

Special Issue on **Resilience and Reliability in Communication Networks under Security Incidents**

WILEY



CALL FOR PAPERS

Our current society is becoming more and more dependent on communication networks, whose disruption can create a severe impact in our daily lives. Therefore, we are interested in keeping these networks operating at acceptable service levels under the presence of security incidents such as malicious attacks.

Due to the significance of these communications networks and our dependability on them, cyber-attacks and malicious behaviors that attempt to damage their normal operation have become a paramount problem for our current lifestyle. As it is crucial for these communication networks to offer an acceptable service even under security incidents, we have to maximize their reliability and resilience. Although reliability and resilience are related concepts, they represent different and desirable aspects that communication networks should have under any type of threat. While reliability represents the ability of a network to operate satisfactorily in a timely manner, resilience deals with the ability of a network to recover from adversity. More specifically, the focus of this special issue is the study of the effect that malicious attacks have on the reliability of communication networks, and the proposal and evaluation of mechanisms to counter this effect, both at design and operation stages.

This special issue welcomes original and high-quality research articles as well as review articles that present the state-of-the-art research results and technologies enabling resilience and/or reliability in communication networks under security incidents.

Potential topics include but are not limited to the following:

- Impact of security incidents and malicious attacks in network reliability
- Design and evaluation of reliable communication networks which are resilient against cyber-attacks
- Trade-offs of reliability and resilience against security incidents in communication networks
- Survivability in critical networks infrastructures under cyber-attacks
- Resilience and reliability against security incidents in:
 - Software-defined networks (SDN)
 - Data centers
 - Wireless sensor networks and ad hoc networks
 - Content-oriented networks
 - Cloud computing
 - Fault-tolerant networks
 - IoT

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

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

Lead Guest Editor

Jose M. Gimenez-Guzman, University of Alcala, Alcala de Henares, Spain
josem.gimenez@uah.es

Guest Editors

Christian Callegari, Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Pisa, Italy
christian.callegari@iet.unipi.it

David Tipper, University of Pittsburgh, Pittsburgh, USA
dtipper@pitt.edu

Bernardo Alarcos Alcazar, University of Alcala, Alcala de Henares, Spain
bernardo.alarcos@uah.es

Submission Deadline

Friday, 10 May 2019

Publication Date

September 2019