instituto de telecomunicações

New physical layer security technology comprising an innovative secure channel training scheme that protects a two user non-orthogonal multiple access (NOMA) system against eavesdropping attacks. This technology improves the confidentiality level of the current and future wireless systems, more specifically in scenarios in which the transmission channel is shared by several terminals using a power domain NOMA scheme.

Tech offer | Secure channel training method for NOMA systems

In commercial wireless standards, the protection against eavesdropping attacks has been provided by cryptographic protocols. The secrecy provided by these protocols relies on the assumption that some complex mathematical problems would take thousands of years to be solved using conventional computing methods. However, with the recent progresses in the field of quantum processing, some of these problems will be solvable, making less secure the current cryptographic techniques.

In wireless networks, one of the solutions to address these new threats in secrecy is physical layer security. The main area behind physical layer security is to use the channel dynamics to create uncertainty at the eavesdropper. Contrarily to what happens with commercial cryptosystems, in physical layer security the secrecy performance is quantified from an information theoretical perspective not relying on any type of technological limitation at the eavesdropper. This invention was designed and evaluated using physical layer security principles and comprises an innovative secure channel training scheme that protects a NOMA system against eavesdropping attacks coming from inside and outside of the network.

APPLICATIONS

This invention is targeted to support low throughput services with stringent secrecy requirements.
All type of services that need to exchange small blocks of critical information with maximum secrecy are target applications.

EXCHANGE OF SECRET KEYS

EXCHANGE OF BANKING INFORMATION, such as:

- Credit card numbers
- Passwords

IMPROVING SECURITY OF WIRELESS NETWORKS

SECURE NETWORK ASSOCIATION

BENEFITS

INDEPENDENCE OF COMPUTATIONAL CAPABILITIES AVAILABLE AT THE EAVESDROPPER: this solution assures high security performance, being resistant to attacks carried using advanced processing technologies (e.g. quantum computation).

PROTECTION AGAINST ATTACKS FROM INSIDE AND OUTSIDE OF THE NETWORK: this invention considers not only the presence of undetectable passive eavesdroppers that remain located outside of the network, but also internal attacks coming from eavesdroppers registered as legitimate users inside the network.

instituto de telecomunicações

INTELLECTUAL PROPERTY

- USA patent pending (US17622971)
- European patent pending (EP20751285)
- Portuguese patent granted (PT115616)

INVENTORS

Researchers from:

- Instituto de Telecomunicações (IT)
- Universidade de Aveiro

SCIENTIFIC PUBLICATIONS

G. Anjos, D. Castanheira, A. Silva and A. Gameiro, "Securing Non-Orthogonal Multiple Access Systems Against Simultaneous Eavesdropping Attacks Coming from Inside and Outside of the Network," *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2019, pp. 1-7, doi: 10.1109/PIMRC.2019.8904169.

G. Anjos, D. Castanheira, A. Silva and A. Gameiro, "A Method Exploiting the Channel-Training Phase to Achieve Secrecy in a Fading Broadcast Channel," in *IEEE Transactions on Signal and Information Processing over Networks*, doi: 10.1109/TSIPN.2022.3161086.

DEVELOPMENT STAGE

TRL 2

The evaluation of the present invention was done using already proved theorems and channel models widely acknowledged in the field of information theory and wireless communications, respectively. In a second stage, computer simulations were compared with the derived theoretical results.

The hardware materialization of this invention is feasible using current state of art applying specific integrated circuit technologies.

KEYWORDS

Physical Layer Security (PLS)
Non-Orthogonal Multiple Access (NOMA)
Secure Channel Training
Cooperative Jamming
Eavesdropping

TARGET MARKET

This type of technology targets a generation of mobile communications beyond 5G. IT seeks partners among companies that manufacture chip for wireless communications.

COMMERCIAL OFFERING

- Licensing agreement
- Testing new applications
- Joint further developments

CONTACT

Instituto de Telecomunicações
Campus Universitário de Santiago
3810-193 Aveiro | Portugal
Tel: +351 234 377 900
Email: ipr@av.it.pt
Web: www.it.pt

TECHNOLOGY ID

PI-1009