Mesh Networking
Research and Technology
for Multihop Wireless Networks

Mesh networking refers to a broad class of wireless networks in which nodes collaboratively route packets. Meshes can be ad hoc, in which nodes must route to one another with no dedicated infrastructure; they can also act as edge networks to a larger network infrastructure, such as the Internet, letting wireless nodes route through one another for complete IP connectivity. Although mesh nodes are often stationary, they can also be mobile. Combined with wireless communication’s inherent dynamics, these variations imply that, in mesh networking, the network must automatically adapt and self-configure. Mesh nodes must therefore automatically discover each other and identify the best routes to other nodes and networks. This issue presents a series of articles describing the advantages and challenges of mesh networking, as well as application studies of the technology.

Why Mesh Networking?
One possible alternative to mesh networks are cellular networks, which currently provide data coverage in much of the world. Unfortunately, they aren’t always an ideal solution. First, cellular is expensive, and most cellular providers charge tens of dollars per month per node for data service. (Short messaging service is even more expensive—sending an SMS costs more per bit than sending a similar amount of data to the Hubble telescope!) Second, due to complexities inherent in long-range data transmission, wide-area cellular is likely to always be at a bandwidth disadvantage when compared to local-area wireless.

Third, because mobile telephony operates in licensed spectrum and uses complex, expensive systems, end users can’t provide or improve coverage. In contrast, anyone can deploy unlicensed wireless, such as Wi-Fi and WiMAX. Economies of scale have made Wi-Fi an attractive starting point for many situations that its original design didn’t consider, such as 200-km point-to-point links that provide connectivity to remote areas. Laying down a cable over such a distance is prohibitively expensive, and in rural areas, the danger of someone accidentally digging and cut-
ting the cable is very real. A wireless link, in comparison, simply requires an Internet connection on one end and maintenance at both end points. In some cases, that Internet connection can even be to a cellular network.

All the benefits of mesh networks — lower costs, scalability, and easy installation — introduce new challenges. Unlike wired media, in which signal interference from the surrounding environment is limited by shielded cables, wireless media is vulnerable to many external effects. Stand between a Wi-Fi device and its base station, and the signal strength will drop significantly. Wireless communication quality degrades with distance, often irregularly. In practice, these two effects mean that simple, single-hop wireless networks have limited reach. For wireless to reach beyond tightly controlled environments, such as office buildings, meshes offer an attractive solution because they let networks adapt to changing conditions, extend beyond single wired access points, and route around failures.

Mesh Networking Applications

The simplest examples of meshes involve a few 802.11 repeaters extending wireless access in homes. More sophisticated examples of 802.11 meshes include the municipal area networks that cover some cities; these networks use hundreds of access points (APs), only some of which have Internet connectivity. Clients connect to nearby APs, which might in turn send data directly to the Internet or route through another AP if Internet connectivity isn’t available. Examples of companies selling such products include Tropos Networks and Meraki Networks. These meshes extend an Internet AP’s reach, providing connectivity to urban as well as rural areas.

Sensor networks also depend on wireless meshes. The typical sensor networking application involves several small, wireless, battery-powered sensing nodes, which collect and report information about remote environments. For example, a group of researchers in Switzerland recently deployed numerous such nodes in the Swiss Alps for avalanche detection and to study global warming’s effects on permafrost (http://sensorscope.epfl.ch).

These nodes measure temperature, wind speed, solar radiation, humidity, and other environmental parameters. They relay this data through a mesh to a gateway that connects to a cellular network. Mesh networking eliminates the need for expensive, power-hungry cellular service on each node and makes it possible to easily and quickly integrate new nodes into existing networks.

Mesh Networking Challenges

A future in which wireless dominates networking at the edge raises a range of problems other than just providing connectivity. Security is one example. Unlike a wired network, in which snooping on data requires physical access to the medium (through a compromised host, for instance), anyone close enough can overhear wireless.

Power is another challenge. One of wireless’s advantages is that devices no longer need to be tethered to a networking infrastructure; this also means that low-power devices are untethered from the power infrastructure as well. Such low-power wireless applications are typically more concerned with conserving energy than with throughput or performance, resulting in deep implications to wireless protocol design.

In this Issue

This issue of IC contains four articles that provide an excellent introduction to some of the challenges, issues, and ideas that mesh networking researchers examine today.

“The Rise of People-Centric Sensing,” by Andrew T. Campbell and his colleagues, describes a new class of computing services that ubiquitous wireless could enable. Mobile, personal devices, such as phones, can provide dense real-time sensor data. Public services, social networks, and virtual environments could then use these data streams to enhance services, ranging from avoiding traffic to learning your friend is nearby.

The second article, “Deploying Rural Community Wireless Mesh Networks,” by Johnathan Ishmael and his colleagues, starts by observing that rural areas often don’t have the same high-speed network access that’s available in urban areas. Given that access to information has a significant economic benefit, this divide can have long-term social and societal implications. The authors report on their experiences deploying a wireless mesh in a rural English village that lets most of the village share the school’s high-speed radio link. They describe how network use evolved after installation as users took advantage of the greater capacity,
and they touch on the problems and challenges of maintaining such a network.

In “Securing Wireless Mesh Networks,” Steve Glass, Marius Portmann, and Vallipuram Muthukumarasamy provide an overview of the many security challenges that wireless meshes face. 802.11s is a standards effort within the IEEE to amend Wi-Fi to better support mesh networking. The article describes many attacks mesh routing can suffer from, such as routing attacks, rushing attacks, black holes, and wormholes. Many of these attacks stem from the fact that we can’t secure the wireless channel itself.

The final article, “Extending IP to Low-Power Wireless Personal Area Networks,” by Jonathan Hui and David Culler, looks at how tiny, embedded wireless devices will interoperate and communicate. Embedded systems today are often vertically integrated with proprietary protocols and services; the authors describe the effort within the IETF to extend IP to these devices while addressing their harsh energy, RAM, and networking constraints.

Together, these four articles should give you a glimpse into the huge research and engineering effort going into wireless and mesh networking today. These technologies promise a future in which it’s possible to cover increasingly remote and expansive locations with always-on wireless connectivity.

Samuel Madden is an associate professor of electrical engineering and computer science at the Massachusetts Institute of Technology’s Computer Science and Artificial Intelligence Laboratory. His research interests include databases, sensor networks, and mobile computing. Madden has a PhD in computer science from the University of California, Berkeley. Contact him at madden@csail.mit.edu.

Philip Levis is an assistant professor of computer science and electrical engineering at Stanford University. His research interests include low-power computing, wireless networking, and sensor networks. Levis has a PhD in computer science from the University of California, Berkeley. Contact him at pal@cs.stanford.edu.