ITU Journal
Future and evolving technologies

FREE I FAST I FOR ALL

The *ITU Journal on Future and Evolving Technologies (ITU J-FET)* is an international journal providing complete coverage of all communications and networking paradigms, free of charge for both readers and authors. The ITU Journal considers yet-to-be-published papers addressing fundamental and applied research. It shares new techniques and concepts, analyses and tutorials, and learnings from experiments and physical and simulated test beds. It also discusses the implications of the latest research results for policy and regulation, legal frameworks, and the economy and society. This publication builds bridges between disciplines, connects theory with application, and stimulates international dialogue. Its interdisciplinary approach reflects ITU's comprehensive field of interest and explores the convergence of ICT with other disciplines. The ITU Journal welcomes submissions at any time, on any topic within its scope.

Special issue on

AI-driven security in 5G and beyond

Call for papers

The significant advances in wireless networks in the past decade have made a variety of Internet of Things (IoT) use cases possible, greatly facilitating many operations in our daily lives. IoT is only expected to grow with 5G and beyond networks, which will primarily rely on software-defined networking (SDN) and network functions virtualization (NFV) for achieving the promised quality of service. The prevalence of IoT and the large attack surface that it has created calls for intelligent security solutions that achieve real-time, automated intrusion detection/mitigation, as well as authentication and data integrity preservation in these networks.

Artificial intelligence (AI) tools, especially machine learning (ML) and deep learning (DL), come to the rescue for achieving real-time analysis of the massive amounts of network traffic data generated in 5G and beyond networks to discover anomalies and cyber-attacks, as well as provide effective mechanisms for authentication and data integrity preservation. AI tools will also play an important role in optimizing the performance of these networks under strict security constraints, when combined with the power of network virtualization and network slicing technologies. Despite the high potential of creating self-managing networks with the power of AI, adversarial attacks on the utilized algorithms are an important factor to consider, which could lead to significant performance degradation and disruptions in network operation.

This special issue seeks novel contributions dealing with security issues in networking technologies in the 5G and beyond era through utilization of AI tools.

Suggested topics	
ML and DL-based based intrusion detection and prevention	• Anomaly detection in core and/or radio networks in 5G and beyond • Attack classification in core and/or radio networks in 5G and beyond • Intrusion detection/prevention in IoT networks • SDN and AI-based solutions for intrusion detection/prevention • Novel datasets for ML and DL-based intrusion detection in 5G and beyond
ML and DL-based authentication and integrity assurance	• ML and DL-based user equipment/network device/service authentication algorithms • ML and DL-based data integrity assurance algorithms
Federated learning for security	• Cyber threat intelligence • Federated ML/deep learning for anomaly detection • Federated ML/deep learning for attack classification • Blockchain-based federated learning for security
Adversarial ML in networks	• Adversarial attacks on ML-based approaches for network security and optimization • Techniques for mitigating adversarial attacks on networks
ML and DL-based network optimization with security constraints	• Placement optimization of security VNFs • Secure network slicing optimization • Intelligent forwarding with SDN

Keywords
Machine learning, network security, deep learning, wireless communications, intrusion detection, cyber security, 5G, 6G

Additional information
Please visit the ITU Journal website at: https://www.itu.int/en/journal/j-fet/Pages/default.aspx. Inquiries should be addressed to Alessia Magliarditi at: journal@itu.int.

Deadlines extended
Paper submission: 3 April 2023
Paper acceptance notification: 24 April 2023
Camera-ready paper submission: 15 May 2023

Paper submission
This special issue calls for original scientific papers. Submitted papers should not be under consideration for publication elsewhere. Submissions must be made electronically using EDAS: Editor's Assistant at: https://edas.info/N29174. Templates and guidelines can be found at: https://www.itu.int/en/journal/j-fet/Pages/submission-guidelines.aspx

Publication
Papers will be published on the ITU digital library.

Editor-in-Chief
Ian F. Akyildiz, Truva Inc., USA
(ian.akyildiz@itu.int)

Leading Guest Editor
Pelin Angin, Middle East Technical University, Turkey

Guest Editors
- Mohammad Hossein Anisi, University of Essex, UK
- Bharat Bhargava, Purdue University, USA
- Ganapathy Mani, Qualcomm, USA
- Ilsun You, Soonchunhyang University, Republic of Korea

Editorial Board
The list of the Editors is available at: https://www.itu.int/en/journal/j-fet/Pages/editorial-board.aspx