

Possible Improvements in Ad Hoc Networks to Lead Towards Ubiquitous Computing

Charles C. Hoffmeyer
cchoffme@cchoffme.com

Michigan Technological University
Houghton, Michigan 49931

Abstract—Wireless data communication systems have been desired for many years, but attempts have failed to be successful in fulfilling user needs. These failures range from cost, connectivity, reliability / quality of service, routing and configuration. With some intervention, Ad Hoc networks could allow for ubiquitous computing. This paper will focus on improvements to Ad Hoc technologies in aforementioned realms.

I. INTRODUCTION

Computers are everywhere. Wherever we go, we use technology - work, class, and home. We carry it with us in PDAs and communicate via cellular networks. There are even computer chips in our tennis shoes. With the information potential at our fingertips (or toes), one must ask what is keeping us from connecting to the network ubiquitously. Why have we failed to obtain this goal?

The simple answer is that current connectivity is variant, and alternatives are costly. In the mid 1990's, mobile users could purchase bulky satellite network interface devices. These were highly sensitive to weather, only worked in a small number of areas due to limited coverage areas, and were incredibly costly (both to use and maintain). Many people chose not to communicate while mobile over this network because of these limitations. In the late 90's, cellular providers began selling broadband data access over their infrastructure. This too was very costly (often ranging from a dime to a dollar or more per minute) and frequently lost connection during peak voice usage times. While effective, the shortfalls have kept users from maintaining constant connectivity. As of late, 802.11a, 802.11b, and 802.11g wireless networks (also known as WiFi networks) are being deployed for consumer use. WiFi networks have the advantage of providing users with instant, fast connectivity at little cost beyond the initial equipment. These too fail, mostly due to their short communication range, resulting in a

service capacity of a rather limited number of nodes in a given region.

This does not mean we should give up on the idea of continuous connectivity. Rather, we should look to the unconventional decentralized Ad Hoc network. These networks rely on only the existence of other nodes to communicate and pass messages. In the past, this network style was considered highly inefficient and unreliable. However, with protocol enhancements, Ad Hoc networks could bring a ubiquitous computing environment that users have desired for years.

Improvements discussed include connectivity and configuration, routing, and reliability / quality of service.

II. CONNECTIVITY AND CONFIGURATION

Ad Hoc wireless network nodes present a unique problem in terms of connectivity and configuration. Random nodes that may have never been seen on any network before, which want to become part of a preexisting one must determine how to configure themselves properly. In addition, unlike traditional networks, nodes may appear and disappear at random or they may change their identities by moving around the capable network range.

The number of nodes possibly connecting to the network suggests that it is not possible to manually configure each node, and since we do not know all the nodes that may become part of the network, they cannot be pre-configured. Energy constraints also limit the distance that any one node can communicate, or reach a central node for configuration information (if such a node exists). To achieve connection, there are two effective solutions: MAC and Self-Configuration.

In [5], A virtual backbone (Fig. 1) is constructed by centrally localized nodes. Each backbone node is one hop away from another backbone node and/or one hop away from the node desiring to be on the network. The Medium Access Control address (MAC) is broadcasted

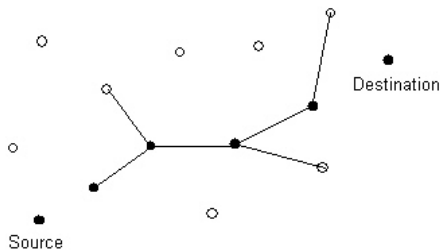


Fig. 1. Virtual Backbone Connectivity

by the joining node and received by a backbone node. That backbone node adds it into its 'connecting dominating set'. In doing so, any messages travelling along the backbone for a given node can be broadcasted only in the region where the node had been last seen by the backbone, and ensure connectivity at all times to the network. The only downside to this is that the node must know which protocol to use and how to request service constantly until it receives a network response.

Connectivity can also occur by Self-Configuration. The ASCENT (Adaptive Self-Configuring sEnsor Network Topology) project at UCLA [1] provides a means for short range nodes to communicate with as few nodes as technically feasible. Instead of having a virtual backbone, as in [5], nodes communicate directly with the destination node whenever possible. To join the network, the requesting node broadcasts its presence to an awake node. It in turn assigns it a unique identifier and alerts the other nodes of the requesting nodes presence. The nearby 'neighbors' introduce themselves to the requesting node, so it knows who it can communicate with. Its map of in-range nodes changes as it moves about the region.

How nodes connect is very important to maintain stable network connectivity. The first method uses a 'one hop to the backbone' technique. This is similar to the physical infrastructure of the Internet, which is a well tested and working method. At the same time, this method can result in large demands to the node chosen as part of the virtual backbone in user-condensed regions. Not only does this increase delay and congestion, but can drain energy resources of the backbone node rapidly. This can be accounted for by decreasing the disk-radius range around each backbone node, but in turn this will reduce the accessibility to the network.

A more ideal solution would be to combine these two methods of connectivity. Maintaining a reasonable virtual backbone is necessary, but each nodes transfer radius will need to be significantly reduced in compar-

ison to stand-alone nodes. If a node can communicate with another without use of the backbone, it should do so whenever possible. Each backbone node must have the capacity to control its relay. This is to ensure that the energy of one node is not consumed more than is desired during peak usage. Our backbone now becomes flexible as other nodes can relay traffic during times where a node previously providing backbone service had become overwhelmed. Multiple hops on all nodes must be allowed to make this solution tenable.

For connectivity to the Internet, there must exist some node on the Ad Hoc network which is a physical interface node that can repackage and retransmit Internet data. Many of these nodes should exist in larger networks to avoid Internet bound traffic congestion. If the Ad Hoc network uses the TCP/IP protocol, this can be done with ease.

III. ROUTING

In physical networks, computers are expected to remain in the same location at all times. This decreases their problem complexity in routing packets to that node as traffic to a location becomes more specific. Unfortunately, this complexity causes trouble with Ad Hoc routing and ensuring that packets are received by their intended destination because nodes can appear or vanish out of communication range at 'random' and they can also move around within the network region. As such, specialized routing techniques are necessary. This section will discuss the a range of routing protocols.

A. Hop-By-Hop

In the Hop-By-Hop routing method, all nodes are considered equal to one another, with the exception of their capable bandwidth. Each node maintains information about the network topology, as they see it (Fig. 2). [6] requires that the following assumptions be met for Hop-By-Hop to function properly:

- 1) Topology information is obtained by routing nodes using a link-state routing protocol.
- 2) Each node independently makes decisions.
- 3) All nodes receive the same amount of bandwidth, and there is a limit to the number of nodes admitted through it.
- 4) Queueing delays at each node account for the largest part of the delay. Premium traffic should experience near-zero delay.

This model also requires that all nodes in the region are connected by one or more edges to other nodes. Before transmitting, this network protocol establishes a

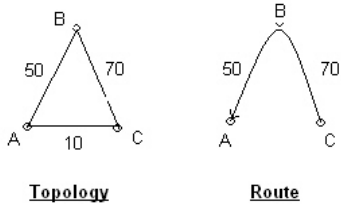


Fig. 2. Hop-By-Hop

virtual circuit, determining which path to take by considering its available bandwidth. As bandwidth becomes unavailable on the larger paths, smaller capacity paths can be used efficiently until the load disbursts. One concern in similar style routing protocols is that loops will occur in routing, causing the packet to be ‘lost’ within the network. As Hop-by-Hop ensures a simple path, this cannot occur. Redundancy is eliminated as the path is set up.

B. Quality of Service Routing

“Quality of Service Routing requires not only to find a route from a source to destination, but a route which satisfies the QoS requirements” [9]. Generally, this includes terms of bandwidth allotted to the communication, and delay limits. This type of routing is incredibly difficult in wireless networks because of the ever changing topology and sharing of bandwidth among close nodes. QoS routing is best used when topology change is rare to moderate.

Zhu proposes that there be a certain and limited number of ‘slots’ where communications can be made, each with their own fixed bandwidths. When a node wants to use the network, it must reserve slots and establish a communications path. This route cannot contain conflicts if it is expected to maintain Quality of Service. Also, “When a node n_i transmits to n_j , in slot s_k , n_j itself does not transmit (a node cannot receive and transmit at the same time) and n_i is the only transmitting neighbor of n_j in that slot” [9]. This ensures two things in the quest to obtain Quality of Service:

- 1) no other inbound communications are heading to n_j from neighbors, and
- 2) n_i can transmit without causing interference to its neighbors.

If a path breaks due to mobile nodes, a reliable path must be reestablished by the requesting node, if Quality of Service is desired. Due to the nature and reliability

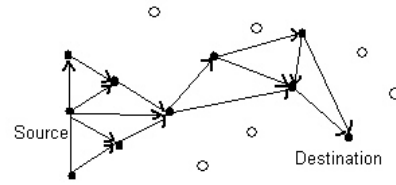


Fig. 3. Gossip Based Routing

of Ad Hoc networks, this routing protocol works best in small networks with low node mobility.

C. Gossip Based Routing

Gossip based networks for data communications operate in a similar fashion to common “office gossip”. As in water-cooler conversations, one person tells a group of people something which results in some of those people relaying the same message to other groups, and so on. One significant difference is that while conventional office gossip is sometimes modified in the transfer, data gossip can be repeated exactly as it was received. This ensures high reliability in end to end message verification. As these examples show gossip has proven to be a valid means of message routing.

Example 1: This past September, I went to Chicago with a friend. A teacher in the middle of Michigan told another teacher at another school that I married my friend while in Chicago. The next day, I received phone calls from people on the other side of the state that I hadn’t spoken with in months who were complaining because they weren’t invited to the wedding. [Which never happened.]

Example 2: Recently, Michigan Technological University President Curt Tompkins sent out a mass e-mail message to students at MTU about copyright and intellectual property violations. A student found that the letter Tompkins ‘wrote’ and signed his name to was identical to one sent at Penn State. Such a large number of students had written him overnight, he was forced to send a mass-apology instead of individual responses to the students.

These examples indicate that gossip can be effective in both broadcasting and routing messages in the physical world. It follows logically that the same event would occur in the electronic world.

Gossip is distinct from network flooding. Nodes have a probability that they will refuse to pass the message on. There is a great possibility of message exhaustion before it ever reaches its destination. [2] presents a protocol to ensure that the message survives until it reaches its destination, while reducing network congestion by 35% over flooding.

It achieves this by adding three values to the standard message header: probability of gossip, how many hops the message should travel before using the probability, and the minimum copies a node should receive of a message. The value for minimum copies is used to determine if the probability value should be used. If a node does not receive this minimum by the timeout, it will transmit the message to all of the neighbor nodes. If the value of messages received is greater than the minimum, it uses the probability to determine if it will transmit the node. The hop value broadcasts with a probability of one to all the nodes within the hop value of the source node. A node can only relay the message if the destination is routable from the gossiping node. This ensures that flooding does not occur. “Experiments show that we get the most significant performance improvement by taking [minimum copies] = 1” [2].

While this protocol delivers the message in a expedient manner, it can cause multiple copies of the same message to be transferred over the network, resulting in heavy bandwidth usage and congestion as shown in Figure 3.

D. Scalability of Other Common Protocols

[4] defines routing scalability as “the ability of a network to support the increase of its limiting parameters”. For their research, they determined that the largest limiting factor was network load and this resulted in determining that the best protocols varied based on situation.

Situation	Routing Protocol
No Routing	Plain Flooding
Reactive	Standard Link State
Proactive	Dynamic Source Routing
Hybrid	Zone Routing Protocol
Hierarchical	Hierarchical Link State
Limited Dissemination	Hazy Sighted Link State

TABLE I
SITUATIONAL ROUTING PROTOCOLS FROM [4]

This research indicates that the Hazy Sighted Link State scales best because it requires only maintaining a limited subset of the domain. As such there is a

significant decrease in the control overhead throughout the network, while able to maintain flexibility throughout node expansion or contraction. Other protocols discussed in Section III may be more efficient than the Hazy Sighted Link Protocol.

IV. RELIABILITY

Maintaining scalable and reliable network communication is essential to the success of Ad Hoc networking, in conjunction with maintaining a large availability radius. Reliability is key, as an unreliable Ad Hoc network will be of no more benefit than any preexisting solution.

A general consensus has been made that in order to ensure that packets are received by their destination, the recipient should be able to acknowledge receipt from the source node. There are two techniques suggested in [7]: Basic Access Method (also known as the two-way handshake method), and the Request-to-Send / Clear-to-Send Method (also known as the four-way handshake method). As the common Internet Protocols (TCP/IP), uses RTS / CTS, it is the preferred method to maintain reliability. Unfortunately, it causes network congestion and long delays in wireless networks because the path is reserved for the entire time a source is waiting for a positive ACK. As nodes roam, many timeouts may occur before the source located the desired node. The Basic Access Method allows for the acknowledgement to be sent along any available route to the source, resulting in BAM as the better choice for reliability assurance since it does not result in network congestion.

Quality of service methods of routing (discussed in Section III) also add greatly to network reliability.

V. CONCLUSION

Ad Hoc networks have great potential to be broadly used in making ubiquitous computing possible and successful. For this to occur, two things must happen. First, psychological changes must occur in the mindset of the network user. Ad Hoc networks work on basis that traffic can pass through any or all nodes on the network, in order to maintain a large availability radius. Many current WiFi users lock their base stations so others cannot utilize them. This defeats Ad Hoc availability and usefulness. Secondly, standardized protocols must be established to ensure that new nodes will be available to configure themselves and provide a broad level of services. As many of the cited papers discussed, usefulness of a protocol depends on network scale. As the vision of Ad Hoc networking is to provide a very large region with service, protocols should be chosen accordingly.

REFERENCES

- [1] A. Cerpa and D. Estrin, "ASCENT: Adaptive Self-Configuring Sensor Networks Topologies", IEEE InfoCom 2002 Proceedings, Volume 3, pp. 1278-1287, June 2002.
- [2] Z. J. Haas, J. Y. Halpern, and L. Li, "Gossip-Based Ad Hoc Routing", IEEE InfoCom 2002 Proceedings, Volume 3, pp. 1707-1716, June 2002.
- [3] D. Julian, M. Chiang, D. O'Neill, and S. Boyd, "QoS and Firmness Constrained Convex Optimization of Resource Allocation for Wireless Cellular and Ad Hoc Networks", IEEE InfoCom 2002 Proceedings, Volume 2, pp. 477-485, June 2002.
- [4] C. A. Santivanez, B. McDonald, I. Stavrakakis, and R. Ramanathan, "On the Scalability of Ad Hoc Routing Protocols", IEEE InfoCom 2002 Proceedings, Volume 3, pp. 1688-1697, June 2002.
- [5] P. Wan, K. M. Alzoubi, and O. Frieder, "Distributed Construction of Connected Dominating Set in Wireless Ad Hoc Networks", IEEE InfoCom 2002 Proceedings, Volume 3, pp. 1597-1604, June 2002.
- [6] J. Wang, and K. Nahrstedt, "Hop-by-Hop Routing Algorithms For Premium-Class Traffic in DiffServ Networks", IEEE InfoCom 2002 Proceedings, Volume 2, pp. 705-714, June 2002.
- [7] H. Wu, Y. Peng, K. Long, S. Cheng, and J. Ma, "Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysis and Enhancement", IEEE InfoCom 2002 Proceedings, Volume 2, pp. 599-607, June 2002.
- [8] W. Ye, J. Heidemann, and D. Estrin, "An Energy-Efficient MAC Protocol for Wireless Sensor Networks", IEEE InfoCom 2002 Proceedings, Volume 3, pp. 1567-1576, June 2002.
- [9] C. Zhu, and M. S. Corson, "QoS routing for mobile ad hoc networks", IEEE InfoCom 2002 Proceedings, Volume 2, pp. 958-967, June 2002.