Thesis/Project Proposal

Name	Attacks implementation and detection in WSNs
Contacts	Luigi Pomante <luigi.pomante@univaq.it> Walter Tiberti <walter.tiberti@graduate.univaq.it>
Type	Implementation, Research
Keywords	WSN, Intrusion Detection System, WIDS
Description	The Wireless Sensor Networks (WSN) are, like any other kind of network, vulnerable to different attack vectors. In particular, there are a series of WSN-specific attacks that can compromise the overall functionality of the WSN. One of the possible solutions to reduce the attack surface and to stop/mitigate the attack on WSN, an Intrusion Detection System (IDS) can be adopted. WIDS [1] is a UNIVAQ proof-of-concept IDS for WSN. It has been implemented on top of TinyOS (with the name *TinyWIDS* [2]). WIDS is a misuse-based IDS: it tries to estimate an operating *state* of the WSN motes in respect of a series of known attacks modeled as *Weak Process Models.* The project activities are the following: 1) Analyze the state-of-the-art for critical attacks and exploits on WSN platforms 2) Model the attacks found as WPMs 3) Integrate such attacks in WIDS/TinyWIDS 4) Conduct a series of experiments to validate and performance footprint of TinyWIDS with the modeled attacks
Expected Duration	3-5 months
References (Online)	[1] https://ieeexplore.ieee.org/document/6775056 [2] https://www.researchgate.net/publication/329460779_TinyWIDS_a_WPM-based_Intrusion_Detection_System_for_TinyOS2x802154_Wireless_Sensor_Networks
References (Attached)	