1. Record Nr. TD17056783

Autore	Badawy, Ahmed Mohamed Habelroman B M
Titolo	Practical Secrecy at the Physical Layer: Key Extraction Methods with Applications in Cognitive Radio [Tesi di dottorato]
Editore	Politecnico di Torino, 2017
Lingua di pubblicazione	Inglese
Formato	Tesi di dottorato
Livello bibliografico	Monografia
Note	In relazione con http://porto.polito.it/2674477/

Sommario

The broadcast nature of wireless communication imposes the risk of information leakage to adversarial or unauthorized receivers. Therefore, information security between intended users remains a challenging issue. Currently, wireless security relies on cryptographic techniques and protocols that lie at the upper layers of the wireless network. One main drawback of these existing techniques is the necessity of a complex key management scheme in the case of symmetric ciphers and high computational complexity in the case of asymmetric ciphers. On the other hand, physical layer security has attracted significant interest from the research community due to its potential to generate information-theoretic secure keys. In addition, since the vast majority of physical layer security techniques exploit the inherent randomness of the communication channel, key exchange is no longer mandatory. However, additive white Gaussian noise, interference, channel estimation errors and the fact that communicating transceivers employ different radio frequency (RF) chains are among the reasons that limit utilization of secret key generation (SKG) algorithms to high signal to noise ratio levels. The scope of this dissertation is to design novel secret key generation algorithms to overcome this main drawback. In particular, we design a channel based SKG algorithm that increases the dynamic range of the key generation system. In addition, we design an algorithm that exploits angle of arrival (AoA) as a common source of randomness to

	generate the secret key. Existing AoA estimation systems either have high hardware and computation complexities or low performance, which hinder their incorporation within the context of SKG. To overcome this challenge, we design a novel high performance yet simple and efficient AoA estimation system that fits the objective of collecting sequences of AoAs for SKG. Cognitive radio networks (CRNs) are designed to increase spectrum usage efficiency by allowing secondary users (SUs) to exploit spectrum slots that are unused by the spectrum owners, i.e., primary users (PUs). Hence, spectrum sensing (SS) is essential in any CRN. CRNs can work both in opportunistic (interweaved) as well as overlay and/or underlay (limited interference) fashions. CRNs typically operate at low SNR levels, particularly, to support overlay/underlay operations. Similar to other wireless networks, CRNs are susceptible to various physical layer security attacks including spectrum sensing data falsification and eavesdropping. In addition to the generalized SKG methods provided in this thesis and due to the peculiarity of CRNs, we further provide a specific method of SKG for CRNs. After studying, developing and implementing several SS techniques, we design an SKG algorithm that exploits SS data. Our algorithm does not interrupt the SS operation and does not require additional time to generate the secret key. Therefore, it is suitable for CRNs.
Localizzazioni e accesso	http://memoria.depositolegale.it/*/http://porto.polito.it/2674477/1/BADAWY_PhD_Thesis.pdf