WI-FI vs. INTERNET OF THINGS

WI-FI IS THE INVISIBLE WORKHORSE of modern life. But Wi-Fi is struggling. And the next phase of the Internet—the Internet of Things—could break it.

Startups and Internet service providers are developing an application layer that divorces some functions from the base networking standard, IEEE 802.11. Many new features sprouting up within this layer—such as mesh networks (a set of routers that work together to extend wireless coverage) and provisioning tactics (which define how wireless devices connect to networks)—have been developed in response to the Internet of Things.

It reminds me of the Zigbee mesh-network specification for small, low-power digital radios, which has layers for specific classes of devices built on top of the radio. This has sowed confusion among customers about which Zigbee devices actually work with one another. I fear that Wi-Fi is heading in the same direction.

Consider a mesh Wi-Fi system. Companies including Eero, Google, and Securifi have created products that promise reliable coverage throughout every square centimeter of a home. But this works only if you buy all of your mesh routers from the same vendor.

Companies soon realized they could pop a network-based security product into mesh routers and add the ability to prioritize devices. But where does an application layer end and the core Wi-Fi standard begin?

Comcast Corp. offers a good case study. In 2017, it revamped its Wi-Fi products, layering on services such as parental controls. Comcast implemented software from a startup called Cirrent to make it easier to provision, or add, a device to your network. Cirrent’s software sits on Comcast routers and also lives on a variety of consumer devices from Bose, Electrolux, and others.

When a product with Cirrent’s software comes into a Comcast home, it automatically connects to the Wi-Fi network. But Cirrent’s solution is implemented piecemeal by vendors. And if you don’t have Cirrent’s software on your router, your Electrolux washer may not connect.

Applications like Cirrent’s do solve common Wi-Fi problems, but they also lock users into certain chip vendors, router makers, and service providers.

“If you want to think of it as an application layer on top of the standard, as an economic matter, it makes sense,” says Fahri Diner, CEO of the startup Plume.

Plume’s own software improves coverage by tweaking the capacity on routers around the home. Comcast uses it, and Plume has signed deals with companies, including Samsung, to turn their devices into mesh routers that run its software.

Diner is working with major Wi-Fi chip vendors to ensure compatibility, and he is open-sourcing some of the necessary code. But if not every vendor uses it, Plume’s dynamic network optimization won’t operate on an incompatible router.

The only solution to fragmentation will be at the Wi-Fi Alliance, which certifies Wi-Fi devices. Brian Bedrosian, vice president of marketing for IoT at Cypress Semiconductor Corp., says simpler provisioning and neighbor-aware networks (which let devices speak to one another without a Wi-Fi access point) must become part of the Wi-Fi certification specification.

“By comparison, it could be like the Zigbee spec, which has been a disaster,” he says. Hopefully, the Wi-Fi Alliance won’t let that happen.