IEEE Internet of Things Journal

Special Issue on Intrusion Detection for the Internet of Things

The proliferation of IoT devices in everyday human life has made their security a critical requirement. Currently those devices are not very secure because of several reasons. First, manufacturers do not account much for security, releasing products that are vulnerable to attacks, thus leaving users with security issues that are unlikely to be resolved. Second, many IoT devices do not have enough computing power to run an antivirus or even do not allow one to install an antivirus. Finally, the heterogeneity which characterizes the IoT in terms of applications, hardware, and software, expands the attack surface, while at the same time increases the difficulty of deploying all-encompassing security solutions. Despite some sort of security provided by IoT enabling technologies (e.g., communication protocols), or by intrusion prevention systems (e.g., network firewalls), attackers still find ways to compromise devices, or the communication between them. Unlike laptop and desktop computers (which have frequent on-off cycles), many IoT devices such as webcams and wireless routers operate 24/7 unattended. This makes IoT devices particularly prone to various attacks, such as attacks aiming at recruiting devices for botnets. This makes IoT networks dangerous not only for themselves but also for remote systems that are victims of attacks launched by infected IoT devices. Moreover, IoT-based systems that handle sensitive data (e.g., healthcare IS) need to promptly react to malicious activities in order to prevent private data from leaving the network. The key to protect IoT networks, thus, is to monitor for threats by means of an Intrusion Detection System (IDS). Intrusion detection is a specific aspect of cybersecurity which deserves particular attention as IDSes represent the last line of defense of computer systems. This special issue aims at gathering the recent advances and novel contributions from both academia and industry in the field of Intrusion Detection for the IoT.
Topics of interest include, but are not limited to:

- Machine learning based IDS
- Host-based IDS
- Network-based IDS
- Anomaly-based IDS
- Signature-based IDS
- Specification-based IDS
- Distributed IDS
- Privacy preserving IDS
- Malware detection
- Botnet detection
- Intrusion detection for VANET
- Intrusion detection for IoT-based industrial control systems
- Intrusion detection for IoT-based healthcare monitoring systems
- Intrusion detection for cloud-based IoT applications
- Intrusion detection at the edge/fog
- Novel attacks and related countermeasures
- Zero-day attack detection
- Game theory for the IoT security
- Scalable intrusion detection
- IDS placement strategies
- Intrusion detection for software defined IoT networks
- Intrusion detection for narrowband IoT networks
- Intrusion detection for mobile networks

Important Dates

Submission Deadline: April 1, 2022
First Review Due: May 15, 2022
Revision Due: June 30, 2022
Sec. Review Due/Notification: July 30, 2022
Final Manuscript Due: August 15, 2022
Publication Date: 2022

Submission Guidelines

Authors need to follow the manuscript format and allowable number of pages described at: http://ieeeiotj.org/guidelines-for-authors/ To submit a manuscript for consideration for the special issue, please visit the journal submission website at: https://mc.manuscriptcentral.com/iot

Guest Editors

Elisa Bertino (bertino@purdue.edu) Purdue University, West Lafayette, IN, USA.
Kui Ren (kuiren@zju.edu.cn) Zhejiang University, Zhejiang, China.
Antonino Rullo (n.rullo@dimes.unical.it) University of Calabria, Rende, Italy.