Cooperative Communications with Confidential Messages

Results in Brief

Secure data exchange in ad hoc networks

Cooperation amongst nodes could make wireless networks vulnerable and susceptible to attacks. EU-funded scientists explored such security issues for ad hoc networks.

DIGITAL ECONOMY

© Thinkstock

In the near future, conventional wireless networks are expected to be superseded by decentralised ones, with different mobile terminals joining and leaving the network. While designing such systems, an important concern is the reliable exchange of confidential data amongst trusted network nodes.

The project 'Cooperative communications with confidential messages' (CCCM) focused on increasing security in ad hoc networks, where heterogeneous nodes cannot exchange cryptographic keys with absolute secrecy. The underlying idea was to design a network in which data is transmitted from the source to the destination node with minimal power. To a great extent, this would guard against malicious nodes receiving data not intended for them.

To increase throughput, other friendly users would be able to cooperate with the sender. For a given power, the project sought to maximise reliability and throughput of wireless ad hoc networks while ensuring confidential communication.

Cooperative nodes were found to improve overall network security either by acting as relays or sending interference to the eavesdropper (jammers). Except for mobile, such nodes could be fixed, thus allowing managed infrastructure networks to enhance secure transmission. In particular, secrecy throughput was increased when modelling the ad hoc network in a square lattice.

Scientists also found that it was possible to keep data confidential from intermediate nodes. This concept was useful since it enabled secure transmission via untrusted cooperative nodes. In such a case, their use as jammers proved to be more effective compared to their relay counterparts.

Another part of project work involved combining information-theoretic with conventional cryptographic secrecy. Based on this, perfectly secure links supported by cooperative nodes were used for exchanging secret keys between the legitimate parties, resulting in increased secrecy throughput.

Project findings open up new possibilities in cooperative communications. In particular, in addition to mobile ad hoc networks, information-theoretic secrecy could find practical use in a wide range of fields. These include near-field communication and radio frequency identification networks, network coding systems, social networking safety and privacy on the smart grid.

Keywords

Secure data | data exchange | ad hoc network | wireless networks | confidential data | network nodes | cooperative communications | cryptographic | cooperative node | jammers | secure transmission | secrecy throughput | information-theoretic

Project Information

CCCM

Grant agreement ID: 237669

Project closed

Start date
1 December 2009

End date
31 May 2013

Funded under
Specific programme "People" implementing the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007 to 2013)

Total cost

€ 251 049,26

EU contribution
€ 251 049,26

Coordinated by
ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE
Switzerland

Last update: 22 January 2015

Permalink: https://cordis.europa.eu/article/id/151935-secure-data-exchange-in-adhoc-networks