Adaptive Security in ODMAC for Multihop Energy Harvesting Wireless Sensor Networks -
DTU Orbit (29/12/2018)


Energy Harvesting Wireless Sensor Networks (EH-WSNs) represent an interesting new paradigm where individual nodes forming a network are powered by energy sources scavenged from the surrounding environment. This technique provides numerous advantages, but also new design challenges. Securing the communications under energy constraints represents one of these key challenges. The amount of energy available is theoretically infinite in the long run but highly variable over short periods of time, and managing it is a crucial aspect. In this paper we present an adaptive approach for security in multihop EH-WSNs which allows different nodes to dynamically choose the most appropriate energy-affecting parameters such as encryption algorithm and key size, providing in this way energy savings. In order to provide evidence of the approach’s feasibility in a real-world network, we have designed and implemented it as extension of on-demand medium access control (ODMAC), a receiver-initiated (RI) MAC protocol specifically designed and developed to address the foundational energy-related needs of Energy Harvesting Wireless Sensor Networks.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Department of Informatics and Mathematical Modeling, Embedded Systems Engineering, University of Bristol, Örebro University
Contributors: Di Mauro, A., Fafoutis, X., Dragoni, N.
Number of pages: 11
Publication date: 2015
Peer-reviewed: Yes

Publication information
Journal: International Journal of Distributed Sensor Networks
Volume: 2015
Article number: 760302
ISSN (Print): 1550-1329
Ratings:
Web of Science (2018): Indexed yes
Scopus rating (2017): CiteScore 1.34 SJR 0.255 SNIP 0.745
Web of Science (2017): Impact factor 1.787
Web of Science (2017): Indexed yes
Scopus rating (2016): CiteScore 1.16 SJR 0.256 SNIP 0.727
Web of Science (2016): Impact factor 1.239
Scopus rating (2015): CiteScore 1.1 SJR 0.256 SNIP 0.877
Web of Science (2015): Impact factor 0.906
Web of Science (2015): Indexed yes
Scopus rating (2014): CiteScore 0.85 SJR 0.242 SNIP 0.699
Web of Science (2014): Impact factor 0.665
Web of Science (2014): Indexed yes
Scopus rating (2013): CiteScore 1.13 SJR 0.231 SNIP 0.899
Web of Science (2013): Impact factor 0.923
Scopus rating (2012): CiteScore 0.87 SJR 0.192 SNIP 0.586
Web of Science (2012): Impact factor 0.727
Scopus rating (2011): CiteScore 0.53 SJR 0.16 SNIP 0.44
Web of Science (2011): Impact factor 0.203
Scopus rating (2010): SJR 0.146 SNIP 0.237
Web of Science (2010): Impact factor 0.067
Scopus rating (2009): SJR 0.303 SNIP 0.78
Web of Science (2009): Indexed yes
Scopus rating (2008): SJR 0.287 SNIP 0.919
Scopus rating (2007): SJR 0.193 SNIP 1.045
Original language: English
Keywords: COMPUTER, TELECOMMUNICATIONS, BLOCK CIPHER, PROTOCOLS
Electronic versions:
760302.pdf
DOIs:
10.1155/2015/760302