

Superstorm Sandy Reveals Wireless Network Vulnerabilities

Elliott Drucker

“Superstorm” Sandy, the latest natural disaster to hit the U. S., impacted a very large geographical area that comprises some of the most densely populated regions



Elliott Drucker

in the country. Amid stories of tragic loss of life and staggering property and infrastructure damage we also learned that in many hard-hit areas wireless networks suffered widespread outages, some lasting for several days.

We have seen this scenario play out before. When Hurricane Katrina devastated New Orleans in 2005 cell phone service in much of that city was essentially non-existent for days. In 2003, a blackout that struck much of the northeastern U.S. resulted in outages that affected tens of millions. What is new with Sandy, however, is that a substantial portion of the population now relies solely on wireless for at least basic (voice and text) communications, and many count on wireless broadband networks for email and Internet access. This is important because the scope of outages caused by Sandy were substantially greater for wireless networks than for traditional wireline services.

This apparently greater vulnerability of wireless networks, which also occurred in Katrina, seems to defy logic. After all, unlike telephone lines the physical medium connecting users to wireless networks, the radio channel, is—at least at the frequencies used for commercial networks—immune to flooding, falling trees, and other calamities associated with these sorts of disasters. So why are wireless networks comparatively fragile, and what can be done to make them more robust? The “why” part is actually pretty easy to understand. Figuring out what to do about it is a much more complex problem.

Radio base stations are by far a cellular network’s biggest vulnerability. The public often refers to these as “cell towers” even though in urban areas most are located on the tops or sides of existing structures rather than on dedicated towers. In a nasty storm, individual base stations can fail due to direct physical damage. Antennas can be struck by lightning or blown off their moorings, and base station electronics located at or below ground level can be flooded. Such failures probably contributed a bit to the service outages related to Sandy and Katrina, but in the

Superstorm Sandy Reveals Wireless Network Vulnerabilities

Published on Wireless Week (<http://www.wirelessweek.com>)

vast majority of cases the base stations that went out of service were completely undamaged. Instead, the two main culprits were backhaul failure and loss of AC power.

In modern urban wireless networks, particularly in the U. S., most radio station backhaul is cobbled together using a combination of leased wireline digital circuits, dedicated fiberoptic facilities, and microwave links. The wire and fiber portions of backhaul facilities are subject to the same sorts of disruptions as conventional telephone networks, but for various reasons seem to be much more vulnerable. Part of this disparity may be caused by wireline network operators who, faced with widespread damage, are understandably more focused on restoring service to their regular customers than to the cellular networks to whom they lease digital facilities. The good news here is the recent emergence of competitive dedicated backhaul networks. Unlike traditional local exchange carriers, dedicated backhaul providers can optimize their networks, and their disaster recovery systems, to the needs of wireless operators who are their primary customers.

Another relatively recent enhancement to backhaul reliability is provided by the re-emergence of microwave as a major component. Properly configured microwave links, including redundant electronics and robust backup power systems, can be “disaster hardened” fairly easily. What’s more, microwave lends itself to relatively simple provision of path-redundant “loops” that allow continuation of service even after a single-point failure.

But even if backhaul remains connected, most base stations will eventually go out of service after losing AC power. Widespread power failure is a hallmark of most natural disasters, so correspondingly widespread wireless service outage will predictably follow. It won’t happen immediately because many base stations have at least some backup power system, usually in the form of batteries. But due to economic constraints, the battery system installed in a typical urban “macrocell” is only good for a few hours of service.

It is now pretty clear that loss of power was the main cause of wireless service outages in the aftermath of Sandy. The same was true for Katrina, which then led the FCC to push for new regulations requiring wireless network operators to equip their base stations with a minimum level of backup power. The operators successfully pushed back, and the FCC ultimately relented. I would not be surprised, however, if the issue is revisited after Sandy.

One way to improve overall network reliability is to equip at least some “critical” base stations with generators that can provide backup power indefinitely – as long as they have fuel. Unfortunately, as demonstrated by Katrina and more recently by Sandy, timely refueling of large numbers of power generators spread out over a metro area can be a real problem when surface transportation is severely disrupted. What’s worse, backup generators and their fuel systems are usually located at or below ground level, where they are vulnerable to flooding.

A more practical and effective approach to base station power backup may be provided by a combination of improving battery technology, driven largely by the

Superstorm Sandy Reveals Wireless Network Vulnerabilities

Published on Wireless Week (<http://www.wirelessweek.com>)

push towards hybrid and all electric vehicles, and application of service constraints. In terms of both weight and volume, the latest lithium polymer battery technology delivers about five or six times the energy storage density of the lead acid cells still in widespread use for base station backup power. This suggests that a “standard” backup endurance of, say, 24 hours should be quite practical today, with promises of further improvement as battery technology evolves.

That’s good, of course, but if wireless networks are to match the level of “disaster-proofing” provided by traditional wireline services, base station backup power endurance will probably have to be measured in days rather than hours. I suspect that the best way – perhaps the only way – to achieve this is by constraining levels of service and thus reducing base station power consumption.

Here’s how such a service constraint system could work. A network administrator might invoke power conservation for affected base stations when a widespread power outage is expected to continue for more than a few hours. Reduction of power consumption could be achieved in a number of ways. For example, a base station might limit the maximum forward channel power transmitted to any particular user device. This could significantly reduce the power required for what are typically the base station’s biggest power hogs, its linear power amplifiers. There would be some loss of indoor coverage reliability but no significant reduction in communications capacity. Alternatively, or in addition, the number of channels or amount of bandwidth provided by the base station could be reduced, perhaps accompanied by restrictions on per-user usage. Just putting clamps on bandwidth-hog applications like streaming video would probably allow broadband networks to offer acceptable quality of service despite significantly reduced throughput capacity.

For better or worse, a natural disaster has once again demonstrated just how vulnerable today’s wireless networks are to the effects of natural and man-made disasters, particularly widespread and long-lasting power outages. One way or another—social pressure, government regulation, or simple competition—operators may be forced to deal with the problem. It’s an area ripe for innovation, something that the wireless industry is very good at.

Source URL (retrieved on 06/11/2013 - 4:17pm):

<http://www.wirelessweek.com/articles/2012/12/superstorm-sandy-reveals-wireless-network-vulnerabilities>