Physical Layer Authentication in WiFi networks

Introduction:

Researchers studying physical layer security envision a paradigm shift in the methods for ensuring security and privacy in wireless networks. Traditionally, cryptographic mechanisms are introduced in the higher layers of the protocol stack so as to allow security features such as message authentication and encryption. However, the research community believes that due to the increase in use of wireless communications, such methods alone will not be sufficient to provide security in future wireless networks where low latencies and real-time performance are important design goals.

Physical layer security exploits various properties of the transmitting devices and their physical communication channel to secure communication. Such features can be device specific e.g., hardware impairments or carrier frequency offset [1], or channel characteristics e.g., received signal strength or channel frequency responses [2]. Security mechanisms at the physical layer greatly rely on using features that are unique for each communication link. Therefore, studying properties of such features e.g., correlations, variation over time and in space lays a foundation for implementation of physical layer security schemes.

Thesis Outline:

This thesis project gives the student opportunity to work with software defined radios from Ettus Research [3]. The focus is on doing indoor measurements of various channel and hardware features that are of interest for physical layer security schemes. In order to do this, the student will need to evaluate an existing OFDM transceiver implementation for IEEE 802.11a/g/p. The scope of the project is to provide an analysis of the measurements which deepens the understanding on what features can be of use in the context of physical layer security.

The expected outcomes of this master thesis project is in summary:
1) Verification and performance evaluation of the 802.11 implementation on the Ettus software defined radios with a special focus on real-time capabilities (i.e., which latency constraints can be satisfied and which are its limitations?).
2) Provide measurements of indoor channel responses and device specific features for an uplink with 2 users and 1 access point.
3) Analysis of the measurements with respect to their usefulness in the context of physical layer security (e.g., what is the typical coherence time, correlation between neighbouring channels in an indoor environment).
4) Given that the first tasks are completed within the expected time frame, the student is encourage to develop and implement a physical layer authentication scheme on the software defined radios.

Please note that the final grade is not dependent on completing task 4).

Requirements:

The candidate is expected to have good theoretic knowledge within the fields of digital communication, digital signal processing and estimation theory. Furthermore, good programming skills are necessary. Knowledge on or previous experience with WiFi, software defined radios or wireless security is a plus but not necessary.

Contact:

Ragnar Thobaben ragnart@kth.se
Henrik Forssell hefo@kth.se

References:

[1] - Ur Rahman, M.M.; Yasmeen, A.; Gross, J., "PHY layer authentication via drifting oscillators," in Global Communications Conference (GLOBECOM), 2014 IEEE , vol., no., pp.716-721, 8-12 Dec. 2014
doi: 10.1109/GLOCOM.2014.7036892
[2] - Liang Xiao; Greenstein, L.; Mandayam, N.; Trappe, W., "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," in Communications, 2007. ICC '07. IEEE International Conference on , vol., no., pp.4646-4651, 24-28 June 2007
doi: 10.1109/ICC.2007.767
[3] - http://www.ettus.com/product/details/UN210-KIT