IEEE International Conference on Communications

16-20 May 2022 // Seoul, Korea

Intelligent Connectivity for Smart World

Workshop on E-health Security for Future 6G

General Co-chairs

- **Eduard A. Jorswieck**
  TU Braunschweig, Germany
- **Babak Hossein Khalaj**
  Sharif University of Technology, Iran
- **Waltenegus Dargie**
  TU Dresden, Germany

Main contact

mletafati@ee.sharif.edu

Important Dates

- ❖ Paper submission deadline: **January 20, 2022**
- ❖ Notification of acceptance: March 06, 2022
- ❖ Camera-ready papers: March 15, 2022

Submission link

https://edas.info/N28800

Webpage link

https://www.ifn.ing.tu-bs.de/health-sec

Scope

Envisioned by the sixth generation (6G) of wireless networking, the human body becomes part of the network architecture that collects sensitive data for multiple purposes such as health and safety, aiming to enhance the quality of our lives. The 6G technology will be the fabric that can make newly-emerged technologies such as wearable devices, intelligent Internet of Medical Things (IoMT), and hospital-to-home (H2H) services become part of a unified network. On the other hand, the vitality of e-health systems exacerbates the effect of adversarial attacks, such as eavesdropping, Man-in-the-Middle (MitM), and Denial-of-Service (DoS). To secure 6G-enabled e-health services, lightweight and scalable security mechanisms are highly required. The area of PHY layer security (PHY-Sec) plays a pivotal role in reducing both the latency as well as the complexity of novel security standards which is crucial for e-health vertical of 6G for providing promising solutions to secure the most critical and less-investigated network sectors in 6G, which are the ones corresponding to digital healthcare.

Topics

We seek original completed and unpublished work not currently under review by anyother journal/magazine/conference. Topics of interest include, but are not limited to:

- Context-aware intelligent PHY-sec for e-health
- Learning-assisted secure communications for e-health
- Security aspects of utilizing digital twins for 6G-enabled e-health applications
- Security issues of 6G-enabled telemedicine
- Physical layer security for e-health cyber physical systems
- Post-quantum security for long-term e-health data
- Covert communications schemes for e-health transmissions
- Visible Light Communication (VLC) for e-health and employment of local trust zones
- Quality of e-Health Security for 6G: Analytical formulations and practical experiments
- Privacy-preserving e-health: Performance metrics (quantitative measures) and experiments
- URLLC for secure medical imaging through immersive wireless AR/VR
- Security and privacy concerns of deep learning algorithms in e-health technologies
- Real-time robustness of e-health services against adversarial attacks in 6G
- Secure molecular intra-body and wireless body area communications
- Physical layer security for wireless implantable medical devices
- Secure Human Bond Communications (HBC)
- Secure analysis of big data in e-health

Paper Submission

The workshop accepts only novel, previously unpublished papers. The page length limit for all initial submissions for review is SIX (6) printed pages (10-point font) and must be written in English.All final submissions of accepted papers must be written in English with a maximum paper length of six (6) printed pages (10-point font) including figures. No more than one (1) additional printed page (10-point font) may be included in final submissions and the extra page (the 7th page) will incur an over length page charge of USD100. For more information, please see IEEE ICC 2022 official website: https://icc2022.ieee-icc.org/authors