336
Accession number:20124315605142
Title:Towards security in nano-communication: Challenges and opportunities
Authors:Dressler, Falko (1); Kargl, Frank (2)
Author affiliation:(1) Computer and Communication Systems, University of Innsbruck, Austria; (2) Distributed Systems, University of Ulm, Germany; (3) Distributed and Embedded Security, University of Twente, Netherlands
Corresponding author:Dressler, F.(falko.dressler@uibk.ac.at)
Source title:Nano Communication Networks
Abbreviated source title:Nano Commun. Netw.
Volume:3
Issue:3
Issue date:September 2012
Publication year:2012
Pages:151-160
Language:English
ISSN:18787789
Document type:Journal article (JA)
Publisher:Elsevier, P.O. Box 211, Amsterdam, 1000 AE, Netherlands
Abstract:Incredible improvements in the field of nano-technologies have enabled nano-scale machines that promise new solutions for several applications in biomedical, industry and military fields. Some of these applications require or might exploit the potential advantages of communication and hence cooperative behavior of these nano-scale machines to achieve a common and challenging objective that exceeds the capabilities of a single device. Extensions to known wireless communication mechanisms as well as completely novel approaches have been investigated. Examples include RF radio communication in the terahertz band or molecular communication based on transmitter molecules. Yet, one question has not been considered so far and that is nano-communication security, i.e., how we can protect such systems from manipulation by malicious parties? Our objective in this paper is to provide some first insights into this new field and to highlight some of the open research challenges. We start from a discussion of classical security objectives and their relevance in nano-networking. Looking at the well-understood field of sensor networks, we derive requirements and investigate if and how available solutions can be applied to nano-communication. Our main observation is that, especially for molecular communication, existing security and cryptographic solutions might not be applicable. In this context, we coin the new term biochemical cryptography that might open a completely new research direction and lead to significant improvements in the field of molecular communication. We point out similarities with typical network architectures where they exist but also highlight completely new challenges where existing solutions do not apply. © 2012 Elsevier Ltd.
Number of references:31
Main heading:Cooperative communication
Controlled terms:Behavioral research - Communication - Cryptography - Military applications - Nanotechnology - Network architecture - Sensor networks - Wireless telecommunication systems
Uncontrolled terms:Co-operative behaviors - Military fields - Molecular communication - Nano-communication - Nano-scale machines - New solutions - Research challenges - Research

directions - Security - Security objectives - Terahertz band - Wireless communications
Classification code:761 Nanotechnology - 732 Control Devices - 723 Computer Software, Data Handling and Applications - 971 Social Sciences - 722.3 Data Communication, Equipment and Techniques - 716 Telecommunication; Radar, Radio and Television - 404.1 Military Engineering - 722 Computer Systems and Equipment
DOI:10.1016/j.nancom.2012.08.001
Database:Compendex