# Mobile Wide Area Wireless Fault-Tolerance

J. S. Pascoe†, G. Sibley‡, V. S. Sunderam‡ and R. J. Loader†

†Department of Computer Science
The University of Reading
United Kingdom
RG6 6AY
J.S.Pascoe@reading.ac.uk
Roger.Loader@reading.ac.uk

‡Math & Computer Science
Emory University
Atlanta, Georgia
30302
gsibley@emory.edu
vss@mathcs.emory.edu

**Abstract.** This paper presents work-in-progress that is developing a novel fault-tolerant mechanism for use in mobile wide area wireless networks. As a developmental platform, we are using the Ricochet service which offers ubiquitous metropolitan scale wireless network coverage in several major US cities. We postulate that the majority of network failures in infrastructures such as Ricochet are caused by environmental factors. From this, we propose a GPS based mechanism that intelligently gathers semantic data pertaining to specific geographic areas (or *trouble spots*) which cause communication problems. To facilitate the categorisation of trouble spots, we propose a list of suitable metrics to analyse the status of a wireless connection. Finally, we experimentally evaluate their effectiveness.

## 1 Introduction

Recent work in the field of mobile wireless communication protocols has centered around *ad hoc* networking, in particular, disciplines such as routing have become very mature. Protocols such as ODMRP (On Demand Multicast Routing Protocol) [12, 11, 13, 6], AMRoute [1], CAMP [4], RBM [2] and LAM [10] all support this observation. Until recently, metropolitan scale wide area wireless research was not feasible as there were no suitable infrastructures to support such work. With the advent of developments such as Ricochet [9] and Bluetooth [7], this view is changing.

Recent work by the authors [19, 16, 15, 18, 17] has addressed the issue of fault-tolerance in multicast collaborative computing environments, in particular, the *Collaborative Computing Frameworks* [21] which has been developed at Emory University. Following the successful completion of this work, it was decided to extend the fault-tolerance protocols into the domain of wide area wireless communication. The exemplar for this work is the Ricochet wireless network which is rapidly becoming a popular city scale system for this type of research.

Ricochet is a wireless metropolitan area network that has been installed in several major US cities. It is a subscriber based system that offers a fixed bandwidth limit of 128Kbps through small portable radio modems. Note that unlike most other wireless networks, Ricochet is not ad hoc, that is, although nodes may move arbitrarily throughout the network, the communication infrastructure and thus the networks topology does not change. This requires that the importance of issues such as routing and intermittent communication be readjusted. Thus, in order to provide fault-tolerance within such a network, a new series of challenges must be addressed. The most notable of these, is

V.N. Alexandrov et al. (Eds.): ICCS 2001, LNCS 2073, pp. 385–394, 2001.

the networks resilience in relation to environmental factors (e.g. a user may experience a temporary drop in communication whilst driving through a tunnel).

In this paper, we present a GPS based scheme that addresses these issues and also proposes a set of metrics to evaluate the state of a wireless connection. This in turn allows us to identify and categorise problem areas (or *trouble spots*), the underlying premise being to pre-emptively eliminate problems when other hosts subsequently visit the area.

This paper is structured as follows: in sections 2 and 3 we respectively describe our recent work in the Collaborative Computing Frameworks and outline the structure of the Ricochet network. Section 4 then presents our novel approach to fault-tolerance that extends the work discussed in section 2. To facilitate data collection within trouble spots, section 5 proposes a series of link-state evaluation metrics. In order to prove their effectiveness, we experimentally evaluate these metrics before finally giving our conclusions.

## 2 The Collaborative Computing Frameworks

The *Collaborative Computing Frameworks (or CCF)* is an environment that provides an Internet scale *collaboratory*. Highlights of the CCF include multiple levels of Quality of Service semantics, a novel variant on the virtual synchrony [21] algorithm, IP based WAN tunneling, an X multiplexor and a suite of purpose designed tools.

The underlying abstraction of the CCF is split into two distinct components; *sessions* are heavyweight groups, that is, each user wishing to participate in the collaboratory must register with a session. Once part of a session[1], each user is free to join an arbitrary number of *channels* or lightweight groups. Channels provide a mechanism for logically separating messages at different levels of Quality of Service. As an example, consider a collaborative audio tool that requires two channels to operate (the first for control messages, and the second as a data stream). The first channel may operate using a reliable mechanism whereas the second may be configured for unreliable data transfer (thus maximising data throughput). This abstraction allows an application to simultaneously operate across multiple levels of Quality of Service and in doing so, provides a more flexible transport mechanism than other collaborative environments.

Our recent work [19, 16, 15, 18, 17] addressed the issue of adding fault-tolerance into the CCF. Our approach differed from other datagram oriented schemes in that it is based on a reliable multicast primitive. This provides a significant enhancement over other work, since the number of message exchanges required to form consensus is drastically reduced.

The approach is based on two distributed elections. The first ratifies membership issues (such as failed hosts) and the second deals with the more subtle channel oriented faults. On detection of a failure, an election is called by the *error master* (i.e. the session owner). Each session member then probes the network to obtain an up-to-date snapshot of the sessions state. These results are then sent to the error master which collates, counts and multicasts the outcome of the election to the remaining session members[2].

The implementation of the mechanism is multi-threaded with one thread acting as an *error monitor* and the other as an *error handler*. The error monitor is responsible

[1] Note that the first user to join a session is called the *session owner*.

[2] For brevity, we do not discuss other scenarios such as the failure of the error master here. Instead, the interested reader is referred to [19, 16, 15].

for logging failures and mediating the invocation of the error handler which then coordinates the protocol's election phase. By basing the implementation on two complementing entities, the mechanism as a whole becomes more extensible, efficient and effective.

## 3 The Ricochet Network

The Ricochet network is present in 8 major US cities with further expansion into another 13 being planned in the near future. The network offers a fixed bandwidth of 128Kbps and is accessible to the general public through small portable wireless modems. The network itself consists of 7 architectural components which are grouped hierarchically to provide the service.

- *Wireless Modems* – Ricochet modems are small devices that can be connected to any portable workstation.
- *Microcell Radios* – Microcell radios communicate with user workstations through wireless modems. In addition, they perform error checking and are responsible for sending acknowledgements.
- *Wired Access Points* – Wired Access Points or WAPs are installed within a 10-20 square mile area. Each WAP collects and converts wireless data into a form suitable for transmission on a wired IP network.
- *Network Interface Facility* – A Network Interface Facility connects a group of WAPs to the Network Operations Centers.
- *Ricochet Gateway* – The Ricochet gateway is part of each Network Operations Center and connects the Ricochet network to other systems.
- *Network Operations Centers* – The Network Operations Centers are the hub of the entire system. They provide a means for monitoring and control within the network.
- *Name Server* – The name server maintains access control and routing information for every radio and service within the wireless network.

The overall topological structure of the networks wireless component is a mesh, since microcell radios are placed at regular intervals in a 'checkerboard' fashion. In [12] the authors argue that the additional redundancy in a mesh provides a more robust wireless network topology than that of a tree or a star.

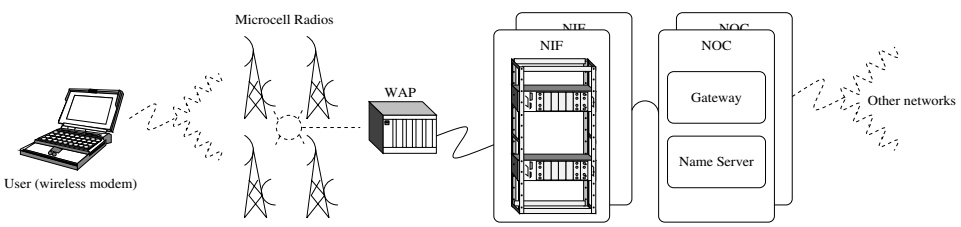


**Fig. 1.** The Ricochet Communication Architecture

## 4 Wireless Wide Area Fault-Tolerance

The migration to a wireless transmission medium in the CCF requires the consideration of several new fundamental issues:

- *Message Garbling* – Messages are more likely to be garbled, particularly in noisy environments (e.g. the central area of a city). In terms of the CCF, this has implications in guaranteeing reliable Quality of Service semantics.
- *Intermittent Connectivity* – Hosts are likely to experience unpredictable intermittent connectivity problems that can last for arbitrary amounts of time. In this situation, a loss of contact should not result in the host being removed from the session (if at all possible).

As noted above, we consider the majority of problems in a Ricochet network to be caused by environmental factors. Preliminary experimentation with the system has revealed that specific types of problem occur in relation to geographic locations (trouble spots). From this, we propose the following classification of trouble spots in a metropolitan area wireless network (see table 1). For brevity, a comprehensive classification is not given here. A discussion on additional metrics such as signal strength is given in [22].

Note that this classification also extends to failures at a network level. For example, the failure of a microcell radio would either be classified as a fatal disconnection or a long disconnection (depending on whether the user was stationary or moving).

Trouble spots can be of an arbitrary size, but often occur in predictable patterns. Trouble spots of the first classification would include areas in which there are many high buildings present (e.g. the center of a city). Short disconnection trouble spots are typically small and span an area of less than 10 square meters. Long disconnection trouble spots are inherently larger and are exemplified by road bridges and tunnels. Fatal disconnection areas are small, specific and occur in regular formations (e.g. lines). This type of trouble spot is usually encountered when a wireless modem moves beyond the networks range, for example, as the user travels out of the city. Using Ricochet, the user experiences a sharp drop in communication i.e. fading does not occur.

In order to facilitate mobility, the error monitor / error handler protocols require extension to incorporate an intelligent geographic view of the network. Composition of this view can be achieved by collecting data about trouble spots as they occur and then using this information to prevent (or intelligently deal with) other hosts encountering the same problem. The worst case scenario is when the trouble spot is not known to the system. In this instance, the following chain of events is observed:

| No. | Description | Characteristics |
|---|---|---|
| 1 | Message garbling | messages are garbled or echoed |
| 2 | Short disconnection | suspended connection (short period) |
| 3 | Long disconnection | suspended connection (longer period) |
| 4 | Fatal disconnection | connection dropped |

**Table 1.** Classification of Trouble Spots in Metropolitan Area Networks

1. A user encounters an arbitrary communication problem as they are moving across a city. This problem can be of any nature (e.g. a link failure or transmission errors). The nature of the trouble spot is identified and the geographic position is noted.
2. A server (running as part of the CCF) is contacted and informed of the new trouble spot. The trouble spot is categorised and some appropriate resolution strategy is adopted.
3. The host performs any action necessary to rectify the situation.

In the second scenario, the user encounters a known trouble spot and so the situation is dealt with differently. The server realises that a host is about to encounter a network problem, and so depending on the category and the semantics of the trouble spot, it can respond in a number of ways:

- *change the channel QoS dynamically* – the host maybe traveling into an area that is known to garble messages. In this case, the server may request that the QoS for any unreliable channels be upgraded to a reliable mechanism until the host moves out of the affected area.
- *do nothing* – the trouble spot may cause a small problem (e.g. a short disconnection) that can easily be accommodated by the buffering in the existing protocols.
- *begin logging messages* – a longer drop in communication is too substantial for the existing protocols to deal with. However, it is not usually necessary to forcefully remove the session member and so the server may begin to record messages to later facilitate an off-line replay.
- *warn the user* – the host maybe traveling beyond the range of the network and so a fatal disconnection may be about to occur. In this case the server may warn the user of the impending problem and ask for an indication of intent. If the user opts to leave the network, then the error master will forcefully remove the participant to preserve the sessions health.

Regardless of whether the host has prior information about a trouble spot, it must re-examine the area to ascertain whether its semantics have changed. If this is the case, the server is updated with the new information. Note that an individual server will store trouble spot data for a particular area. Mechanisms for distributing such servers are being investigated and will be reported on in a future presentation.

The scheme outlined above requires that a node periodically sends its location to the server. For this, we use the Global Positioning System (GPS). The idea of using GPS as a protocol enhancement is not new; ODMRP [11] makes extensive use of GPS in its 'mobility prediction' system. Also, the use of GPS for gathering positional data in wireless networks is mentioned in [12]. However, as we intend to use GPS in a fault-tolerant context, there is (at least to the authors knowledge) no conflict in novelty.

GPS offers a significant number of advantages over a network dependent (triangulated) mechanism. Most notably, GPS offers complete worldwide compatibility and will deliver positional information to an accuracy of within 10 meters. In terms of a metropolitan area network, this granularity is considered to be sufficient for most applications. The fault-tolerance mechanisms presented here will operate in any wireless environment and exhibit no dependencies on both the network and the CCF.

## 5 Wireless Link-State Evaluation Metrics

One outstanding issue is the pertinent question of how to ascertain the semantics relating to a specific trouble spot. When encountered, a trouble spot is initially detected

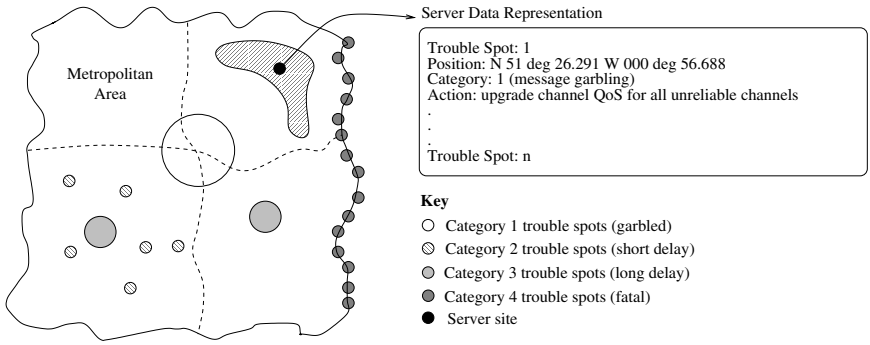


**Fig. 2.** Geographic Example of Trouble Spot Data

by the occurrence of fault reports through the use of reliable multicast. At this stage, the system must determine (by executing a series of diagnostic tests) which category of trouble spot it has encountered so that it may invoke an appropriate failure handler. In order to achieve this, we propose the following metrics for evaluating the state of a wireless connection in a non ad hoc network.

- *Packet loss* – packet loss at the wireless network interface is a function of not only the power of the received signal, but also the path loss and the state of the network. Packet loss is inversely proportional to signal strength and as such, a high packet loss indicates a drop (or imminent drop) in connection. Thus, packet loss is an important metric in determining trouble spots of the second, third and fourth categories.
- *Path loss* – Wireless network interfaces are designed to operate with a specific signal-to-noise ratio, that is, signal strength to the power of the receiver noise should not fall below a specified value. Note that in free space, signal strength decays inversely with the square of the distance from the source. In a metropolitan environment, this decay is much greater, firstly because of objects and people and secondly, because of destructive interference caused by reflections from these objects. These combine to form path loss which offers a quantitative metric of the signal disruption due to environmental factors. In conjunction with the other metrics, a high path loss indicates a trouble spot of the first category.
- *Response time* – The response time of the network is the duration between a message being transmitted and the reply being received. It can often be useful in classifying trouble spots when the packet loss and path loss are both low. In this circumstance, a high response time will indicate a network problem related to the wired component of the infrastructure.

The above metrics were suggested by a number of sources, the most notable being [8], [23] and the IETF MANET[3] metrics for the evaluation of ad hoc routing protocol performance [3].

[3] Mobile Ad-hoc NETworks working group.

## 6 Metric Evaluation

For brevity, we only evaluate the performance of the above metrics in relation to trouble spots of the first category, namely, message garbling. More results pertaining to the other categories are available in [22]. The evaluation environment consists of a single laptop connected to the Internet through a Ricochet modem. The laptop is moved along a 10 meter path at a speed of approximately 1 m/s. Message garbling is achieved by obscuring part of the laptops path with several large metal objects. Note that the objective of the experiment is to evaluate the effect of environmental disruptions in terms of the proposed metrics. Thus, an experimental distance of 10 meters is sufficient to achieve the required focus.

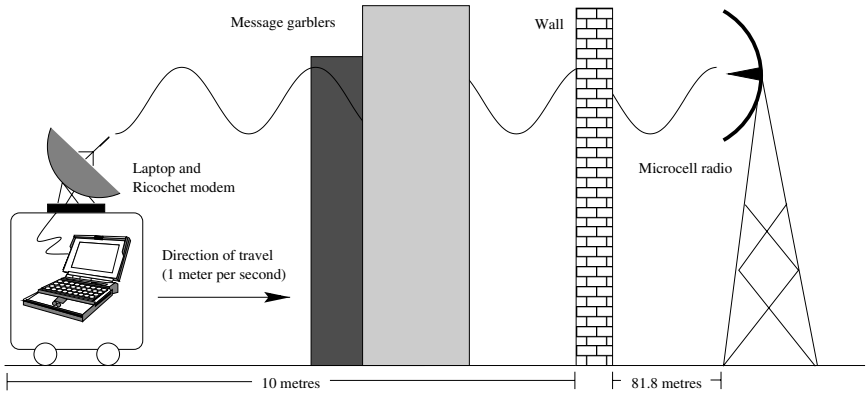


**Fig. 3.** The Experimental Evaluation Environment

### 6.1 Packet Loss

Determining a measure of packet loss can be effectively achieved in a number of ways. One such method is to use a reliable transport protocol and to monitor the number of failure reports returned from a fixed number of transmissions. As the CCF implements a reliable multicast primitive, it is this method that we adopt here. Note that as an enhancement, it is often possible to gather packet loss and response time statistics simultaneously.

### 6.2 Path Loss

The model we use for calculating path loss is the log-distance model as outlined in [20]. There are several models for determining path loss, but a discussion on these is beyond the scope of this paper. Instead, the interested reader is referred to [5, 20]. Using the log-distance path loss model, the average path loss for an arbitrary transmitter receiver (T-R) separation is expressed as a function of distance using the path loss exponent $n$.

$$\overline{PL}(d) \quad \left(\frac{d}{d_0}\right)^n \; or \; \overline{PL}(dB) = \overline{PL}(d_0) + 10n \, log\left(\frac{d}{d_0}\right) \tag{1}$$

The value $n$ indicates the rate at which path loss increases with distance, $d_0$ is the close-in reference distance[4] and $d$ is the T-R separation (which in this case varies between 81.8 m and 91.8 m). Table 2 gives the typical path loss exponents for a variety of mobile radio environments.

| Environment | Path Loss exponent, $n$ |
|---|---|
| Free space | 2 |
| Urban area cellular radio | 2.7 to 3.5 |
| Shadowed urban cellular radio | 3 to 5 |
| In building line-of-sight | 1.6 to 1.8 |
| Obstructed in building | 4 to 6 |
| Obstructed in factories | 2 to 3 |

**Table 2.** Path loss exponent values for various mobile radio environments

### 6.3 Response Time

Network response time is typically tested with a simple message transaction. As an example, consider two hosts (denoted by the identifiers A and B). In ascertaining the network response time, host A will record a timestamp before transmitting a message to host B. Host B then immediately returns an acknowledgement message to A who records a second timestamp. The average difference between the two timings is taken as the *round-trip latency* or response time of the network.

### 6.4 Results

The results from the tests are shown in figure 4 below. Note that the data has been averaged over numerous runs.

The data below show that a network anomaly exists at $\approx$ 87 meters away from the transmitter. The trouble spot is clearly of the message garbling category since both packet loss and response time did not tend towards their maximums (i.e a packet loss of 100% and a response time of would have indicated a disconnection). Due to the relatively small variation in T-R separation, path loss remained approximately constant throughout the experiments. The mean path loss of the experimental environment was calculated, which when compared to the garbled signal strength, indicated that a poor quality (although existent) connection was present. It is envisaged that path loss and signal strength will fulfill a more prominent role when used in city scale testing.

## 7 Conclusion

In this paper, we have presented a novel approach to fault-tolerance in non ad hoc metropolitan area wireless networks. The discussion began with an overview of the Collaborative Computing Frameworks and gave a technical breakdown of the Ricochet wireless network. We highlighted the differences between ad hoc and non ad hoc wireless networks before postulating that the majority of failures in a non ad hoc metropolitan area wireless network were due to environmental factors. Following this, we proposed a new approach to fault-tolerance which introduced the notion of a trouble spot.

[4] In metropolitan scale cellular systems, it is important to select an appropriate close-in reference distance [14]. In these experiments, we used a value of 200 m.

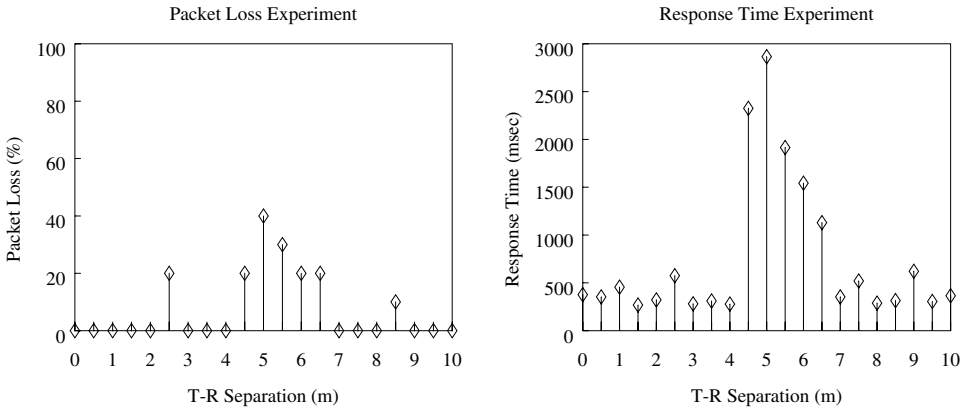


**Fig. 4.** Response time and packet loss experimental results

We then argue that by categorising trouble spots, the system can take both reactive and pro-active action in eliminating the impact of network failures. This raised the question of how to determine the semantics of a particular trouble spot and to address this, we proposed a set of suitable metrics. In section 6 we experimentally evaluated the effectiveness of these metrics.

This scheme is currently being implemented as part of the CCF in Reading and as such is work-in-progress. When finished, an evaluation and critical comparison will be conducted and reported on in a future presentation.

## References

1. E. Bommaiah, M. Liu, A. McAuley, and R. Talpade. *Ad Hoc Multicast Routing Protocol*. IETF Mobile Ad Hoc Networking (MANET) Working Group, August 1998. RFC 2501.
2. M. S. Corson and S. G. Batshell. A Reservation Based Mutlicast Routing Protocol (RBM) for Mobile Networks: Initial Route Construction Phase. *ACM/Baltzer Wireless Networks*, 1(4):427–450, December 1995.
3. S. Corson and J. Macker. *Routing Protocol Performance Issues and Evaluation Considerations*. IETF Mobile Ad Hoc Networking (MANET) Working Group, 1999. RFC 2501.
4. J. J. Garcia-Luna-Aceves and E. L. Madruga. A Multicast Routing Protocol For Ad Hoc Networks. In *Proc. IEEE INFOCOM*, pages 784–792, 1999.
5. J. D. Gibson. *The Mobile Communications Handbook*. CRC Press, 1996.
6. Mobile Ad Hoc Networking (MANET) Working Group. *On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks*. IETF, 1999. INTERNET-DRAFT.
7. The Bluetooth Special Interest Group. The Official Bluetooth Website, 1999. URL: *http://www.bluetooth.com/*.
8. F. Halsall. *Data Communications, Computer Networks and Open Systems*. Addison-Wesley, fourth edition, 1995.
9. Metricom Incorporated. Ricochet Technology Overview, 1999. URL: *http://www.ricochet.com/ricochet_advantage/tech_overview/*.
10. L. Ji and M. S. Corson. A Lightweight Adaptive Multicast Algorithm. In *Proc. IEEE GLOBECOM*, pages 1036–1042, November 1998.

11. S. Lee, M. Gerla, and C. Chiang. On-Demand Multicast Routing Protocol. In *Proc. IEEE WCNC*, pages 1298–1302, 1999.
12. S. Lee, W. Su, and M. Gerla. Ad hoc Wireless Multicast with Mobility Prediction. In *Proc. IEEE International Conference on Computer Communications and Networks*, pages 4–9, 1999.
13. S. Lee, W. Su, J. Hsu, M. Gerla, and R. Bagrodia. A Performance Comparison Study of Ad Hoc Wireless Multicast Protocols. In *Proc. IEEE INFOCOM*, 2000.
14. W. C. Y. Lee. *Mobile Communications Engineering*. McGraw Hill, second edition, 1997.
15. R. J. Loader and J. S. Pascoe. Future Directions of The CCF Project. Technical report, The University of Reading, Department of Computer Science, 2000. Available by request (in press).
16. R. J. Loader, J. S. Pascoe, and V. S. Sunderam. The Introduction of Fault Tolerance to CCTL. Technical Report RUCS/2000/TR/011/A, The University of Reading, Department of Computer Science, 2000.
17. J. S. Pascoe and R. Loader. A Survey on Safety-Critical Multicast Networking. In *Proc. Safecomp 2000*, October 2000.
18. J. S. Pascoe and R. Loader. The Application of Industrial Multicast Network Technolgies to Robotics. In *Proc. 8th International Symposium on Intelligent Robotic Systems*, July 2000.
19. J. S. Pascoe, R. J. Loader, and V. S. Sunderam. The Implementation and Evaluation of Fault Tolerance in CCTL. Technical Report RUCS/2000/TR/011/A, The University of Reading, Department of Computer Science, 2000.
20. T. Rappaport. *Wireless Communications Principles and Practice*. Prentice Hall, 1996.
21. I. Rhee, S. Cheung, P. Hutto, A. Krantz, and V. Sunderam. Group Communication Support for Distributed Collaboration Systems. In *Proc. Cluster Computing: Networks, Software Tools and Applications*, December 1998.
22. G. Sibley. Ricochet Network Personal Communications. Technical Report 1100-01, Department of Math and Computer Science, 2000. Emory University.
23. Y. Tu, D. Estrin, and S. Gupta. Worst Case Performance Analysis of Wireless Ad Hoc Routing Protocols: Case Study. Technical report, Univeristy of Southern California, 2000.