Security and Communication Networks

Special Issue on

Security Communication in On-Body Wearable Wireless Networks

CALL FOR PAPERS

An on-body wireless network (or simply oBWN) is a networked collection of wearable (programmable) sensor and actuators nodes that can communicate among themselves. The sensor nodes have computation, storage, wireless transmission, acting, and sensing capabilities. Common physiologically sensed signals/data include body motion, skin temperature, heart rate, skin conductivity, brain and muscle activities, and biomarkers. A wide range of application scenarios is enabled by oBWN technologies. Specifically, oBWN-based systems can be used to directly monitor several vital signs continuously and non-invasively, as tiny wireless sensors are placed on the skin and sometimes integrated with the garments. However, typical characteristics of oBWNs, such as severe resource constraints and harsh environmental conditions, pose additional unique challenges for security and privacy support. In this special issue, we will approach major security and privacy issues and potential attacks in oBWNs.

In this special issue, we concentrate mainly on security and privacy as well as the emerging applications of on-body wireless network. It aims to bring together researchers and practitioners from wireless and sensor networking, security, and distributed computing communities, with the goal of promoting discussions and collaborations. We are interested in novel research on all aspects of security in on-body wireless network and tradeoff between security and performance such as QoS, dependability, reliability, and scalability. The special issue covers industrial issues/applications and academic research into security and privacy for oBWNs. The practical aspects of the developments will be highly valued. Papers with a strong cryptographic background will not be considered as part of this special issue.

Potential topics include but are not limited to the following:

- Attacks on MAC layer, network layer, OS, and side-channel attacks in wearable devices
- Energy-efficient secure routing protocols in on-body wireless networks
- Users' awareness to security solutions in wearables
- Privacy and security issues for wearable devices: integrating security in protocols, sensor design, channel, and actuators
- Biometric user authentication and continuous authentication for wearable devices
- Security and privacy frameworks (simulators, tools, and platforms) for oBWN
- Cross-layer design and lightweight solutions for security, privacy, and trust of oBWNs

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/scn/bwwn/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Alvaro Araujo, Universidad Politécnica de Madrid, Madrid, Spain
araujo@b105.upm.es

Guest Editors
Hacene Fouchal, Université de Reims Champagne-Ardenne, Ardenne, France
hacene.fouchal@univ-reims.fr

Milena Radenkovic, University of Nottingham, Nottingham, UK
milena.radenkovic@nottingham.ac.uk

Submission Deadline
Friday, 1 February 2019

Publication Date
June 2019