

Sending secret messages over public internet lines can take place with new technique

A new technique sends secret messages under other people's noses so cleverly that it would impress James Bond--yet the procedure is so firmly rooted in the real world that it can be instantly used with existing equipment and infrastructure.

At this week's annual meeting of the Optical Society of America in Rochester, N.Y., Bernard Wu and Evgenii Narimanov of Princeton University will present a method for transmitting secret messages over existing public fiber-optic networks, such as those operated by Internet service providers. This technique could immediately allow inexpensive, widespread, and secure transmission of confidential and sensitive data by governments and businesses.

Wu and Narimanov's technique is not the usual form of encryption, in which computer software scrambles a message. Instead, it's a more hardware-oriented form of encryption--it uses the real-world properties of an optical-fiber network to cloak a message. The sender transmits an optical signal that is so faint that it is very hard to detect, let alone decode.

The method takes advantage of the fact that real-world fiber-optics systems inevitably have low levels of "noise," random jitters in the light waves that transmit information through the network. The new technique hides the secret message in this optical noise.

In the technique, the sender first translates the secret message into an ultrashort pulse of light. Then, a commercially available optical device (called an optical CDMA encoder) spreads the intense, short pulse into a long, faint stream of optical data, so that the optical message is fainter than the noisy jitters in the fiber-optic network. The intended recipient decodes the message by employing information on how the secret message was originally spread out and using an optical device to compress the message back to its original state. The method is very secure: even if eavesdroppers knew a secret transmission was taking place, any slight imperfection in their knowledge of how the secret signal was spread out would make it too hard to pick out amidst the more intense public signal.

Although the researchers have made public this transmission scheme, and the components for carrying it out are all available, lead author Bernard Wu does not think this technique is being used yet.

"As the method uses optical CDMA technology, which is still undergoing significant research, I don't think any government or corporation is implementing this technique yet," Wu says.

While Wu foresees that government and businesses would have the greatest use for this technique, consumer applications are possible, he says. For example, consumers may occasionally transmit sensitive data via fiber-optic lines for a banking transaction. "This would not be a primary transmission scheme one would employ 24/7, as the price for enhanced security is a lower transmission rate," says Wu. Yet, since consumers send encrypted information to banks only intermittently, "the stealth method is practical" for that purpose, he says.

For more details, see article:

"A method for secure communications over a public fiber-optical network," Bernard B. Wu and Evgenii E. Narimanov, published in *Optics Express*, Vol. 14, Issue 9, pp. 3738-3751, full text at <http://www.opticsexpress.org/abstract.cfm?id=89578>

Source: Optical Society of America

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.