Meshing Together: Advantages and Challenges of Deploying Ad Hoc Wireless Networks

Peter Stanforth & Vann Hasty, MeshNetworks Inc.

Ad hoc wireless networks were originally developed through Packet Radio experiments funded by the Department of Defense's Advanced Research Projects Agency (DARPA) more than 20 years ago, and have since been deployed with great success by the US military. This technology has recently become commercially viable and an extremely attractive solution to fulfill the ever growing demand for high bandwidth, low-cost wireless solutions. An *ad hoc* wireless - a.k.a. peer-to-peer wireless – system offers considerable advantages over more traditional wireless network architectures such as cellular or wireless local area networks (WLAN) but also poses different technical challenges. By providing a brief overview of *ad hoc* wireless technology we will examine some of the major advantages and challenges of deploying *ad hoc* wireless networks.

An *ad hoc* wireless network is a collection of mobile terminals (e.g. handheld devices, mobile phones, automotive telematics systems, etc.) that communicate directly with each other without the aid of established infrastructure (figure 1). Through multi-hop connections, the terminals act as routers/relays for each other and extend the range and coverage (figure 2) of communications between parties. Traditional wireless networks, such as cellular and WLAN, rely on single-hop architectures with the control residing in a centralized location and therefore no peer-to-peer communication. There are expectations that *ad hoc* wireless systems will require less power while providing higher capacity and robustness, without significant infrastructure investments. This leads to the belief that *ad hoc* wireless systems can be successfully deployed at a much lower cost than traditional wireless topology. However, wireless *ad hoc* networking is more complex than traditional wireless systems, and while it solves a number of traditional network shortcomings, it comes with its own set of technological challenges that must be solved.

Some industry cynics claim that *ad hoc* wireless networks will not scale, will not provide the required throughput, are not secure, and will deplete the batteries of all the host devices thus making the technology commercially unfeasible. Contrary to that viewpoint, a growing number of commercial companies are developing and deploying products based on *ad hoc* wireless technology, which is indicative that these issues can and will be successfully resolved. In addition to these companies pioneering the technology for commercial use, the Internet Engineering Task Force (IETF), through its Mobile IP and Mobile *Ad hoc* Networking (MANET) initiatives, is striving to standardize protocols and architecture solutions.

Taken individually, a case can be made for and against each claim. Performance of the technology in real life, however, will be dictated by the overall system architecture and mechanisms that balance these conflicts in the most efficient manner. The real attraction of a mesh topology is its ability to significantly improve the capability of any RF modulation scheme by:

- Requiring less power
- Having the ability to be rapidly deployed and reconfigured
- Providing better frequency reuse
- Not requiring Lines of Sight (LOS)
- Being able to load balance around congestion
- Providing redundancy to deal with failure
- Requiring less centralized infrastructure
- Providing capacity and scalability improvements

Reduction of power is achieved by choosing to transmit over two short distances versus one longer one. This translates into either a lower transmit power, or a higher data transmission speed. Either one will limit the total energy transmitted. This can be demonstrated simply with an 802.11b network by placing a node half way between a transmitting node and the AP. If the transmitting node is only able to maintain a 1mbit data rate directly, the 7dB of gain achieved by halving the transmit range results in the data rate improving to 11mbits. The result of these lower powered hops is that the devices achieve higher system throughput and create less interference into their environment (figure 3).

Because wireless ad hoc networking requires no infrastructure, the terminals must cooperate to organize into a network resolve contention for the available bandwidth and discover and maintain routes amongst themselves. These tasks become more complex as the number of nodes in the network grows. Without specific action being taken, the network will grind to a halt as the nodes spend all their time trying to figure this out. The challenges lie in both the media access and routing protocols.

Most *ad hoc* wireless networks use some form of Carrier Sense Multiple Access (CSMA) random access scheme, similar to the protocols defined by Apple for Appletalk and made wireless by early WLAN pioneers. These protocols have to be extended to deal with hidden node and exposed node problems (figure 4). When E tries to communicate with D it may not hear a concurrent attempt by C to talk to D. C is a hidden node to E. In contrast if node B wants to talk to node A, but hears a communication from C to D, B is may decide that the channel is busy and not attempt to send to A. B becomes an exposed node to C. These collisions, caused by the non-synchronized nature of the protocol create inefficiencies; if not managed, they can be so damaging that large networks choke.

Routing can be divided into proactive and reactive protocols. A proactive protocol keeps track of all the nodes so it has immediate access. A reactive protocol only finds a route to a node when it needs to. In general, proactive routing protocols are low latency, but not scalable. Reactive protocols are highly scalable, but have high latency. The goal of most research is to find ways to get the best of both worlds - low latency and high scalability - without the drawbacks.

The many new and existing applications for *ad hoc* wireless networks make it extremely promising. The technology's characteristic lack of infrastructure is very appealing to the military and for public safety first-responders, in addition to machine-to-machine communications such as sensor networks, process control pumps, and, in mobile environments, provides vehicle-to-vehicle communication for smart highways.

Ultimately, multi-hopping networks can exploit LOS improvements for last mile wireless solutions and to extend WLAN hotspots, and may in time become the true wireless Internet as a replacement for today's cellular systems.

Ad Hoc And 802.11

There are several companies today providing ad hoc self forming capability to 802.11 radio systems. Most are doing so within the confines of the current standard, implementing routing at layer 2.5 (below IP) or layer 3. There are however areas in which enhancements to the existing standards would make the addition of ad hoc routing much simpler, more efficient and more effective. These are discussed below.

There are demonstrable advantages to adding ad hoc routing to 802.11 networks though in some cases there are trade-offs to be made in order to exploit these advantages. The primary reason for the trade-offs is lack of definition or capability in the existing standards. This discussion will focus on two specific topologies of ad hoc networking applied to 802.11 networks in order to highlight the general advantages and issues. The first we will call "client meshing" the second "infrastructure meshing". Each is discussed individually but they can be used together.

Client meshing

In this topology every end point has the capability of being a source and sink for data as well as a relay/router for other devices. In a peer to peer mode of operation this is the only option available. (Figure 2). In this mode the range of the clients and robustness is extended by the ability to leverage one another to relay traffic to distant users. In one such example MeshNetworks created a network of 50 clients (industry standard PCMCIA 802.11b nic cards in an assortment of laptop computers) that could communicate over a distance of almost 5 miles.

When client meshing is employed along with APs the overall network coverage can be improved while at the same time providing significant capacity increases. The range improvement is easy to comprehend as a user does not have to have a LOS connection to the AP as long as it can communicate with someone who does. The capacity gains are a little more subtle. The first reaction of a user is to ask why they should share their nice 11mbit link with someone else. The inference being that their own throughput will be degraded by doing so. In fact the opposite is true. The AP is a shared resource and if I can help get someone else's packets through quicker then I free up more time for me to use it. Figure 5 shows a simple scenario where 1 user is close to the AP and able to communicate at 11mbits/sec where as the second user is only able to connect at a 1mbit data rate because of the distance from the AP. IF both users place a constant load on the AP the AP will max out at 1.1mbits/sec of throughput. This is because the distant user throttles back the closer user. Figure 6 repeats the test with the distant user hopping through the close user and the capacity of the AP goes up to 1.5mbits/sec a 35% increase[1]. This improvement is realized by the utilization of least energy and power control considerations in the routing algorithm. The amount of the increase will be somewhat dependent on the topology of the users, the fairness algorithms and the overhead of the routing protocol but we have seen between 15% and 40% in different scenarios.

There are several potential issues with client meshing today. First it is implied that all devices have the software drivers installed to enable ad hoc networking, and that a minimum number to obtain critical mass are available. MeshNetworks solves the latter with a concept we call a Wireless Router which is a device designed to seed a network but there is no easy answer for the former today. The second major issue is security. It is possible to utilize WEP with client meshing but the 802.11i standards for more sophisticated encryption and key distribution (AES WPA etc) are only defined for infrastructure mode so the potential for incompatibility is high. There is a less serious issue related to the battery consumption of a device like a laptop acting as a router/relay. It can be demonstrated that the same mechanism that improves throughput described above will also minimize the battery draw for all devices but additional criteria are needed to cover other circumstances. MeshNetworks utilizes a battery awareness constraint in it's routing but such a capability is not part of the current 802.11 standard.

Infrastructure meshing

In this mode only the access points are meshed. The major reasons for differentiating infrastructure meshing is to leverage ad hoc networking to reduce the backhaul costs. This is of particular interest to hotspot and outdoor deployments of 802.11 where backhaul may include a recurring fee to a telco, Figure 7. In this mode the clients talk directly to the AP as defined in the standard and can exploit all the currently defined security and mobility capability transparently. With the right RF technology this also allows APs to become mobile. The AP can use the same transceiver or a second transceiver to provide interconnection, relay and routing to other AP. The current Wireless distribution System (WDS) mode in 802.11 is a form of infrastructure meshing but as defined and used to date is very clumsy and decimates the performance. In figure 8 the when AP 1 Is relaying information to AP 2 it paralyses the entire access network. Infrastructure meshing only makes sense if the AP has at lease 2 transceivers. The second transceiver could be operating in the same frequency band on a different channel (both being 802.11b for instance) or more effectively in a different frequency. The ideal being to use different spectrum for access and backhaul. For instance 802.11a access and 802.11g backhaul to maximize capacity and range.

[1] This scenario was measured using Opnet with 802.11 and a DV routing algorithm as well as validated with a real 802.11 radio.

The disadvantages of infrastructure meshing are that it does not allow the capacity increases and robustness shown in client meshing and can, if improperly configured and deployed create substantial bottlenecks. It also increase the cost/complexity of the AP but given the recurring cost of a telco backhaul can be equivalent to the cost of the AP on a monthly basis the incremental cost is soon paid back.

Implications for the 802.11 standard.

There are many enhancements that can be made to the 802.11 standards to improve the capability and interoperability of ad hoc networks. Some are more contentious and challenging than others. The easiest place to start is to better define the interface between the MAC and the higher layers. Today mode implementations of 802.11 above the MAC are highly proprietary and integrating an ad hoc protocol is thus time consuming and expensive. There are a number of capabilities that are useful. The first is a standard definition and access to the radio link metrics. This is currently an activity of the 802.11k working group. This includes RSSI but also the number or retransmissions and amount of error correction done on a packet is also helpful to know. A standard way of controlling the power/data rate of the transmitter is also needed so that the option exists to multi hop at higher data rates than single hop at lower rates.

The next step is to extend the existing 802.11 standard MAC to allow information pertinent to ad hoc networking to be passed across the network efficiently. The key information is neighbor discovery, Identification of APs and the ability to support location awareness. These would provide common basic building blocks for the ad hoc routing protocols.

Finally, and most contentious, is the standardization of a layer 2.5 or layer 3 ad hoc routing protocol. This will not be easy. There are as many protocol proposals as there are companies building solutions. The primary reason is that there is not a single protocol that is ideally suited for all situations. Protocols loosely fall into two groups which, in a very generalized way, are proactive meaning they are good for real-time communication with low latency, or reactive which means they can scale but have too much latency for real time applications and mobile applications. The solution is probably to define an interworking capability so that different protocols can co-exist and hopefully interact in an efficient manner with each other.

Recommendations and Lessons Learned

Feedback from MAC/LLC to Routing implementation

- Immediate feedback of the TX and Rx status of packets received is critical in developing a reliable ad-hoc routing network. This status data is typically available in some form from the MAC layer implementations of 802.11 hardware, but is seldom available outside of the scope of the link layer. In Layer 2 routing implementations based in or immediately above the link layer this information can be passed directly. In layer 3 implementations the cost of reporting per-packet information up to the network layer of a protocol stack may be computationally or architecturally prohibitive. In that case a cumulative derivative value can be computed in a small module collocated near the MAC. This value can then be reported to the routing layer on a less frequent per-destination basis. Most current driver/stack combinations do not pass this information up in the stack.

- Mac layer acknowledgements for transmitted directed packets must be reported to some agent of the routing implementations. This is necessary to determine the status of links in the multi-hop network.
- Some normalized measure of signal quality or S/N ratio of received packets must be reported on a per packet basis to some agent of the routing implementation.
- Management packets should be made available to some agent of the routing implementation so they can be used to inform the routing of status of individual neighboring stations.

Feedback from the PHY

- A normalized measure of the number of corrected bit errors on a received per-packet should be made available to some agent of the routing implementation. This can be used to predict degrading links in the network and proactively switch routes.

MAC Layer Management Entity control from the routing implementation

- Fine-grained control of the data rate selection on a per-packet basis is necessary to select routes with the highest end-to-end throughput rates. Most current data rate selection algorithms implemented heavily favors the star topology of infrastructure networks.
- Transmit power control on a per-packet basis is necessary to optimize frequency reuse.

Basic MAC functionality

- Group traffic should not be limited to the basic supported data rates for the ad-hoc network in order to optimize frequency reuse and quickly establish the bi-directionality of links between neighbors at data rates above the available basic rate set. This is especially important for routing networks that build and distribute topology information in/from group frames.
- Power saving mode needs some work to remove the timing hazards possible at exposed nodes in networks without full 1 hop connectivity.

Security in ad-hoc

- Need I say more?

Location Based Services (LBS)

- Location based services need something more robust than an RSSI measurement as this is too easily attenuated. In order to use a Time Of Flight/Time Of Arrival (TOF/TOA) technique the timing becomes critical to the accuracy. This can be coordinated to some extent in a infrastructure mode where all the radios can be synchronized but in an ad hoc mode without coordinated synchronization some form of ranging ping is required. In this case the accuracy is determined by how deterministic the turn around time at the receiving node is.

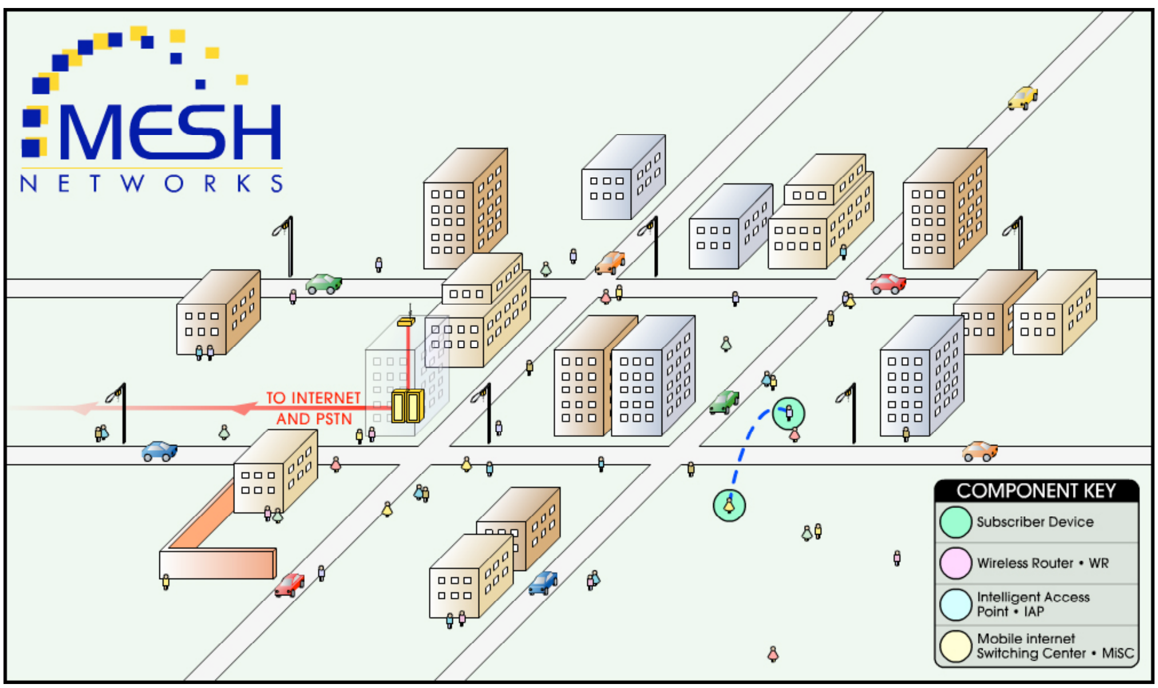


Figure 1

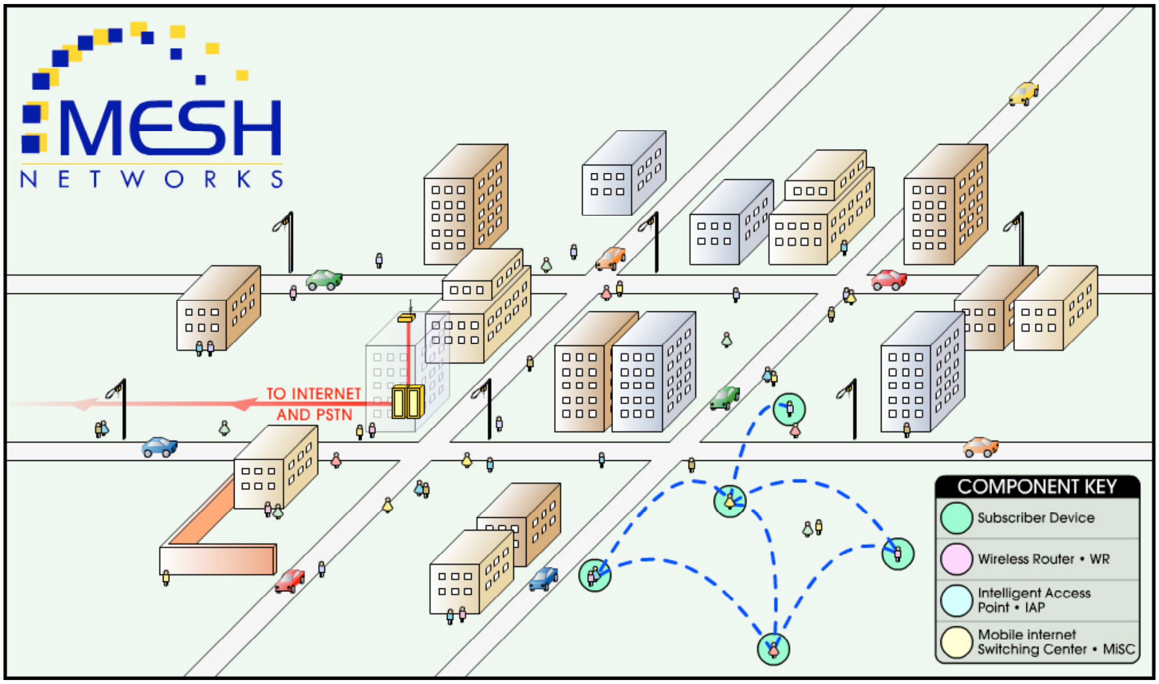


Figure 2

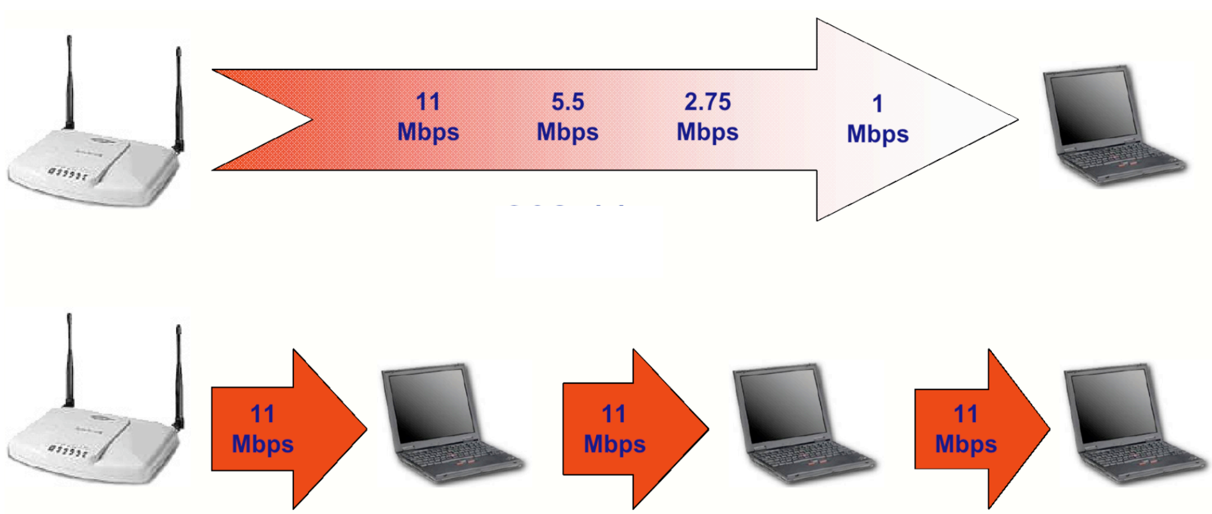
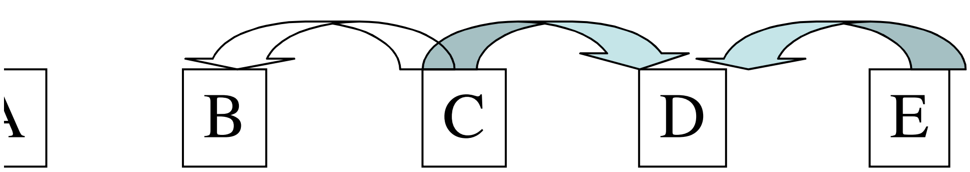


Figure 3

Figure 4



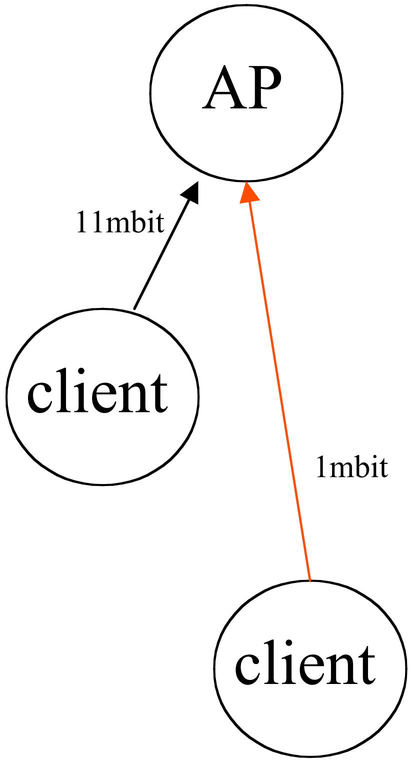


Figure 5

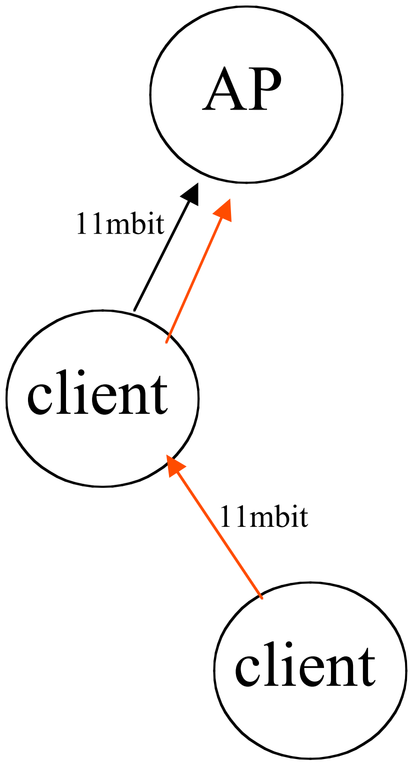


Figure 6

Figure 7

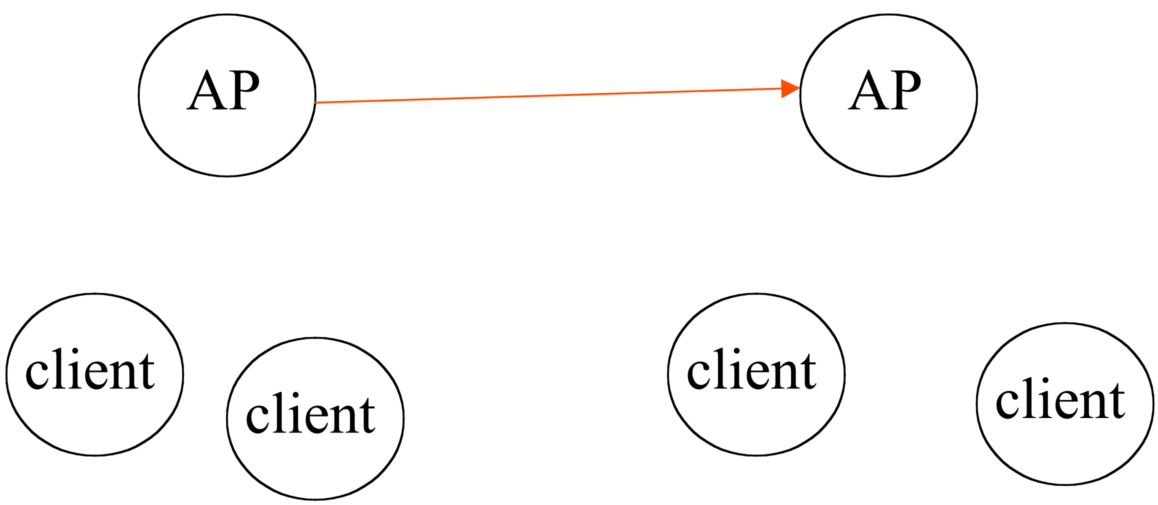


Figure 8

References

[1] DESIGN CHALLENGES FOR ENERGY-CONSTRAINED
AD HOC WIRELESS NETWORKS
Andrea J. Goldsmith, Stanford University
Stephen B. Wicker, Cornell University
IEEE wireless Communications August 2002

[2] A CHANNEL ACCESS SCHEME FOR LARGE DENSE PACKET RADIO NETWORKS
Timothy J. Sheppard, BBN
IEEE Communications August 1996

[3]
Timothy J. Shepard_
BBN Systems and Technologies
A Channel Access Scheme for Large Dense Packet Radio Networks
Timothy J. Shepard
A Channel Access Scheme for Large Dense Packet Radio Networks
Timothy J. Shepard
A Channel Access Scheme for Large Dense Packet Radio Networks
Timothy J. Shepard_
A Channel Access Scheme for Large Dense Packet Radio Networks