{n_1, \ldots, n_k\} \subseteq \text{neighbourhood}(n) \]

**Definition 13** A node \( n \) is collision centred iff its neighbourhood can be partitioned into sets of nodes \( p_1, \ldots, p_k \) such that

1. each \( p_i \) is a collision set for \( n \)
2. \( \forall i \neq j. \ p_i \cap p_j = \emptyset \) (the sets are mutually exclusive) and
3. \( p_1 \cup \ldots \cup p_k = \text{neighbourhood}(n) \) (the sets form a covering of the node’s neighbourhood)

**Definition 14** A node \( n \) is collision threatened if it is collision centred for a partition \( p_1 \ldots p_k \) of its neighbours and

\[ \exists \sigma, r_{p_1}, \ldots, r_{p_k}. \forall i. \ p_i \in \text{transmitters}(r_{p_i}, \sigma) \]

**Theorem 15** Collision Theorem

If a multi-hop network has at least one node \( n \) which is collision threatened then MHWflood is unreliable.
PROOF.

Let node \( n \) be collision threatened by node sets \( p_1 \ldots p_k \). During the rounds in which no neighbours of \( n \) are transmitting, then \( \text{landscape}[n_x][n_y] = \text{EMPTY} \) and thus \( \text{nstate}[n]=\text{WAIT} \). During the rounds \( r_{pi} \) in which the nodes of collision set \( p_i \) transmit then \( \text{landscape}[n_x][n_y] = \text{NOISE} \) because each member node of \( p_i \) transmits data to cell \( n_x, n_y \) and \( d \oplus \ldots \oplus d = \text{NOISE} \) for any \( d \in \text{Data} \cup \{\text{NOISE}\} \). Thus, \( \text{nstate}[n]=\text{WAIT} \) during these rounds. Therefore, there are no rounds in which \( n \) is able to receive the flood message, and so the flood is unreliable.

\( \square \)

The collision theorem characterise the properties needed for a network to contain collision threatened nodes, but it does not provide a recipe for generating such a set. We have also constructed neighbourhood collision sets for a variety of regular topologies similar to the example in Section 1. In addition, simulations have been used to generate collision sets for topologies with many neighbours or irregular topologies. However, not every network topology has the collision neighbourhood property. In particular, in the next section we present two topologies (ribbon and spine) that do not contain collision threatened nodes, and thus that are reliable for flooding, albeit under the unrealistic assumption of no transmission noise.

4 Optimising Reliability and Efficiency

The flood theorems show that it is possible for some network nodes to miss the flood as a result of a disconnected topology, transmission noise or signal collisions. But how significant is this possibility, and how can the network and protocol be optimised to increase reliability? In order to address these questions we performed a series of simulation experiments.

The \textit{MHWflood} specification is an operational model. Given a specific network topology in a landscape, a footprint model and values for protocol constants such as maximum back-off, each of the actions of the specification can be implemented as methods which update state variables in a programming language such as Java. Our simulation program is a simple transliteration of the \textit{MHWflood} specification given in Section 2. Each non-deterministic choice in the specification (that is, the order in which nodes transmit, random back-offs and footprint noise) is implemented using a random seed to choose a program alternative. The choice between noise or data in a footprint cell is weighted by the reception probability \( \text{RecvP}(d) \), but all other choices are equally divided.
<table>
<thead>
<tr>
<th>Landscape</th>
<th>maxX by maxY</th>
<th>67 x 34 to 194 x 256 cells</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>maxNodes</td>
<td>1024</td>
</tr>
<tr>
<td></td>
<td>maxXnodes</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td>maxYnodes</td>
<td>32</td>
</tr>
<tr>
<td>Topologies</td>
<td>nodePos</td>
<td>7 types: see Figure 9</td>
</tr>
<tr>
<td></td>
<td>Source</td>
<td>Top left corner</td>
</tr>
<tr>
<td>Footprint types</td>
<td>All 112 data cells (avg)</td>
<td>Dense, Low noise, Average,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High noise: see Figure 10</td>
</tr>
<tr>
<td>Flood Rules</td>
<td>Retransmission Prob.</td>
<td>1.0, 0.75, 0.5, 0.25</td>
</tr>
<tr>
<td>Simulation</td>
<td>Simulation Runs</td>
<td>500 per Configuration</td>
</tr>
</tbody>
</table>

Fig. 8. Parameters used for Reliability Experiments

between the alternatives.

Different network topologies, footprint types and protocol re-transmission probabilities were considered for a network of 1024 nodes. All simulated network configurations are summarised in Figure 8 and full results are given in [20].

The following metrics were used to evaluate the performance of flooding in different simulation settings:

- **reliability** the number of nodes which received the flood, as a percentage of the total number of nodes in the network, maxNodes.
- **cost** the number of simulation cycles needed to complete the flood.
- **cover** the number of simulation cycles needed to reach all receiving nodes.
- **efficiency** the percentage ratio of cover to cost.
- **success** a triple (s90, s50, s00) giving the percentage of runs with at least 90% reliability, between 50 and 90% and between 0 and 50% reliability. The success triple summaries the shape of the underlying data distribution that is averaged for the reliability metric.

### 4.1 Network Topologies

Our proof of the unreliability theorem highlights the importance of nodes’ positions in the landscape, not just their density in their landscape. Previous studies have shown that increasing node density decreases the efficiency of flooding [3,11,21], and that the optimum number of neighbours for efficiency
is six [21]. To the best of our knowledge, this paper reports the first study of the effects of the shape of the network topology on the performance of flooding, that is, we consider the relative positions of network nodes in a landscape.

Figure 9 shows the seven different network topologies tested in this paper. The topologies vary both node density and also node position in the landscape. Five regular topologies are considered: four based on hexagonal arrangement of the nodes, and the fifth on a square grid. We also consider two topologies which prevent collisions during flooding: ribbon and spine. The ribbon topology allows only one path from source to all nodes. The spine topology has a backbone path with independent ribbons leading from it. The flood source node is at the top left hand corner of each network topology.

4.2 Transmission Footprints

Recent empirical studies have highlighted the irregularity of the radio transmission footprints of wireless nodes [13,8,15,9]. Footprints have been shown to be both asymmetric and noisy and the size and shape of footprints varies widely between individual nodes, even when all use the same transmission power. We experimented with the four different footprints shown in Figure 10: three taken from experiments with Mica motes [13,14] and, for comparison purposes, an idealised, circular footprint with no noise. All four footprints contain the same number of landscape cells with good data (112 on average). The high and low noise footprints are those of individual motes and the average footprint is calculated from 100 motes transmitting at medium power [13,14]. As can be seen in Figure 10, the high noise footprint reaches the largest area of landscape, but many cells within this range contain noise. The
idealised footprint covers the smallest landscape area, but every cell within the footprint receives good data.

4.3 Probabilistic Flooding

There are several published strategies for reducing the effects of the broadcast storm by varying the flooding protocol’s transmission rules [3,4,22]. In our experiments we considered one of these strategies: varying the probability that a node which receives a packet chooses to retransmit it. A simple change to the flood send rule specifies this variation:

\[
\text{PROB} = \{1.0, 0.75, 0.5, 0.25\}
\]

\[
\text{transmit\_done (n:Node) (p:PROB)} =_{\text{def}}
\]

\[
\text{nstate}[n] = \text{TRYSEND} \land (0 \leq \text{random} \leq 1) \land
\]

\[
((\text{random} \leq p \land \text{MAC\_send}(n)) \lor (\text{random} > p)) \land
\]

\[
\text{nstate}'[n] = \text{DONE}
\]

4.4 Results

Figure 11 summarises the effect of network topology on flooding performance. The three most dense topologies are highly reliable, for both average noise and ideal (no noise) footprints. The spine and ribbon topologies, which have no redundant connections between nodes, are extremely unreliable for noisy footprints, but have 100% reliability for ideal footprints. For dense footprints the low reliability of the square grid is entirely due to collisions. The high
reliability of the spine and ribbon for dense footprints is due to the lack of noise and lack of collisions. For idealised footprints, the cost of flooding is very high for the topologies with no redundant connections: 99 cycles for the spine and 1023 cycles for the ribbon. It is possible to substantially improve the reliability of flooding in the square grid with ideal footprints by using a larger backoff or introducing a random wait before MAC transmissions, but this significantly increases the cost of flooding. The medium topology is optimal for reliability (98.6%), cost (43.8 cycles) and efficiency (91.6%) for the average noisy footprints observed in sensor network experiments.

Figure 12 shows the effect of different footprint types on flooding performance for four network topologies. Reliability is over 99% for all footprints in the very dense and dense topologies. Reliability increases as footprint noise decreases for the sparse and medium topology. For the grid topology, all footprints lead to low reliability flooding, but the best performance is with the average noise footprint. The very dense topology is interesting because the cost of flooding is significantly reduced as footprint noise is reduced. For sparse and medium topologies there is a small increase in flooding cost as footprint noise is reduced. There is, thus, a trade-off to be made between maximum reliability.
Fig. 12. The Effect of Different Footprint Types on Reliability (solid lines), Efficiency (dotted lines) and Cost (bars) for Very Dense (top left), Dense (top right), Sparse (bottom left), and Grid (bottom right) Topologies

and minimum cost. A noisy footprint reaches a larger area of the landscape than a dense footprint, allowing the flood to reach distant nodes more quickly. The distant nodes are then able to retransmit without interference, and so the flood reaches all nodes more quickly. The optimal footprint type for reliability, cost and efficiency is the average footprint, and the next best is the high noise footprint.

That noisy footprints benefit performance is ideal for the design of applications such as wireless sensor networks with limited resources, because each node’s energy resources are low, and so using low power (but noisy) transmissions prolongs the life of the network [1]. That noisy footprints do not compromise reliability appreciably is also useful for sensor network applications because overcoming collisions using protocols such as RTS/CTS [12] requires many extra packets to be transmitted, using extra node power and thus reducing the lifetime of the network.

Figure 13 shows the effect of probabilistic retransmission on cost (bars) and reliability (lines). Probabilistic retransmission can improve performance if the number of redundant transmissions is already very high; that is, in the very dense and dense topologies. Otherwise, for example for the medium topology, the flood becomes unreliable under this strategy. A retransmission probability of 0.25 is optimal for the very dense topology (dark line and bar), 0.5 for the
5 Related Work

Several simulation studies have analysed the efficiency of flooding, although not usually its reliability, and presented modifications to flooding to improve its performance. Ni, Tsang, Chen and Sheu introduced the term broadcast storm problem for flooding protocols in mobile ad hoc networks [3]. Geometric analysis is used to investigate the contribution of broadcast redundancy, and MAC layer contention and collisions to the performance of flooding. For example, when equal, circular broadcast footprints (that is, our analytical footprint model) are assumed for all nodes, then when a node receives a message and re-broadcasts it, no more than 61% additional coverage of nodes can be achieved. Also, if there are any more than 6 nodes within the broadcast footprint of a node, then the probability that all these nodes experience contention is at least 0.8. The paper also proposes several mechanisms for reducing the broadcast storm problem: each based on changes to the retransmission rule of the basic
flooding protocol. Simulation experiments are used to analyse their performance of these new mechanisms. Reliability (number of reachable hosts which receive the flood), saved retransmissions and latency (cost) are measured. Different node densities are considered ranging from over 300 to 4 neighbours per footprint. Nodes are randomly placed in the landscape, and are mobile during flood runs. Idealised dense transmission footprints, only, are tested. In this paper we analyse not only different node densities, but also different placements of nodes in a topology, and not only idealised dense footprints, but also a three different noisy transmission footprints observed in network experiments.

Simon et al use simulations together with a search algorithm to find the parameters which optimise a given performance function [22]. Their simulator is implemented in MATLAB; it incorporates an analytical model of noisy footprints, and models collisions and contention for a static network of nodes. Downey and Cardell-Oliver present an extensible Java simulator framework for multi-hop wireless networks, based on the formal model presented in this paper. The simulator is used to investigate the effect of the limited network resources on the time and resource efficiency and scalability of the flooding algorithm. While [23] shows benefits of our model for flexible simulation, this paper presents the model in full and emphasises its benefits for formal verification.

There are several other analytical models which have been used to study flooding. Differential equations have been used to create epidemiological models for the spread of disease and can also be used to analyse flooding algorithms [11]. As in the broadcast storm study, an idealised, dense transmission footprint is assumed and different densities of network nodes are considered. In addition, nodes are mobile, and follow a random movement model. The epidemic model describes the infection of all nodes, which is comparable to reception latency in this paper. However, it does not allow the protocol followed by the nodes to be changed, different transmission footprints to be used, nor does it allow the measurement of settling time. Percolation theory and random graph theory have also been used to analyse flooding, and in particular to investigate phase transitions in probabilistic flooding algorithms: the probability for which the protocol’s behaviour changes between reliable and unreliable flooding [4]. Different node densities, and both static and mobile nodes are considered. As with the epidemic model, this approach suffers from modelling inflexibility because of the assumptions of the underlying theories. For example, although collisions are modelled, MAC layer back-off is not.

The performance of protocols for managing the shared landscape in wireless, multi-hop networks has been extensively studied since the 1970s when the hidden terminal problem [5] and CSMA performance [6] were analysed by Tobagi and Kleinrock. The growth of wireless network applications in recent years
has led to researchers revisiting proposed solutions to problems such as the request to send, clear to send handshake protocol. Xu, Gerla and Bae [12] analyse weaknesses of this handshaking protocol under the realistic assumption that interference and carrier sense distances are larger than transmission distances for nodes. They propose a conservative reply scheme which makes the trade-off of reducing the effective transmission range of nodes to eliminate (or reduce) packet collisions caused by large interference ranges. We do not test the RTS/CTS protocol in this paper, since the extra packets required would be prohibitively expensive for low powered motes in the sensor network applications we are currently developing. Previous authors have analysed performance from either geometric arguments about a round of transmissions from neighbouring nodes, or using probability distributions of traffic [6,5,12]. Our model allows analysis of sequences of protocol actions, both for proving properties of specific protocols, and for simulation under packet arrival rates generated by specific network configurations.

Given the known problems with the accuracy of simulators for wireless networks [7], perhaps the best way to study the performance of flooding protocols is by measuring that performance in real networks. This approach is taken by Ganesan et al [8,13] for studying flooding in wireless sensor networks and by Woo, Tong and Culler [9] for studying data gathering protocols. In [9], both physical experiments and simulations are used to study data gathering protocols. As in this paper, collision, contention, and footprint noise are modelled. The Ganesan et al study used a sensor network consisting of 156 Mica motes [17] placed in a regular square grid pattern in a landscape of 13 by 13 landscape cells, each of 2 foot square. In order to measure transmission footprints, each node in the network, in turn, transmitted 20 packets at different transmit power settings. The number of these packets received by each surrounding node was recorded [13] and this data is used in this paper to define empirical transmission footprints [14]. In a second experiment, a flood was initiated from a node in the middle of the base of the 156 node grid, and each node recorded its transmission and reception of messages during the flood. Although the network node density was the same in all experiments, node transmission power was varied. This resulted in different size footprints, ranging from projected average number of nodes reached from 30 to 194 nodes. Varying transmission power thus gives a similar effect to varying node density. Reliability appears to have been 100% in all experiments for the very dense network topology used in the experiment. Efficiency and cost were recorded for retransmission probability of 1.0 and different footprint sizes resulting from varying transmission power. As in our experiments, for very high power (that is, high node density) the cost of flooding was observed to be significantly higher and the efficiency lower than for very low transmission power (that is, low node density). Although gathering real performance data is critical for validating models, this approach has the disadvantage that only a small part of the design space can be explored. The network topology for the Ganesan
experiment is very dense, and the landscape area is small compared with the area of transmission footprints: in many experiments much of the transmission footprint was outside the landscape of nodes. A total of 30 flood runs were recorded. In simulation experiments, however, we are able to consider a much larger network, and many more transmission runs.

6 Conclusions

This paper presents a new formal model of wireless, multi-hop network behaviour, and proves that the flooding protocol is unreliable under the following conditions:

- some network nodes are disconnected from the source node, or
- transmission noise is allowed, or
- nodes are open to collisions from sets of their neighbouring nodes.

The model is also used to perform simulation experiments to analyse the percentage of runs which fail to reach all nodes, and the efficiency of the flood for different network topologies, radio transmission properties and flood retransmission rules. Our results confirm a fundamental limit on the reliability of wireless, multi-hop network protocols such as flooding, and show how network configurations can be selected to optimise reliability and efficiency:

- The density of network nodes (relative to the reach of transmission footprints) affects the reliability and cost of flooding. High density gives the best reliability, but highest cost. Low node density can result in the flood dying out before reaching most of the network nodes.
- The noisiness of a node’s transmission footprint has a minor effect on the reliability of flooding, but may have a major effect on flooding cost, depending on the network topology.
- Varying the retransmission probability of the flood protocol can lead to significant improvements in flooding cost, wherever there is already significant redundancy in protocol transmissions. The largest cost reductions were observed for the very dense network topology with average footprints.

Our study has highlighted several areas for further work. There is clearly a need for more empirical data from multi-hop wireless network applications in order to validate and improve the accuracy of models, such as ours, that are used for verification and simulation analysis. Explicit specification of network models is important because the performance predictions from several widely used network simulators are known to differ significantly [7]. We also plan to extend our model of wireless, multi-hop networks to include properties such as node energy, and to investigate higher level protocols (than flooding) such

Acknowledgements

The author is grateful for feedback on this work from Amitava Datta, David Glance, Chris McDonald, Patrick Downey and Samantha Chen and advice on the transmission footprints of Mica motes from Deepak Ganesan, Alec Woo and Alberto Cerpa.

References


Author Biography

Rachel Cardell-Oliver is a senior lecturer in the School of Computer Science & Software Engineering at The University of Western Australia. Her research interests include the design, analysis and test of distributed, real-time systems such as wireless sensor networks, embedded systems, and communication protocols. She is currently developing wireless sensor networks for environmental monitoring applications in soil water management, dryland salinity and viticulture. She has a PhD in protocol verification from the Computer Laboratory of the University of Cambridge, UK and a Masters (research) in distributed systems from The University of Western Australia.