Secure, synchronized, social TV

April 1 2011, by Larry Hardesty

Research Laboratory of Electronics researchers Muriel Médard and Marie-José Montpetit (inset), in a simulation of the type of video chat that could benefit from network coding. Graphic: Christine Daniloff

Network coding is an innovative new approach to network design that promises much more efficient use of bandwidth, and MIT researchers have made seminal contributions to its development. But in recent work, some of those researchers have concentrated on a different application of the same technology: secure communication. Media companies have shown interest in the new work as a means of simultaneously protecting their content and their customers' privacy.

In an ordinary network, such as the Internet or the cellular network, packets of data are relayed from source to destination by a series of special-purpose devices called routers. The routers read the destinations of the packets but leave them otherwise undisturbed. With network

coding, however, the contents of different packets are mixed together. Given enough information about how the mixing was done, a computer at the receiving end can separate the data back out again. Because each hybrid packet in some sense represents the contents of more than one regular packet, the method can end up saving bandwidth. In experiments conducted at MIT, network coding was able to consistently increase the data capacity of a wireless network to about three times what it was initially.

Until the hybrid packets are decoded, however, they're total gibberish, and without some basic information about how they were produced, decoding them is next to impossible. So while network coding offers a more efficient use of bandwidth, it also offers an efficient means of securing information.

In a pair of papers last year in the *IEEE Journal of Selected Areas in Communications*, Muriel Médard, a professor in MIT's Research Laboratory of Electronics, members of João Barros's group at Portugal's University of Porto and researchers at the Spanish telecom company Telefónica set out the theoretical basis for a system that would use network coding for secure communications. NBC expressed interest in the technology as a way to protect content disseminated over the Internet, and in March, Médard; Marie-José Montpetit, a research scientist at RLE; Frank Fitzek, an associate professor of engineering at Denmark's University of Aalborg; and students from both groups went to New York City to demonstrate the technology at 30 Rockefeller Plaza.The virtual living room

The demo was meant to illustrate the application of network coding to what has recently been called social TV. With the proliferation of smart phones and tablet computers with high-resolution screens, people are increasingly streaming television programs over the Internet. At the same time, friends watching conventional television programming in different

places are texting and instant-messaging each other with their spontaneous reactions to events on-screen. Social TV anticipates the convergence of these two trends, as friends coordinate times to watch the same streaming video on different types of devices, in different locations, while exchanging commentary.

So conceived, social TV poses a number of technical challenges. One is the allocation of bandwidth, as AT&T discovered when the popularity of streaming video on the original iPhone threatened to overwhelm its network. Another is the synchronization of video streaming to different devices. And a third is the protection of both providers' content and the privacy of consumers' comments. Médard and Montpetit believe that network coding can help with all three.

In the demo at NBC, a small group of people watched the same streaming video on handheld devices. Only one of the devices, however, was connected to the cellular network. It broadcast hybrid data packets to the other devices, which in turn mixed them together and passed them along. So network coding reduced the burden on the cell network. And since all the devices were broadcasting data to each other, and the researchers' algorithms were able to descramble coded packets so efficiently that the synchronization between the devices was nearly perfect.

Security as service

To demonstrate the use of network coding for secure communication, the demo simulated a case in which most of the users were authorized subscribers to NBC content but a couple were not. The unauthorized devices still participated in the coding, hybridizing packets and broadcasting them to their neighbors. But because they weren't initially given the information essential to decoding the packets, they wouldn't have been able to pirate the content. If the unauthorized users agreed to

watch a short advertisement video, however, the decoding keys were delivered to their devices.

Although secure messaging between devices was not a feature of the demo, Médard and Montpetit say that it would use the same technology that content protection does and that they and Fitzek have begun to add it to their system. “The idea is that secure communication becomes another network service,” Montpetit explains. The security of transmissions is an intrinsic feature of the way data packets are hybridized and disseminated. Controlling access is simply a matter of sending users the keys that unlock the data they’re authorized to read.

Sheau Ng, the head of technology R&D at NBCUniversal, says that the technology the researchers demonstrated could have applications in cases in which, for example, several family members in a single location were using separate devices to teleconference simultaneously with a distant relative. But, he says, “That’s not as interesting a scenario as the one where users are in entirely different parts of the physical world.” He believes, however, that network coding is applicable in that case as well. “It’s a multiyear project, and we are just now in the first stages of it,” he says. “We’re quite excited about seeing what the team can come up with.”

Montpetit concurs. “Stay tuned,” she says.

Provided by Massachusetts Institute of Technology