The 15th IEEE International Conference on Security of Information and Networks

Call for Special Session on Emerging trends of using AI/ML to mitigate cyber attacks in SDN

11-13 November 2022, Tunisia

http://www.sinconf.org/sin2022/

Organizing Committee

Honorary Chairs
Adel BOUHOULA , Tunisia

Conference Chair
Omar Cheikhrouhou, Tunisia

Conference Co-Chairs
Mohamed Abid, Tunisia.
Atilla Elçi, Turkey
Naghmeh Moradpoor, United Kingdom
Berna Ors Yalcin, Turkey
Oleg Makarevich, Russia
Pete Burnap, Wales
Manoj S. Gaur, India
Rajveer S. Shekhawat, India
Jaideep Vaidya, USA
Mehmet Orgun, Australia

Program Chair
Habib Youssef, Tunisia

Program Co-Chairs
Kais Loukil, Tunisia.
Olfa Gaddour, Tunisia
Andrei Petrovski, United Kingdom
Alexander Chefranov, TRNC
Maxim Anikeev, Germany
Philipp Reinecke, United Kingdom
Hossain Shahriar, USA
Vijay Laxmi, India
Behnam Rahnama, Iran
Josef Pieprzyk,CSIRO, Australia, Poland

Promotion Chair
Wassim Jmal, Tunisia

Promotion Co-Chairs
Habib M. Kammoun, Tunisia
Oussema Fitouri, Tunisia
Chakib Ghorbel, Tunisia
Xavier Bellekens, Scotland
Şerif Bahtiyar, Turkey
Tahir Sandıkkaya, Turkey
Rajan Shankaran, Australia
Manoj Kumar Bohra, India
Benjamin NGUYEN, France

Publication Chair
Mouna Baklouti, Tunisia

Local Arrangement Chair
Walid Hassairi, Tunisia

Advisory Committee Members
Imed Romdhani , United Kingdom
Anis Koubaa, KSA
Faouzi Zarai, Tunisia
Bart Preneel, Belgium
Bülent Örencik, Turkey
Cetin Kaya Koc, USA
Edward Dawson, Australia
Elisa Bertino, USA
N. Balakrishnan, India
Willy Susilo, Australia
Alexander Shelupanov, Russia

Software Defined Networking (SDN) is inherently vulnerable to several network attacks, especially the Distributed Denial of Service (DDoS). Those attacks are recognized as a major jeopardy for network performance and generally lead to a network failure. Indeed, cyber attacks can easily overload the controller processing capacity and flood switches flow-tables.

Mitigation of cyber attacks can no longer be done with conventional techniques due to the emergence of new threats and processes used to launch those attacks. Today, the migration from defensive strategies based on "react after the occurrence of attacks" to offensive strategies based on "predicting the occurrence of attacks" is compulsory. Henceforth, AI-assisted security is an emerging paradigm in providing and preserving safe networks.

This Special Session provides a forum for broad and diverse audiences to discuss recent advances, challenges, and opportunities at the nexus of AI, networking, and cyber-security. The aim of this special session is to encourage research in areas such as design of attack-mitigation approaches, AI-assisted techniques of attackdetection/classification/prevention and new ideas of self-healing networks.

Topics targeted by this special session include but are not limited to the following:

- Offensive Security paradigm
- AI-assisted security in SDN
- Prediction-based attack detection in SDN
- Classification-based attackdetection in SDN
- Reinforcement Learning (QL)-based attack mitigation in SDN
- Online attack mitigationin SDN
- Network Self-healing approaches in SDN

Special Session Organizers:

Ali El Kamel, Manel Majdoub, and Habib Youssef
PRINCE Research Laboratory, ISITComHammam Sousse, University of Sousse.

Deadlines:

- *Full Paper Submission: Septembre 15, 2022*
- *Notification of Acceptance: September 21, 2022*
- *Camera Ready Submission: October 11, 2022*

For any information, contact:
sinconf@sinconf.org