# Device authentication at the Physical layer in EchoRing

**Introduction:**
Wireless medium being broadcast in nature is prone to passive attacks (eavesdropping) and active attacks (false identity claims) by adversaries. Henceforth, it is of great interest to design, implement and test novel (physical-layer) schemes (e.g., shared secret key generation, device authentication etc.) which ensure secure communication between the legitimate parties while simultaneously keeping the adversaries almost oblivious about it.
EchoRing is a novel token-passing wireless protocol which provides ultra-high reliabilities coupled with very low end-to-end latencies [1]; and therefore, finds its application in many machine-to-machine applications, e.g., industrial automation etc. However, like all other wireless protocols, EchoRing is prone to attacks by adversaries which, if not taken care of, can cause massive damage to the industrial equipment.To this end, there have been some recent efforts where cryptographic mechanisms were employed for device authentication in the EchoRing. Having said this, the goal of this thesis is to incorporate additional physical-layer mechanisms for device authentication so as to enhance the current security-level of the EchoRing.

**Thesis outline:**
The tentative thesis outline is as follows. First of all, the student will do the implementation feasibility analysis, w.r.t. the protocol state machine, token format etc. of EchoRing, of two candidate physical-layer attributes namely: i) wireless channel [2], ii) frequency offset [3], for device authentication framework. For each physical-layer attribute, the student will first evaluate the case when it is time-invariant, followed by the case when it is time-varying. Then, the proposed authentication framework will be implemented on WARP software-defined radios, and thereafter, will be integrated into already existing prototype of EchoRing. Depending upon the student's progress, a far-end extension is also possible where the student will extend the same authentication scheme to the scenario with multiple legitimate nodes and multiple adversaries.

**Requirements:**
Candidate is expected to have reasonable (or, at least, basic) knowledge of security mechanisms employed by existing and upcoming wireless LAN/PAN standards (e.g., 802.11x, Zigbee, Bluetooth etc.). At the same time, some past exposure to FPGA programming is a plus; and therefore, is highly encouraged.

**Contact:**
james.gross@ee.kth.se
mahboob.rahman@ee.kth.se

**References:**
[1] Dombrowski, C., & Gross, J. (2015). EchoRing: A Low-Latency, Reliable Token-passing MAC Protocol for Wireless Industrial Networks. In European Wireless Conference 2015 (EW 2015).
[2] Liang Xiao; Greenstein, L.; Mandayam, N.; Trappe, W., "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," Communications, 2007. ICC '07. IEEE International Conference on , vol., no., pp.4646,4651, 24-28 June 2007.
[3] Ur Rahman, M.M.; Yasmeen, A.; Gross, J., "PHY layer authentication via drifting oscillators," Global Communications Conference (GLOBECOM), 2014 IEEE , vol., no., pp.716,721, 8-12 Dec. 2014.