A disc of scatterers based radio channel model for secure key generation

Author(s) - Institution(s):
Taghrid Mazloum, TPTech
Alain Sibille, TPTech

Corresponding author email: taghrid.mazloum@telecom-paristech.fr

Corresponding WG group: WG1

Abstract:

Physical layer security is a method to ensure the confidentiality of a wireless communication from encryption keys exploiting the randomness of the reciprocal propagation channel between a pair of legitimate users, Alice and Bob. This confidentiality is achieved owing to the decorrelation between these channels and that experienced by a third terminal (Eve), acting as an eavesdropper. In this work, we evaluate the secrecy capacity of a simple channel model, based on a disc of scatterers. The model allows to consider any distance between Alice and Eve within the disc and is thus not limited to a stationary region. Moreover, we develop an analysis of the definition of radio channel scenarios for Alice, Bob and Eve, depending on their degree of knowledge of the environment. The practical relevance of these scenarios is discussed, in relation with the Gaussian or non Gaussian character of the channel statistics and its impact on the computation of the secrecy capacity.