CCE_27

Title of the doctoral program

Computer and Control Engineering

Title of the research activity

Key management techniques in Wireless Sensor Networks

Short description of the research activity

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 in order 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.

The objectives of the proposed activity consist in studying the state-of-the-art of key management protocols for WSNs and to propose new solutions suitable to various application scenarios. The requirements that affect the security protocols will be considered in order to find the best solution for different kinds of WSNs. In particular, the mobility of the nodes and the possibility to add new nodes after the first deployment will be considered.

The proposal of new solutions will start by analyzing the state-of-the-art protocols in order to find their weakness and to overcome them. For example, for key management schemes based on a transitory master key, which are exposed to great risks during the initialization phase, a new strategy could consider the possibility of reducing the time required for the key establishment.

The proposed solutions will be evaluated and compared to state-of-the-art approaches, in order to evaluate their security level and their performance. The analysis of the protocols will be composed by: (a) a theoretical analysis, (b) simulations, and (c) implementation on real nodes.

The theoretical analysis will consider several aspects of the key management protocols. A part of this analysis will evaluate the statistical characteristics of the scheme, in order to analyze the level of security and other network parameters for protocols based on stochastic elements. A security analysis will compare the properties and the requirements of the protocols.

The simulations will be used to analyze the performance of the schemes with a high number of nodes. This kind of investigation allows reaching significant results within a limited time. There are many available tools that allow simulating WSNs, e.g., TOSSIM, which uses the same code written for the TinyOS platform.

The last kind of analysis will be based on an experimental session on a real network. The main platform that will be used will be TinyOS, in order to develop a code that can be used also for the simulations. The main purpose of a real implementation is to validate the results achieved by simulations.

Scientific responsible (name, surname, role, email)

Filippo Gandino, Assistant professor, filippo.gandino@polito.it

Number of vacancies for XXXI cycle (3 years program)

1

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)

www.cad.polito.it