

The First Workshop on Backscatter Communication Security in Internet of Things Environment

October 12-27 2023
Aveiro Congress Center, Portugal

In conjunction with IEEE WF-IoT 2023



Organizing Chairs:

Masoud Kaveh

Alto University

Zhao Li

Xidian University

Zheng Yan

Xidian University

Riku Jäntti

Alto University

Important dates:

Paper submission: Jul 30, 2023

Notification of acceptance: Aug 21, 2023

Camera-ready submission: Sep 29,
2023

Presentation submission: Oct 2, 2023

Description:

The Internet of Things (IoT) has been increasingly adopted into various aspects of our lives however, it faces critical challenges such as security, privacy, and power consumption. Backscatter communication (BC) is a wireless communication technology that enables the transfer of data without requiring a dedicated power source. Instead, BC allows a battery-free device to reflect an RF signal from an ambient wireless environment, making it suitable for low-cost and low-power IoT devices. However, BC is vulnerable to various security threats thus, finding security solutions for BC is highly essential in IoT applications. This workshop seeks theoretical, mathematical, and experimental contributions to BC security in the context of IoT and aims to explore the latest developments, techniques, and solutions to address BC security.

Topics of Interest:

This workshop aims to bring together researchers and practitioners to discuss and explore the security challenges and solutions in BC for IoT networks.

Our topics of interest include but are not limited to:

- Data privacy and protection in backscatter-based IoT
- Key management and authentication protocols for backscatter-based IoT
- Physical-layer security in backscatter-based IoT
- Intrusion detection and prevention for BC in IoT network
- Threat modeling and risk assessment for BC in IoT
- Novel signal processing for BC security
- Secure routing in backscatter-based IoT networks
- Secure localization and tracking in backscatter-based IoT
- AI/ML-based security techniques for BC security
- Standardization and regulation of BC security in IoT environments
- Real-world case studies, experiments, and demonstrations of secure BC

Paper Submission:

All papers must be submitted through eWorks. You must choose the workshop track (Work-06) when submitting your paper in order to be considered for this workshop. The paper should be up to six (6) pages in length. The conference allows up to two additional pages for a maximum length of eight (8) pages upon payment of extra page fees once the paper has been accepted.

The paper can be prepared using the template available through the Authors / Proposers tab from the WF-IoT conference website main page at:

<https://wfiot2023.iot.ieee.org>.

An alternative is to use the IEEE Word or Latex tools that can be found through: <https://conferences.ieeeauthorcenter.ieee.org/write-your-paper/authoring-tools-and-templates/>.

Authors of accepted papers will need to provide a final version of their paper in PDF format and upload it by the camera-ready deadline and complete the assignment of copyright and release form. For your paper to be included in the proceedings and published in IEEE Xplore, at least one author is required to register for WF-IoT 2023 by the deadline.

More information on the workshop:

<https://wfiot2023.iot.ieee.org/1st-workshop-backscatter-communication-security-internet-things-environment>



Aalto University



西安电子科技大学
XIDIAN UNIVERSITY