Faculty of Electrical Engineering & Computer Science
Master Degree Course Electronics Engineering, MSc EE

HSB
Hochschule Bremen
City University of Applied Sciences

Master 2017

Munder Hamruni

Practical Implementation of Physical-Layer Key Generation using Standard WLAN Cards and Performance Evaluation.

ABSTRACT - Masterthesis

The properties of the physical layer in wireless networks are exploited to generate one-time pads which are subsequently used for secure communication between legitimate users. Previous measurement testbeds relied mostly on RSSI information, since such information could be provided by most off-the-shelf wireless network cards. However, it has been shown that a significant performance gain can be obtained by using more fine-grained measurement samples, such as the channel state information (CSI). In this thesis, a measurement testbed is developed using commercially available Intel 5300 NICs, along with a Linux 802.11n CSI Tool. The platform consists of three laptops, running Ubuntu 14.04 LTS, Kernel 3.2, two acting as the legitimate users, Alice and Bob, while the third is acting as an eavesdropper. The initial measurement phase of the key generation process is simulated, where the legitimate users take turns in sending signals in consecutive TDD slots, while the other legitimate user and the eavesdropper are listening. The position of the eavesdropper is varied during the CSI measurements and frequency distributions are obtained. A study of the correlation between the legitimate channels and the eavesdropping channels is presented, along with a performance evaluation of the system.