'Eye in the sky' will bypass Internet traffic jams

October 27 2014, by Bill Steele

When you're driving to work you wish you knew where the traffic jams will be. The same is true on the Internet, but network operators today can't observe or control the paths that carry data beyond the borders of their own networks. For end users this sometimes means poor performance and service outages.

A team of researchers at Cornell, the University of Southern California (USC) and University of Massachusetts has an answer: An electronic "eye in the sky" that can look down on the whole system and gather the information operators need. Their project is funded by a $3 million grant from the National Science Foundation.

"There aretens of thousands of domains on the Internet, and they all have their own objectives. It becomes a little adversarial," said Nate Foster, assistant professor of computer science, a principal investigator on the grant. "How can we use the [tools] that the Internet gives us today to observe and control and give better information to operators?"

Their proposed application, called IN-CONTROL (Programmable Inter-Domain Observation and Control) will collect information from participating networks into a database that network operators can query to find the best routes for their data. It will help operators select the best paths, relay around faults or avoid untrustworthy networks. The database will be distributed in many locations across the Internet for security and scalability.

Such "knowledge planes" have been proposed before, the researchers said, but all previous proposals have required extensive upgrades to network hardware. IN-CONTROL will work with the tools that are already available in Internet routers today. It will build on ideas from Frenetic, a programming language developed by Foster that allows network programmers to write commands for what they want routers and other devices to do without having to understand the details of the hardware. Programmable devices are becoming increasingly common as older equipment is replaced, Foster noted.

Many network operators prohibit releasing details about how their systems are organized. To encourage these operators to participate, the researchers plan to incorporate security mechanisms that will keep the detailed architecture of a network from being exposed. In effect, users will be able to find the best route through town without seeing a map. There also will be safeguards to prevent malicious users from adding false information. A domain might advertise: "We have a faster route; send your data through here," and then spy on the data coming through, Foster explained. To bootstrap the system, the preliminary database will be assembled using the system's own probes that gather basic information about forwarding paths.

Network operators will support the plan, the researchers said, in return for improved performance. Amazon, for example, has reported that every additional 10 milliseconds of delay in loading a page reduces their sales by 1 percent.

Provided by Cornell University