Beyond encryption: Stronger security for wireless communications

November 25 2013

Prof. Holger Boche and Dr. Rafael Schaefer, winner of the Johann Philipp Reis Prize, discuss their novel security system for wireless communications. Credit: U. Benz/TUM

Physically, wireless communication channels are right out in the open, carried through the air on radio waves. A "wiretapper" can eavesdrop on mobile phone and data traffic without actually tapping a wire or optical fiber. An active wiretapper may also control or disturb a legitimate user's channel, or exploit side information to compromise the security of a message. Thus the last line of defense today is encryption, aimed at making the intercepted message difficult if not impossible for anyone other than the intended recipient to decipher. But cryptographic techniques are being rendered less and less secure by advances in computing.

Now, TUM researchers Prof. Holger Boche and Dr. Rafael Schaefer have devised a scheme that wrings provably strong security out of the otherwise vulnerable physical layer. This approach can prevent a would-be eavesdropper from even receiving the transmitted information. The starting point seems counter-intuitive: The scheme uses two physical channels – that is, frequency bands in a wireless system – that are inherently useless, each being incapable of securely transmitting a message.

No reception for eavesdroppers

Normally, there is nothing to be gained by combining two channels with zero capacity: Zero plus zero equals zero. "But in this case," Schaefer explains, "it's as if we're getting a positive result from adding zero to zero. We find that we are able to 'super-activate' the whole system, meaning that combining two useless channels can lead to a positive capacity to transmit confidential messages securely."

Similar results have been reported before, but only in studies of so-called quantum communications, and are not directly applicable to present-day technology. "To the best of our knowledge," Boche says, "this is the first example of super-activation – where zero plus zero is greater than zero – in classical communication scenarios." Boche and Schaefer have also determined how to calculate the "secrecy capacity" of physical-layer channels designed to defeat active wiretappers. In addition, they have characterized the code structure and optimal transceiver design for implementing this scheme, a further step toward practical applications.

Johann Philipp Reis Prize for Rafael Schaefer

In recognition of this research, the Frankfurt-based Association for Electrical, Electronic and Information Technologies (VDE) has just awarded the prestigious Johann Philipp Reis Prize to Rafael Schaefer. The prize, named for the German inventor of the telephone, honors researchers under 40 for outstanding contributions to communications technology. Beginning in December 2013, Schaefer is continuing his work at Princeton University as a postdoctoral researcher with Vincent Poor, professor of electrical engineering and dean of the School of Engineering and Applied Sciences.

More information: Capacity Results and Super-Activation for Wiretap Channels with Active Wiretappers. Holger Boche and Rafael F. Schaefer. IEEE Transactions on Information Forensics and Security, Vol. 8 No. 9, September 2013, pp. 1482-1496. DOI: 10.1109/TIFS.2013.2276049

Wiretap Channels with Side Information – Strong Secrecy Capacity and Optimal Transceiver Design. Holger Boche and Rafael F. Schaefer. IEEE Transactions on Information Forensics and Security, Vol. 8 No. 8, August 2013, pp. 1397-1408. DOI: 10.1109/TIFS.2013.2271424

Provided by Technical University Munich

Citation: Beyond encryption: Stronger security for wireless communications (2013, November 25) retrieved 9 April 2024 from https://phys.org/news/2013-11-encryption-stronger-wireless.html