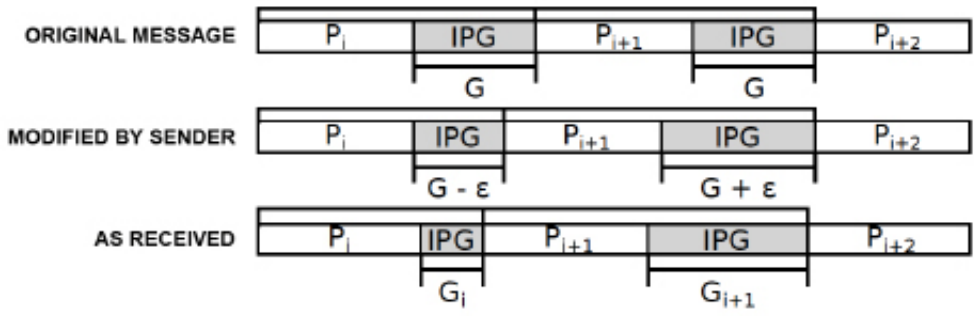
# Making a covert channel on the Internet

June 4 2014, by Bill Steele




On computer networks, packets of data (P) are separated by a standard interpacket delay (IPD). A hidden message can be sent by making the delay longer or shorter than usual. Although the length of the delay may be distorted slightly as the signal travels long distances over the Internet, as long as the delay remains shorter or longer, the message gets through.

(Phys.org) —The best way to keep a message secret is not just to encrypt it, but to hide the fact that the message is even there. Computer scientists have created "covert channels" on the Internet, but they have been slow and fairly easy to detect. Now a Cornell researcher has demonstrated a way to send messages that are undetectable by ordinary methods, with high reliability and enough bandwidth for video chat.

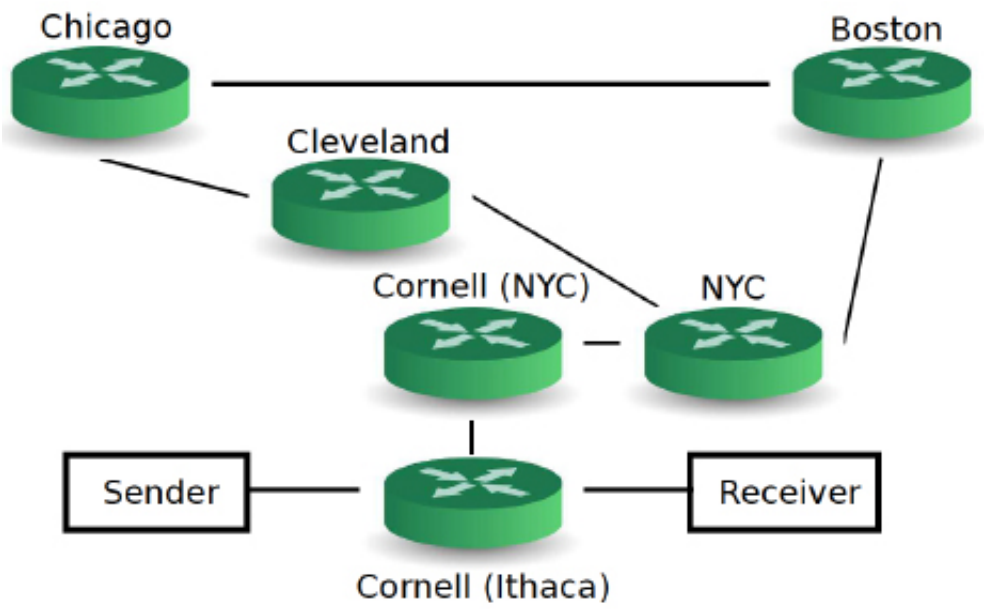
The secret is to go down to the hardware level, where the hidden signal is measured in picoseconds. "If you had the same precise tool that we have you could detect or intercept the message," said Hakim Weatherspoon, assistant professor of computer science. "You'd want the Department of

Defense to deploy this."

Weatherspoon and colleagues described their method at the USENIX Symposium on Networked Systems Design and Implementation, April 2-4 in Seattle.

When you send a message on the Internet, your computer encodes letters, numbers and other data into strings of ones and zeroes and organizes them into "packets" that contain an address and other identifying information followed by a chunk of content. Your computer sees the ones and zeroes as different voltages, but a network interface translates them into pulses of light that it injects into optical fiber to send across town or across the country, with a pulse representing 1 and no pulse representing 0. At the receiving end, similar hardware translates the pulses of light into electrical signals for a computer that gathers related packets together and extracts the message.

The network standard is to insert at least 12 "idle characters" – just a string of zeroes – between packets. A message can be hidden in the data stream by varying the length of that space. Making it longer than normal can represent a one, shorter a zero. When this is done by software, an administrator monitoring the network can easily detect it; a statistical analysis of the traffic will reveal patterns in the timing. A network also can be designed to jam such covert channels by regulating interpacket delays.




To test the covert channel method, researchers sent signals on a round-robin tour of the Internet, starting and ending at the Corrnell campus in Ithaca. Tests showed the method could deliver a hidden message with high bandwidth despite distortion enroute.

Weatherspoon and graduate students Ki Suh Lee and Han Wang created their covert channel, which they call Chupja – a Korean word for spy – at the hardware level, using a network interface card designed by Weatherspoon that allows precise software control over optical signals. A receiver with similar capability can detect the timing variations and read the message, but off-the-shelf hardware used by most networks discards the idle characters before passing packets along to the receiving computer, so the message is invisible to an administrator's monitoring software.

Conventional hardware measures interpacket delays in milliseconds, but a Chupja channel varies them by picoseconds, Weatherspoon explained. Creating the covert channel is an exercise in balance, he added. The variation must be small enough to avoid detection, but large enough to

survive minor delays and distortions as the signal goes through network routers.

In tests, the researchers sent covert messages over thousands of miles and many "hops" on the National Lambda Rail research network – from Ithaca to New York City to Cleveland, Chicago, Boston and back – with less than a 10 percent error rate, which can be managed by standard error-correcting software. Bandwidth is more than 80 kilobits per second. "We're able to send very complex messages," Weatherspoon said. "You can do the things you're used to doing, like looking at websites, but do so covertly."

To protect or prevent such covert channels, the researchers concluded, administrators will have to deploy hardware that can monitor traffic at a finer-grained level.

Provided by Cornell University