Abstract

WIRELESS SENSOR NETWORKS

Security and military applications

Internet-of-Things (IoT) applications are continuously evolving and IoT based devices are being deployed in industrial, residential or city environments in order to achieve greater manufacturing efficiency, higher living standards or prevent hazards. Wireless Sensor Networks (WSN) nodes, an important subcomponent of IoT infrastructures, are collecting, aggregating and transmitting sensitive data that needs to be properly secured. This has become a major concern in the past decade due to the cyber security context.

WSN applications are well known for their special characteristics, for the particular types of infrastructures, the target environment and operational requirements. This is why WSN security becomes a complex topic which involves identifying simple and safe cryptographic primitives, implementing efficient cryptographic mechanisms for the network nodes, adapting the communication protocols and stacks to counteract specific WSN attacks or mitigate their effects.

A side theme in this area of interest is the identification and implementation of custom-made technical methods for achieving greater energy efficiency for all WSN nodes in order to extend the life of the network infrastructure.

Military applications are the engine for the development of many modern technologies, and sensor networks were born right within a military application. The integration of a wide range of functionalities for a WSN node in a small hardware platform, made this type of infrastructure a good candidate for several types of military equipment.

The thesis is structured into two main themes - security in wireless sensor networks and military applications based on sensor networks. The following objectives have been proposed and achieved during this PhD program: conducting a careful analysis of WSN characteristics in order to accumulate specialized knowledge and skills, choosing useful tools for the research activities, conducting a thorough presentation of WSN security issues, choosing a feasible cryptographic instrument for the WSN security context, proposing and developing original WSN security solutions, conducting an analysis of military applications based on WSN infrastructures and proposing new implementation solutions, analyzing the impact of the proposed security solutions on the sensor node energy consumption.