Abstract

Cryptographic Protocols in Wireless Sensor Networks: A Critical Review [†]

Angel Martin del Rey * and Araceli Queiruga Dios

Department of Applied Mathematics, University of Salamanca, 37008 Salamanca, Spain; queirugadios@usal.es

* Correspondence: delrey@usal.es

[†] Presented at the 5th International Symposium on Sensor Science (I3S 2017), Barcelona, Spain, 27–29 September 2017.

Published: 29 November 2017

Wireless sensor networks (WSNs) play a fundamental role in new paradigms such as the Internet of Everything or the Industry 4.0. Usually, these networks are constituted by hundreds or thousands of sensor nodes with limited resource capabilities whose main goal is to monitor, collect, compute and communicate data from the environment in an efficient and distributed way.

WSNs are widely used in several different fields such as environmental management and research, e-health, military and risk management, etc. In many of these applications, the security of the network is a fundamental issue. Consequently, it is crucial to guarantee the confidentiality, integrity, authenticity and availability of the data transmitted through the WSN.

Most of the cryptographic protocols implemented in WSNs for key establishment and data encryption (secret-key cryptosystems and public-key cryptosystems) are adaptations of those used in other types of environments without the limited resources and capabilities of WSNs.

The main goal of this work is to perform a critical review of such cryptographic protocols, focusing the attention on secret-key cryptosystems since this type of protocol requires less processing time than public-key algorithms. The problems, solutions and challenges dealing with this topic will be identified and explicitly shown.

© 2017 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).