Sharing secrets when eavesdroppers are around
How to guarantee a high probability of secrecy in wireless communications by jamming eavesdroppers?

Nabil Romero Zurita
School of Electrical and Electronic Engineering

Listen, do you want to know a secret? Do you promise not to tell...

Alice

Doesn’t know anything about the eavesdroppers (Eves).

Eve A

Eve B

I’m in love with you

I’ve known a secret for a week or two, nobody knows, just we two.

I'm in love with you

Information to transmit could be any kind of digital data.

Bob

For a high probability of secrecy, it is necessary to supply more power for Alice.

Secure Strategy

Transmit the message more strongly in the direction of Bob than to the Eves using multiple antennae and signal processing.

Broadcast corrupting artificial noise in all the directions except towards Bob.

For Bob a good received signal quality with no artificial noise so he can perfectly understand the message.

For Eves, in a probabilistic way, a poor received signal quality corrupted by artificial noise so they cannot understand the message.

Guarantee

How much power must be allocated to the information and artificial noise to guarantee a given probability of secrecy?

Receiver | Signal Quality | Message |
--- | --- | --- |
Bob | Good | Decoded |
Eves | Bad | Not decoded |

High probability of secrecy is guaranteed by an efficient power allocation mechanism based on a probabilistic definition of secrecy that satisfies signal quality levels for Bob and Eves.

This work has been accepted for publication in the IEEE Signal Processing Letters Journal under the title "Outage Probability Based Power Distribution Between Data and Artificial Noise for Physical Layer Security" by N. Romero-Zurita, M. Ghogho, and D. McLernon. 2012.

Lyrics from fragments of the song "Do you want to know a secret" by Lennon and McCartney. Parlophone, London, 1963.