IoT News Roundup

White House Announces Funds for Raft of Smart-City Projects

Last week, the Obama Administration announced a wide-ranging list of smart-city research initiatives with $160 million in funding (a mix of new spending, grants and proposed investments) and 25 new technology collaborations aimed at helping communities improve traffic flow, reduce crime, conserve energy and improve city services. The initiatives

will include creating Internet of Things testbeds and forming partnerships across government, private and academic entities.

The National Science Foundation (NSF) is providing a $35 million grant, with funding spread across nine projects with a range of objectives, including bolstering cyber security and improving public health and safety. One grant recipient, US Ignite, a public-private partnership that has been fostering IoT-based smart-city applications since 2012, will launch projects in 15 U.S. communities with 1-gigabit-per-second Internet service, in an effort to leverage those robust infrastructures to evaluate smart-city applications.

The NSF will also award $3 million to the University of Chicago in order to grow the Array of Things project, on which the university is working with Argonne National Laboratory and a long list of technology providers to collect real-time data regarding the city's environment, infrastructure and activity, for both research and public use.

The U.S. Homeland Security and Transportation departments, as well as the Environmental Protection Agency, are undertaking smart-city projects as part of this large initiative as well.

NB-LTE Wins Standardization Nod

IoT network nodes are often widely deployed in remote areas and in large numbers. They do not transmit large payloads of data, but they enable devices to transmit information over great distances, and while consuming as little battery power as possible. This week, the 3rd Generation Partnership Project (3GPP), a consortium of telecommunications standards bodies, decided to standardize Narrow Band Long-Term Evolution (NB-LTE) technology, which is a variant of LTE cellular technology optimized to meet the performance requirements of IoT nodes. The term "narrow band" refers to the use of a narrow slice of the cellular radio spectrum to transmit short packets of data to and from a large number of devices deployed across a large

area.

The standard focuses specifically on connected devices used for IoT applications, which require that devices consume little power and that communication modules be low-cost. Cellular carriers are phasing out support for 2G cellular networks, which many legacy cellular-based IoT networks use. Those end users will need to upgrade to NB-LTE chipsets, but would continue to leverage cellular networks, which are available globally.

Chipmaker Intel says it plans to offer NB-LTE chipsets and product upgrades beginning in 2016, while Nokia and Ericsson announced plans to support NB-LTE on their respective broadband infrastructures.

“NB-LTE targets lower device complexity and cost, as well as a [long transmission distance] for existing LTE networks, so [NB-LTE nodes] would be reachable even if they are, say, inside a basement,” says Kai Sahala, Nokia’s head of product marketing for mobile broadband. “And it will improve [device] battery life to up to 10 years.”

NB-LTE is one of a handful of competing long-range, low-power data-transmission technologies that leverage different parts of the radio spectrum and various networking technologies and infrastructures.

CUJO Wants to Be Home IoT Guard Dog

A California IoT security startup called CUJO has raised nearly $120,000 in 11 days via an Indiegogo campaign, blowing past its $30,000 goal to raise sufficient funds to manufacture an IoT home-security device. The CUJO plugs into a home’s Wi-Fi router via Ethernet and inspects inbound and outbound data, searching for malware, viruses, phishing attacks and other indications that hackers may be attempting to elicit data-sharing from IoT devices. These include security cameras and baby monitors, as well computers and smartphones, connected to

the home’s network.

The device will perform packet inspection locally, and will link to CUJO’s cloud-based servers for updates regarding malware and phishing threats. The company will also offer homeowners an app, available for iOS or Android devices, through which it will alert them if it detects a security threat on their home network.

Through the campaign, the device is being offered for $49 with six free months of service, after which users will pay an $8.99 monthly or $89 annual subscription fee. According to CUJO, the subscription will ensure that users receive ongoing security updates via its cloud-based host. The company says CUJO is not meant to replace anti-virus software on home computers.

ABOUTCAREERSAUTHORIZED SERVICE PROVIDERSYour Privacy ChoicesTERMS OF USEPRIVACY POLICY