Engineers designing system so cellphones, laptops, other wireless devices can help nab radio-frequency thieves

July 19 2016

University of Utah School of Computing professor Sneha Kumar Kasera and his team of researchers are tasked with creating a crowdsourcing system that allows cellphone and laptop users to help detect and locate someone who is stealing bandwidth on radio frequency waves. The team has received a three-year, $1-million grant from the National Science Foundation (NSF) to devise the system to help tighten security of the nation's radio spectrum, a valuable resource

used for satellite communication and for commercial, public safety and military applications. Credit: Dan Hixson/University of Utah College of Engineering

We crowdsource for business startups, art projects, inventions, even families in need. So why not ask cellphone users to contribute in helping catch high-tech thieves?

University of Utah School of Computing professor Sneha Kumar Kasera and his team of researchers are tasked with creating a system that allows cellphone and laptop users to help detect and locate someone who is stealing bandwidth on radio frequency waves. The team has received a three-year, $1-million grant from the National Science Foundation (NSF) to devise the system to help tighten security of the nation's radio spectrum, a valuable resource used for satellite communication and for commercial, public safety and military applications.

Kasera's grant aligns with the Advanced Wireless Research Initiative announced July 15 by the White House and led by NSF. The initiative researches new wireless technologies, applications and services to make wireless communication faster, more responsive and more robust. NSF also announced it will invest more than $400 million in support of this initiative over the next seven years, according to NSF Program Director Thyaga Nandagopal.

"Fundamental research on advanced wireless will be transformative and take us beyond the current and next generation of wireless—beyond what has been envisioned thus far" said Jim Kurose, head of Computer and Information Science and Engineering at NSF.

The problem of stealing radio frequencies for private use—what Kasera calls "unauthorized spectrum use"—is expected to become much more

serious when more cellphones, laptops and other mobile devices utilize what's called "software-defined radio" technology, a fast-rising technology in which you can change the functions of a radio device by simply updating its software instead of making more costly hardware changes.

Once more devices turn to this technology for better flexibility, it is likely that hackers then will use it to create software to steal radio bandwidth, or worse, create malware for phones and computers meant to disrupt radio and satellite communications. For example, imagine terrorists using malware to attack software-defined radios that clog up emergency-services radio frequencies in the time of a crisis.

"It's not fully understood yet as to what scale this problem currently exists. But this is in anticipation that with more software-defined radios this will become a much bigger problem," says Kasera. "Once you have that software-defined radio capability, hackers will write all kinds of bad apps for them."

Kasera has come up with the idea that everyday users of cellphones and laptops could aid authorities in catching these kinds of hackers. He is researching a system in which people could download an app or piece of software for their devices that can detect if an unauthorized radio frequency is being used and where the offender might be located.

All devices with built-in radios can receive signals within a certain frequency range. When someone with a phone or laptop briefly runs Kasera's software, it could tell authorities if a hacker is using unauthorized bandwidth of a certain frequency range and at what strength it's being transmitted. If enough people in the area are simultaneously running the program, the system also could help locate the thief by triangulating the signal.

Currently, the Federal Communications Commission has an enforcement bureau that detects unauthorized use of radio frequencies whenever it receives complaints, Kasera says, but it's an arduous manual process, and they do not have enough resources to cover all areas.

"We thought that there should be a better way of doing this, and then we started thinking of ideas about crowdsourcing," he says. "Our goal is to be able to monitor for unauthorized use 100 percent of the time, cover 100 percent of the area and cover 100 percent of the frequency, and that can only be achieved at that scale through crowdsourcing."

Kasera's co-researchers include University of Utah electrical and computer engineering associate professor Neal Patwari; School of Computing assistant professor Jeff M. Phillips; researcher Kurt Derr with the Idaho National Laboratory; and Milind Buddhikot, distinguished member of technical staff with Nokia Bell Labs in New Jersey.

Provided by University of Utah