

**Call for application for research scholarships
for post-graduate international candidates**

RESEARCH PROJECT N. 56

Title

Key management techniques in Wireless Sensor Networks

Scientific responsible (name, surname, role)

Filippo Gandino, Assistant Professor (filippo.gandino@polito.it)

Short description of the research activity (max 250 words)

Wireless sensor networks (WSNs) offer benefits in several applications but are vulnerable to various security threats, such as eavesdropping and hardware tampering. In order to reach secure communications among nodes, many approaches employ symmetric encryption. Several key management schemes have been proposed to establish symmetric keys exploiting different techniques (e.g., random distribution of secret material and transitory master key). According to the different applications of WSNs, the state-of-the-art protocols have different characteristics and different gaps.

The proposed research activity will be focused on the study and development of key management protocols. The proposed investigation will consider both the security requirements and the performance (e.g., power consumption, quantity of additional messages, computational effort) of the networks. The research will analyze different possible solutions, evaluating the trade-off in terms of costs and benefits, according to different possible scenarios and applications.

Specific requirements (experiences, skills)

The proposed research involves multidisciplinary knowledge and skills (e.g., computer network and security, advanced programming).

Website of the research group (if any)

Keywords (min 3, max 6)

WSN, security, pervasive computing

Research Area (max 1)

Computer Engineering