Self-Organizing, Self-Healing Wireless Networks[1]

Chip Elliott, Bob Heile
BBN Technologies
10 Moulton Street
Cambridge, MA 02138
617-873-2615
celliott@bbn.com, bheile@bbn.com

Abstract— Self-organizing, self-healing networks -- also called "ad hoc" networks -- are perhaps the most exciting new trend in networking research and development. Every node in such a network has sufficient intelligence to continuously sense and discover other nearby nodes, dynamically determine the optimal path for forwarding data packets from itself hop by hop through the network to any other node in the network, and automatically heal any ruptures in the network fabric that are caused by ongoing movement of the nodes themselves, changes in RF propagation, destruction of nodes, etc. In essence, one need merely launch such radio nodes into some space and they will not only organize themselves into a network but also adapt continuously to changes in the network's connectivity. The field is currently evolving at "Internet speed" -- the first large-scale systems are now being fielded into the US military and yet many of the field's research fundamentals are at present only very poorly understood. This paper begins with an example that introduces some of the fundamental issues for ad hoc networks (hidden terminals, channel access, mobility, scalability, and power constraints). It then discusses the two dominant approaches in current ad hoc networking technologies, "proactive" and "on-demand" path discovery, and compares the strengths and weaknesses of each approach. The paper then presents two brief case studies with which the authors were intimately involved -- of a 400-node, terrestrial, vehicle-based system and of a high-capacity voice and data networkdeployed among drone aircraft -- and concludes with highlights of the current hot research topics in the field.

TABLE OF CONTENTS

1. INTRODUCTION

Self-organizing, self-healing networks – also called "ad hoc" networks – are perhaps the most exciting new trend in networking research and development. Every node in such a network has sufficient intelligence to continuously sense and discover other nearby nodes, dynamically determine the optimal path for forwarding data packets from itself hop by hop through the network to any other node in the network, and automatically heal any ruptures in the network fabric that are caused by ongoing movement of the nodes themselves, changes in RF propagation, destruction of nodes, etc.

This paper introduces ad hoc networking technology via concrete examples that show the fundamental issues in the field and its breadth of application. Readers interested in learning more about the field should consult two excellent technical overviews of the field [15,23]. Further references are supplied throughout this paper for technical approaches to selected aspects of the field. Since this field is developing very quickly, interested readers should also look up the MANET group (Mobile Ad Hoc Networks) in the IETF (Internet Engineering Task Force) body at www.ietf.org. The MANET group serves as an informal clearing house for current work in ad hoc networks.

2. AN EXAMPLE OF THE FUNDAMENTAL ISSUES

Today's armed forces have a very hard problem as they attempt to transition to "network centric" or "data centric" warfare: to leverage the enormous momentum of modern commercial networking technology – in particular Internet technology – for use in a battlespace with no existing communications infrastructure. They must bring their own networks with them, set them up on the fly, and have the networks automatically adapt to the fluid movements of all the components in this network.

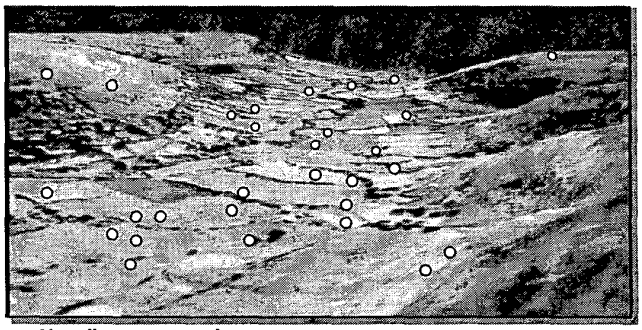

Figure 1 Sample Problem

Figure 1 illustrates one particular aspect of this problem. Here the US Army needs a reliable, high-speed network to connect up to 400 vehicles in a brigade. The vehicles are "dropped" into a landscape without any supporting

[1] 0-7803-5846-5/00/$10.00 © 2000 IEEE

communications infrastructure – no cellular base stations, no fixed radio links, no high-speed satellite data services. And yet they must communicate securely using the standard Internet protocols (the TCP/IP suite) between PC and Unix computers in their vehicles.

How is this possible? In a nutshell, each vehicle contains a small network node that acts as both a radio and a network router. All computers within the vehicle plug into this router via standard interfaces (Ethernet, serial). The nodes execute a suite of "ad hoc" networking protocols that let each node find its nearest neighbors, explore paths through the network, and send messages along these paths (hop by hop, from vehicle to vehicle). As the network topology changes – i.e. as vehicles move in an out of each other's radio range, as jamming occurs, or as nodes are disabled – these protocols automatically adapt to shift traffic flows in reaction to the changes. All the constant buzz and confusion of these ever-shifting radio links is totally invisible to the computers that are attached to the network nodes, however. These computers run the standard applications (mail, web browsers, etc.) and any specialized military applications based on standard IP networking technology. The application programs are unaware that the network is shifting under them; at their level, the network appears to be a stable Internet, albeit one with constantly changing end-to-end delays.

At first blush, this problem resembles that of cellular telephony systems. After all, cellular systems also route traffic to and from moving vehicles. The difference appears minor but is in fact profound: in an ad hoc network, all the base stations are moving too. They are driving at 50 miles per hour through hill and dale! In fact, there is no actual difference between a "base station" and an "endpoint" in ad hoc networks. All nodes are created equal. (We shall see in a case study below how some networking protocols can create "base stations" on the fly, as needed, and retire them when the need passes.)

Two key technical issues differentiate ad hoc networking technologies from cellular technologies and indeed from conventional networking:

- Media-Level Channel Access
- Routing Protocols

The following sections briefly describe each of these issues and the most popular of the current technologies for addressing the issues.

3. Channel Access Techniques

Channel access poses a particularly difficult set of challenges for wireless ad hoc networks. Figure 2 shows in schematic form the fundamental issue, namely, the so-called "hidden terminal problem." This problem arises in a variety of forms; our figure presents the case in a network node (radio, or "terminal") A transmits a packet to node B, at a time that overlaps with a packet transmission from C to D.

Note that neither A nor C is able to determine, by themselves, that this condition is occuring. One likely result of such overlapped transmissions is that both packets will be too garbled to be properly received at their intended destinations; another is that one of the two packets will arrive intact. This might seem like a trivial issue but in fact the experience of many decades has shown that unresolved hidden terminal problems very decidedly lower the message completion rate for an ad hoc network, and thus severely damage the overall network throughput for such networks.

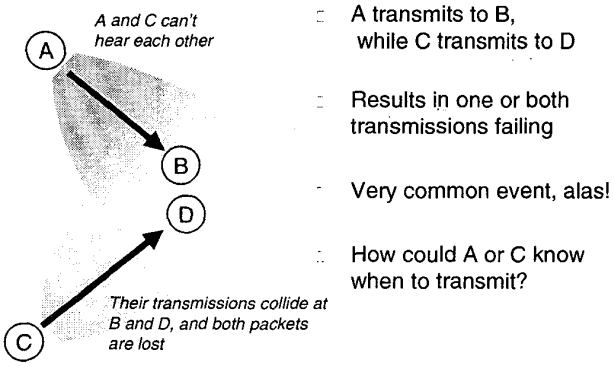

Figure 2 The Hidden Terminal Problem

Many solutions to the hidden terminal problem have been proposed over the course of the past twenty years. A representative sample is in [3,4,6,7,8,13,19,25,26,28]. The two most popular families of solutions are what we call the RTS / CTS approach and the Timeslot approach. Figure 3 illustrates these two competing approaches, together with their associated strengths and weaknesses.

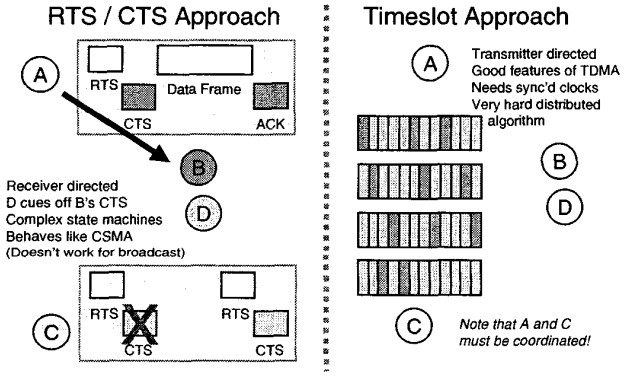

Figure 3 Channel Access Mechanisms

RTS / CTS stands for Request-to-Send, Clear-to-Send. It is a form of Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). As such, the closest mental model for the networking community is that found in Ethernets. When Node A wishes to send to Node B, the following sequence of steps takes place. First A transmits an RTS. If Node B is itself busy, transmitting or receiving, it will not respond at all to the RTS. Furthermore if the channel is already reserved around B, it must not respond to the RTS. Node A will continue to send RTS messages until either some retry limit is reached, or it receives a CTS from B. B's CTS has two functions: it tells A to go ahead and send the data packet, and it tells all other nodes in range to hold off from their transmissions (or sending their own CTS) until Node A's packet transmission is complete. In effect, the CTS creates a zone of silence around Node B. Node A then sends the data packet to B, and B acknowledges its receipt via an ACK message. The complete transaction therefore has four steps: RTS, CTS, Data, ACK.

The RTS / CTS approach has been known for many years [4,13,30] and is widely adopted in radios designed for ad hoc networks. Well-known examples include amateur packet radio networks and the IEEE 802.11 wireless LAN standard.

The state machines that govern exactly when a CTS can be sent are surprisingly tricky, and many variants of this basic scheme have been proposed. These variants attempt to deal with such cases as one RTS stepping onto another RTS, an RTS stepping on a CTS, and so forth. To date there are no convincing performance studies that give good guidance as to which variant to adopt.

In general, the RTS / CTS approach is a good match for typical Internet traffic, which is now widely believed to be "fractal" in its offered load, i.e., highly unpredictable and bursty. This approach makes no attempt to schedule the channel; when a node needs to transmit, it requests the channel and the usual CSMA/CA channel utilization ensues.

Figure 3 also illustrates, in highly schematic form, the basic timeslot (Time Division Multiple Access) approach to ad hoc channel access [e.g. 3,8,21]. Here each node is provided with a schedule for when it is allowed to transmit; some variants also include information as to when the node should turn its receiver on. (Turning the receiver off when not needed can reduce the power requirements for a transceiver.)

The timeslot approach works well at the channel level. It provides the basic building blocks for two valuable services: guaranteed Quality of Service (QOS) since channel access can be scheduled; and receiver power management. However, it imposes a very heavy burden on the ad hoc network layer, namely the burden of calculating and distributing timeslot schedules to the nodes in the network. Such schedules are not difficult to provide for networks whose nodes are stationary. Imagine however that we start with two distinct groups of nodes, each with its own neatly arranged set of timeslots for the nodes in a given group, and that subsets of these nodes move between groups, or indeed that all nodes move within radio range of each other. All the schedules must then be recalculated and distributed to the affected nodes. In essence, these algorithms need to "tile the plain" with harmonious timeslot allocations, much the way that cellular systems perform spatial reuse of frequencies or timeslot schedules. But since all the nodes are constantly shifting around, changing the timeslot schedules in one area very likely has ripple affects that require creating new "colors" (timeslot schedules) across large swaths of the network [24]. Timeslot methods have the further drawback that they work poorly in areas where nodes are densely packed. Each node needs its own slot in one very large shared schedule, and this makes for a relatively large average delay before any node can access the channel.

As mentioned above, a number of other channel access mechanisms have been proposed [e.g. 6,7,19,25,26,28]. In general, though, each of these schemes have properties similar to one of the two approaches described. At present, therefore, one must choose between a very simple CSMA/CA scheme with no hard QOS features, or a complex TDMA scheme that does provide hard QOS.

We now turn to another important issue in channel access, namely the power level to employ for transmissions in the network. Figure 4 illustrates the basic trade-off for power levels. A source node can send a packet to a destination node by either (a) transmitting at sufficient power to deliver the packet directly to the destination, or (b) sending by a series of lower-powered hops. Unfortunately, both approaches have serious drawbacks.

Transmitting at high power, with as few hops through intermediate nodes as possible, generally leads to the lowest overall delay for delivering the packet. However, it also leads to the lowest overall network throughput, since a high-power transmission leads to a large self-interference zone. All nodes within this large zone must keep silent during the high-power transmission, and thus the net system throughput is lower than in networks with better spatial reuse.

Transmitting packets via a series of low-power hops gives good spatial reuse, and hence leads to a network with high overall capacity. However the series of hops incurs a penalty: delay. In most packet-based systems, an entire packet must be received before it can be retransmitted. Thus the total delay equals the number of hops times the sum of the channel access delay for each hop plus the transmission time required for each packet. Speaking loosely, then, an n-hop path requires n times the delay of a single-hop transmission.

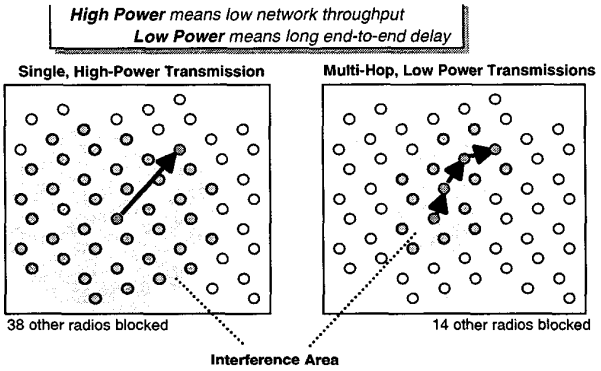

Figure 4 The Delay / Throughput Trade-off.

Ideally, the radios used in ad hoc networks can dynamically adjust the power levels used for transmission on a packet-by-packet basis [e.g. 18,25,27,29]. Then the networking protocols can work together with the channel access mechanism in order to perform the best trades across power, self-interference, and delay. Such trades cannot be made at either one of the layers alone, since they require knowledge of the wireless channel itself, and of the overall network topology, and (if possible) of predicted other traffic in the network.

4. AD HOC ROUTING TECHNIQUES

We now turn to the other major issue in ad hoc networks, namely routing. Routing protocols and their associated algorithms are used to determine paths through the network so a packet can get from its source, hop by hop, to its destination(s). In general, one goal of routing is to choose a suitably "efficient" path, where efficiency can be measured in power expended, amount of self-interference, delay, etc. There are at present two primary families of routing protocols, although others have been used in the past, and there is no compelling reason to believe that these are the only two approaches that will work. One family is the "proactive" routing protocol, which are similar to protocols widely deployed in traditional networks. The other are "on demand" protocols that attempt to determine network paths only as the need arises.

Figure 5 illustrates two important types of "proactive" routing protocols: Link State and Distance Vector. The

relative merits of these two types have been argued for many years and will not be discussed here. The key differences between the two types are easy to summarize, though. Link State allows every node in the network to have an up-to-date "map" of the entire network topology, but at the expense of distributing a certain amount of control traffic to every node so that it can have this map. Distance Vector provides noticeably less information to each node ("all those nodes are over that-a-way") but usually can do so with control traffic that is localized to places where the network topology is changing.[2]

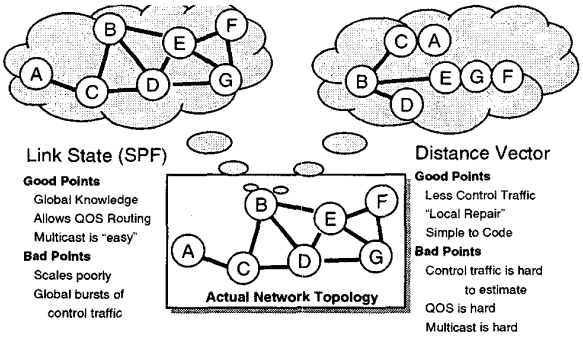

Figure 5 "Proactive" Routing Protocols.

"Proactive" routing protocols constantly monitor the network topology, i.e., determine which node is in radio range of which other nodes. Whenever they detect a change in the topology, they send control traffic so that the routine tables in all the nodes properly reflect this change. Thus in ad hoc networks with mobile nodes, or jamming, or any other source of changes in link connectivity, such networks will have a certain "background hum" of control traffic. As the rate of change increases, the level of control traffic will rise until finally at some point the routing protocols will no longer be able to properly track the current network topology, as they will have exceeded either an artificial cap placed on the amount of control traffic in the network or indeed have exceeded the available channel capacity. See [8,15,17,22,23] for examples of proactive protocols.

"On demand" protocols take a different approach. Such protocols wait until the last second to determine the path that a packet will take through the network. Figure 6 shows the basic steps in a generic "on demand" routing protocol, shown in highly simplified form. See [2,5,9,16,20,] for specific protocols using this approach.

Step 1 is some form of flood search, where the source node (A) sends a query into the network asking for a path to B. In Step 2, the query has made it all the way to B, who then replies with an "I am here" message. This message flows backward through the network to A, and as it does, every node along this backward path learns of the path from itself towards B. Finally in Step 3, A can send a data packet and all the nodes along the way know how to forward the packet towards B. As can be readily imagined, "on demand" protocols usually employ some form of cached information, so that as newer paths to B become available (e.g. as nodes move in the network and the old paths become invalid) the routing tables can be updated.

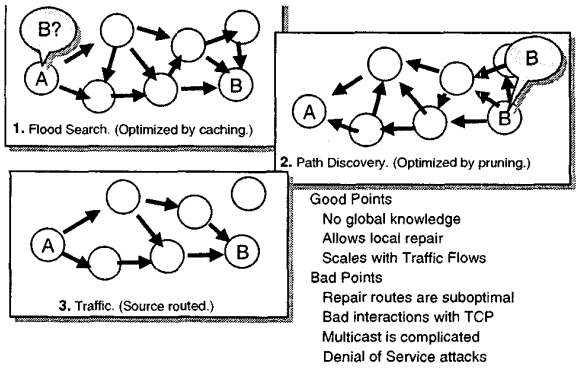

Figure 6 "On Demand" Routing Protocols.

"On demand" protocols scale differently from "proactive" protocols, and in some ways better. The main benefit is that the network expends no "background hum" of control traffic monitoring network topology that no one cares about. The topology is only maintained for those parts of the network that are currently bearing traffic.

These protocols have a number of important drawbacks, however. First, they invoke flooding in order to determine paths to destinations; such flooding can be vulnerable to denial-of-service attacks, for instance, by endlessly requesting a path to some node that doesn't exist in the network. Second, it is difficult to know when cached routing information has become invalid, or which node has a better (newer) cached path towards a destination. There is a tension between setting short cache timers in order to react to network topology changes (e.g. find a shorter path to a node that has moved) vs. the expense of performing a flood when caches have aged out. Third, there is often a "setup" delay for the first packet from a source to a new destination; for intermittent traffic the expense and delay of this setup may dwarf the actual data transmission cost.

In our judgement, it is unlikely that one family of routing protocols is in every case superior to the other. Rather each will show its strengths in certain situations, i.e., for certain predicted mobility models, traffic, and so forth.

5. Case Study #1 – Terrestrial Networking

Our first case study shows one BBN approach for a terrestrial, radio-based ad hoc network. This network is now deployed as the US Army's Near-Term Digital Radio (NTDR) network. It is designed to act as the data-hauling backbone for a brigade's tactical internet. The network accomodates up to roughly 400 vehicles that are driving at speeds of up to 60 or 70 mph. RF links are based on UHF radios, and provide a user-observed throughput of roughly 288 Kbps.

Figure 7 depicts the NTDR Network's overall topology. It is a two-level hierarchical network, with groups of nodes organized into "clusters." Each cluster has a cluster head which acts somewhat like a cellular base-station for that cluster. However, there is no physical different between a cluster head and a member; instead, the ad hoc networking protocols are used in order to automatically make nodes into

2 The two protocols also have rather different patterns to their "convergence times," which is the amount of time that elapses between when a network topology changes and when that change is adequately reflected in the routing tables maintained in each node. This issue, while important in practical networks, is too complex to summarize here.

cluster heads as needed, and to make them resign when the need passes.

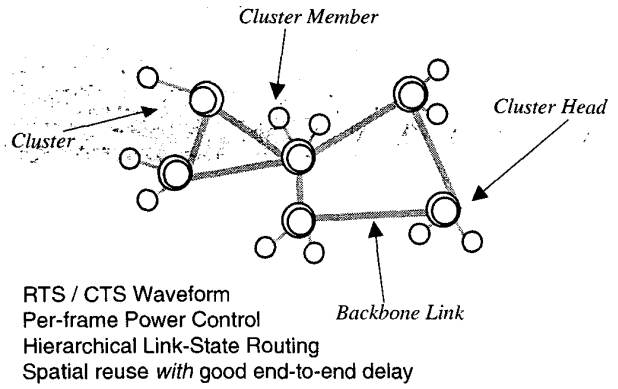

Figure 7 A Hierarchical Ad Hoc Network.

As indicated, this network employs an RTS / CTS waveform because it is designed to carry bursty and unpredictable traffic. The NTDR waveform provides a series of priorities for message traffic, and these priorities are reflected in the RTS / CTS mechanism. Put briefly, the higher priority packets have a shorter time window between RTS and CTS than do lower-priority packets, and thus have a much higher probability of seizing the channel. This radio also provides per-frame power controls.

The NTDR network uses specialized protocols to organize itself into a number of clusters, whose cluster heads are interconnected via a backbone. One set of RF channels are devoted to local (intra-cluster) communications; another are devoted to backbone communication. Thus cluster members communicate with each other, and with their cluster heads, on one channel; and cluster heads communicate among themselves on the other channel.

NTDR's two-level hierarchy plays an essential role in helping to balance the trade discussed above of network capacity vs. delay. The bulk of communications within the network is performed at very low power, i.e., from one cluster member directly to another or to a cluster head. This low power allows a great deal of spatial reuse, and thus boosts the overall network capacity. A smaller fraction of the traffic must traverse a "long haul" route from a cluster member to its cluster head, then across the backbone by a series of hops between cluster heads, and finally the ultimate delivery to its destination member. In this case, the first and last hops are performed on the local channel, and the backbone hops on the other channel. The backbone links are formed at relatively high power in order to form "giant steps" across the network. This arrangement of local transmissions at low-power combined with long-haul transmissions at high power gives the balance between overall capacity and delay.

NTDR's routing is a hierarchical "proactive" (Link State) protocol, and here again the hierarchy is essential. Control traffic in Link State protocols grows rapidly with the number of links in the network topology. A flat network with a thousand nodes would be completely infeasible in conventional Link State protocols; the background control traffic would vastly exceed the available channel capacity. In the NTDR network, however, only the cluster heads participate in the full Link State protocol. Since this number is vastly smaller than the number of cluster members, the control traffic is brought down to a level that can be easily accomodated in the RF channel.

Since the cluster heads contain complete and up-to-date maps of the entire network, they are able to perform sophisticated algorithms that depend on such knowledge. For example, the NTDR network can support optimal distribution trees for "multicast" (one to many, or many to many) traffic so that a single packet can be sent for delivery to a large number of destinations. Such complete map information also allows a potential upgrade to new algorithms that deliberately "shape" the network to better match its current traffic flows. These types of features are difficult to deploy using "on demand" protocols.

6. Case Study #2 – Drone Aircraft Networks

Our second case study describes another BBN ad hoc network which the authors helped design. Figure 8 shows the overall architectural context for this network, namely, as one piece in a very large ad hoc network built of a number of self-organizing sub-networks and component RF technologies. A number of different radios are employed in this large network, and these radios are sited on a wide variety of platforms. Reading the figure from the top, we see both geo-synchronous and low-earth orbiting satellite systems, an ad hoc network of drone aircraft (discussed below), another network of high-speed ATM "trunk" microwave radios, the NTDR network providing a high-mobility backbone, and hand-held radios that provide packetized voice and data via an ad hoc network.[3]

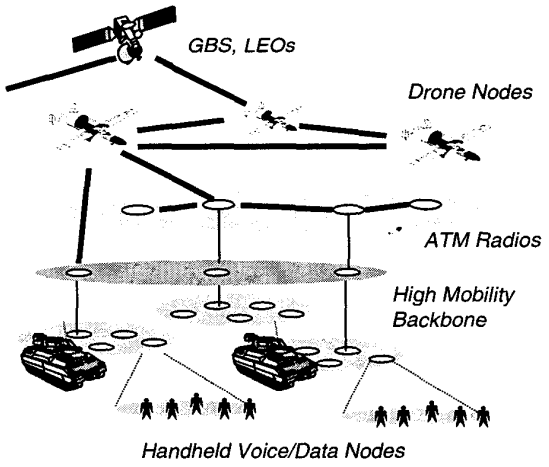

Figure 8 Ad Hoc Network with Drone Aircraft.

This airborne network of drone nodes is being undertaken for DARPA under its Airborne Communications Node (ACN) program. The drone aircraft are expected to be Global Hawk UAVs. Each drone supports a number of high-capacity directional RF links between the drones and to ground stations. These links act as the "backbone" of this particular ad hoc network. As nodes (drones or ground stations) enter the network, new links are formed and the nodes automatically enter the network and begin to

[3] Every network system in this picture has either been built, or is currently being built, by the BBN team represented by the authors.

exchange traffic with other nodes. As nodes exit the network, e.g. to land and refuel, the links are removed.

In addition, each ACN drone aircraft supports a number of "access" services to user devices on the ground. Such services include a PCS-like telephony service, with the drone aircraft as the base station; a paging service; an Internet service for hand-held data devices; and so forth. This setup is somewhat like a conventional cellular system with the notable exception that the base station moves. For example, the drone aircraft may pass out of range of the user devices on the ground and be replaced overhead by another aircraft. Even harder, a drone aircraft may land for refueling and be replaced by a totally new drone that must take over in mid-conversation. In this system, then, the base stations are "handed off" in addition to also having the user devices handed off!

Our approach in this system is resembles that for NTDR. Here the drones act as "cluster heads" and the user devices on the ground act as "cluster members." Once again, routing is performed only between cluster heads, i.e., drones; user devices do not participate in routing protocols. In addition, the RF links between aircraft are constantly monitored for error rates, and the link speed (i.e. FEC level) is constantly adjusted to achieve the best possible performance. In response to these constantly changing link speeds, the network routing tables are constantly being adjusted so they reflect the current best path through the network.

7. Selected Research Areas

The field of ad hoc networking is currently in a creative ferment and a number of distinct research areas are currently receiving attention. The field is indeed notable for its unfinished state. Major systems are already being deployed even though many basic parts of the technology are only partly understood. This section, then, is intended as a "snapshot" of the current research areas that the authors find most interesting.

Hidden Terminal Issues in Broadcasts. The hidden terminal problem has been demonstrated to cause severe performance issues for ad hoc networks, and thus various types of channel access mechanisms have been employed to eliminate or at least mitigate its effects. However, such mechanisms do not work well with broadcast RF transmissions. The problems vary depending on the exact channel access method. RTS / CTS waveforms have no obvious way to deal with a broadcast message; who would send the CTS and what would the corresponding zone of silence be? Timeslot waveforms fare much better with the following two exceptions. First, some timeslot must be reserved for nodes that are moving into the vicinity and must request a space in the schedule; these timeslots are difficult to protect against hidden terminal problems. Second, allowing each node to use its own transmit timeslot for a broadcast makes receiver power management less effective since the receiver must be turned on during all such timeslots. Since the majority of radios currently used in ad hoc networks employ RTS / CTS waveforms (e.g. 802.11 radios), these difficulties are of current practical importance. In particular, routing protocols that rely on beaconing and/or flooding may well suffer from this problem. In addition, those "on demand" protocols that expect to broadcast information so that it can be readily "snooped" by nearby nodes will also suffer. To our knowledge, such issues have not yet been studied in any thorough or quantitative way.

Characterizing Performance Envelopes for Routing Protocols. Each type of routing algorithm has its own ways of breaking under stress, and indeed suffers from different kinds of stress. For instance, Link State algorithms suffer in a predictable way from increasing number of links in the network, and the rate of change of such links which is in turn related to change in RF propagation caused by movement, jamming, self-interference, etc. Distance Vector protocols suffer from similar kinds of stress, but react in different ways. The "on demand" protocols are much more sensitive to the exact traffic flows through a network. At present, there are no overall quantitative studies of how the various mechanisms fail in response to certain types of stress.

Power-Management Issues. Once one assumes that some or all of the nodes are battery-powered, a whole new level of issues arises. By and large, the entire area of "power managed ad hoc networks" is a new research field. The issues range from attempting to perform channel access and routing in ways that minimize energy, to deciding whether it is better to run one node's battery down to empty or spread the load over a number of nodes, to tightly coupling battery discharge characteristics to the high-level strategies for keying transmitters.

Intentional Topologies. In areas where network nodes are densely packed, each node may have a very large number of "potential neighbors" with which it can exchange routing or control traffic. It is often desirable to turn down the node's transmit power and select some subset of these potential neighbors as a node's actual neighbors. In particular, the number of bits required for various types of control traffic often grows more than linearly with the number of actual neighbors. Contrariwise, in areas where nodes are sparsely packed it may be advantageous to turn up the power and attempt to gain a few more "far away" neighbors. But of course as nodes surge around in space, areas that were sparsely populated suddenly become densely populated, and vice versa. And in many ad hoc networks, the nodes can even move; thus some nodes can be moved to more advantageous positions to act as "relays" that improve the overall network topology. This is a very promising field, and the work in this field is likely to have very useful results.

Aspects of Scalability. The simplest measure of scalability is the pure number of network nodes. Scalability in even this simplest sense is still very poorly understood, because the actual number of nodes is not so important as the topology of the nodes and the underlying event model, i.e., the number of messages per second, change in RF connectivity between nodes, and so forth. The relationship between number of nodes and the topology and event model is by no means clear; for instance, do a thousand nodes simply cover ten times as much territory and experience ten times as many link outages as a hundred nodes? It's probably not so simple. Current technology works for networks of some hundreds of nodes; much larger nodes are still problematic. Other aspects of scalability are even less well understood. The interaction of channel access with higher-level protocols such as TCP will influence the offered load on the network and thus the self-interference and indeed even the channel access delays. How can one properly capture such effects?

8. Summary

Ad hoc networks offer that most intriguing blend of practical applicability and still-unsolved research problems. The first networks are now being deployed for real operational use,

and many more are sure to follow in short order. Yet large parts of the technology are still imperfectly understood. This paper introduced the technology and its major issues, illustrated with several examples of ad hoc networks that have actually been built, and concluded with a list of outstanding research issues.

9. REFERENCES

[1] Norm Abramson, "The ALOHA System". Proc. Fall Joint Computer Conf, AFIPS, 1970.

[2] George Aggelou, Rahim Tafazolli, "Relative Distance Micro-discovery Ad Hoc Routing (RDMAR) Protocol," IETF draft-ietf-manet-rdmar-00.txt. September 1999.

[3] A. Alwan et al, (Gerla & Kleinrock at UCLA): "Adaptive Multimedia Networks", my database doesn't say where it was published, 1996.

[4] Vaduvar Bharghavan, A. Demers, S. Shenker, L. Zhang, "MACAW: A Media Access Protocol for Wireless LANs," ACM SIGCOMM conference, 1994.

[5] Josh Broch, David B. Johnson, David A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," IETF draft-ietf-manet-dsr-02.txt, June 1999.

[6] Digital Ocean patent, "Medium access control protocol for wireless network", 1993.

[7] Robert Gallagher, "A Perspective on multiaccess channels", IEEE Trans. on Information Theory, March 1985.

[8] Mario Gerla and J. Tsai, "Multicluster, mobile, multimedia radio network", Baltzer Journals, 1995.

[9] Zygmunt Haas, Marc Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," IETF draft-ietf-manet-zone-zrp-02.txt. June 1999.

[10] IEEE, *Special Issue on Packet Radio Networks*, Proc. IEEE, 75(1), January 1987.

[11] Mingliang Jiang, Jinyang Li, Y.C. Tay, "Cluster Based Routing Protocol (CBRP)," IETF draft-ietf-manet-cbrp-spec-01.txt, August 1999.

[12] Kahn et al, "Advances in packet radio technology", Proc. IEEE, Nov 1978.

[13] Phil Karn, "MACA – A New Channel Access Protocol," ARRL/CRRL Amateur Radio, 9th Computer Networking Conference, September 1990.

[14] Leonard Kleinrock and John Silvester, "Spatial reuse in multihop packet radio networks," Proc. IEEE, 75(1), 1987, pp. 156-167.

[15] Greg Lauer, "Packet-Radio Routing," pp. 351-396, in Routing in Communication Networks, ed. Martha Steenstrup, Prentice Hall, 1995.

[16] Sung-Ju Lee, William Su, Mario Gerla, "On-Demand Multicast Routing Protocol (ODMRP) for Ad Hoc Networks," IETF draft-ietf-manet-odmrp-01.txt. June 1999.

[17] Clifford Lynch and E. Brownrigg, *Packet Radio Networks*. Pergamon Press, 1987.

[18] Metricom patent, "Automatic power level control of a packet communication link", 1993.

[19] Robert Morrow and J. Lehnert, "Packet throughput in slotted ALOHA DS/SSMA radio systems with random signature sequences". IEEE Trans Comm, July 1992.

[20] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das, "Ad Hoc On-Demand Distance Vector (AODV) Routing," IETF draft-ietf-manet-aodv-04.txt, October 1999.

[21] S. Ramanathan, "A Unified Framework and Algorithm for Channel Assignment in Multihop Wireless Networks," Wireless Networks 5 (1999), pp 81-94.

[22] S. Ramanathan and M. Steenstrup, "Hierarchically-Organized, Multihop Mobile Wireless Networks for Quality-of-Service Support," ACM Baltzer MONET (to appear).

[23] S. Ramanathan and M. Steenstrup, "A Survey of Routing Techniques for Mobile Networks," ACM Baltzer NOMAD Special Issue on Routing in Mobile Networks (sister journal of ACM Baltzer Wireless Networks), August 1996.

[24] S. Ramanathan and E.L. Lloyd, "Scheduling Algorithms for Multihop Radio Networks," IEEE/ACM Transactions on Networking, April 1993.

[25] T. Shepherd, MIT PhD thesis, Laboratory for Computer Science, *Decentralized Channel Management in Scalable Multihop Spread-Spectrum Packet Radio Networks.* (July 1995)

[26] Elvino Sousa and J. Silvester, "Spreading code protocols for distributed spread-spectrum packet radio networks", IEEE Trans Comm, Mar 1988.

[27] James Stevens, "Spatial Reuse through Dynamic Power and Routing Control in Common-Channel Random-Access Packet Radio Networks," SURAN Program Technical Note (SRNTN) 59, August 1988.

[28] J. Storey and Fouad Tobagi, "Throughput performance of an unslotted direct-sequence SSMA packet radio network". IEEE Trans Comm, August 1989.

[29] H. Takagi and L. Kleinrock, "Optimal transmission ranges for randomly distributed packet radio terminals", IEEE Trans Comm, vol. COM-32 (3), pp. 246-257, March 1984.

[30] John Zavgren and Greg Lauer, "The Performance Improvement from Receiver-Directed Transmissions in Packet-Radio Networks," Proc. IEEE Tactical Comm. Conference, pp. 65-72. Fort Wayne, May 1988.

10. BIOGRAPHIES

Dr. Robert F. Heile is a 20 year veteran in the field of data communications and wireless data. He is the chair of 802.15, the IEEE working group on Wireless Personal Area Networks, and is currently part of the GTE Technology Organization. Bob joined BBN in early 1997, prior to its

acquisition by GTE, as Vice President, Engineering and Manufacturing for Internetwork Technologies with the mission of commercializing wireless ad hoc networking and wireless personal area networking technologies. From 1990 to 1996, he served as Vice President of Engineering and Business Development for TyLink Corp, a bootstrap start up specializing in high speed digital access products and network and circuit management software, and was a co-founder of Windata, Inc., a developer and manufacturer of wireless local area networking equipment. From 1980-1990, Bob was with Codex Corporation, a subsidiary of Motorola, where he was Vice President/General Manager, Transmission Products, the company's largest and most profitable business unit. Bob holds a Bachelor of Arts degree from Oberlin College, and Master of Arts and Doctorate degrees in Physics from The John Hopkins University.

Chip Elliott is Principal Engineer at BBN. He is currently designing the networking component of the Discoverer II satellite system. Mr. Elliott was chief system architect for the networking component of the U.S. Army's Near-Term Digital Radio (NTDR) program and for the Canadian IRIS tactical network, an advanced telephony network that provides voice, data, plus video conferencing over a packetized IP base. He has provided senior architectural design for other projects, including DARPA's Airborne Communications Node Program, DARPA's Small Unit operations program, and a commercial LEO satellite system. Mr. Elliott serves on the Naval Studies Board for Network-Centric Warfare, under the auspices of the National Academy of Sciences, and on the Defense Science Board task force on Television and Radio. He has previously served on the Army Science Board's "Gray Beard" Panel, which provided a senior review of the U.S. Army's overall tactical Internet design.