IEEE VTS
Connecting the Mobile World

IEEE VEHICULAR TECHNOLOGY Magazine
Connecting the Mobile World

Call for Papers
IEEE VT Magazine Special Issue on AI-Driven Cyber Security Threats to Future Networks

IMPORTANT DATES

Manuscript Submission By
6 January 2020

First Round Reviews
28 February 2019

Second Round Submission By
10 April 2020

Second Round Reviews and Final Decision**: 5 June 2020**

Publication
September 2020

GUEST EDITORS

Sidi-Mohammed Senouci
University of Burgundy, France
Sidi-Mohammed.Senouci@u-bourgogne.fr

Hichem Sedjelmaci
Orange Labs, France
hichem.sedjelmaci@orange.com

Chadi Assi
Concordia University Montreal, Canada
assi@ciise.concordia.ca

Jiajia Liu
Northwestern Polytechnical University, China
liujiajia@nwpu.edu.cn

Mubashir Husain Rehmani
Cork Institute of Technology, Ireland
mshrehmani@gmail.com

Elias Bou-Harb
Florida Atlantic University
ebouharb@fau.edu

5G and Beyond 5G (B5G) networks will support a variety of services and verticals (enhanced mobile broadband, health, industry 4.0, smart energy and automotive). These services, verticals and the critical components that compose 5G architecture (e.g., radio access, edge and core networks) face new cyber security risks and challenges.

A new generation of smart threats defined as Artificial Intelligence (AI)-attacks has emerged. These threats can utilize AI to attack 5G networks or services or hack the AI algorithms used by 5G components. In the first case, AI can be utilized to launch attacks against targets such as autonomous vehicles, drones or manufacturing machinery. In the second case, attackers hack the Machine Learning (ML) algorithms by modifying for instance the labels of ML's classification functions and altering the training data, which cause a decrease on the accuracy classification rate. These threats require a new era of cyber security approaches based on robust AI algorithms to protect future networks from AI-related attacks. Future solutions must consider 5G and B5G network constraints (e.g. overhead, latency, energy and bandwidth consumption).

In this special issue, we invite high-quality original submissions on AI-based solutions for cyber security in 5G and B5G networks. The topics of interest include, but are not limited to:

- AI-attacks against 5G and B5G networks
- AI modeling for network behavior in 5G and B5G networks
- Attacks detection and prediction based on deep and reinforcement learning in 5G and B5G networks
- Cyber protection based on advanced learning to secure 5G and B5G networks
- Cyber threats intelligence based on AI to secure 5G and B5G networks
- AI-cyber security approaches in virtualized environments
- Cyber security games to protect 5G and B5G services
- Lightweight AI-based cyber security to protect low-resources 5G and B5G services and devices (e.g. IoT devices)
- AI-cyber defense for 5G and B5G-based vertical applications

All manuscripts should contain state-of-the-art material presented in a tutorial or survey style, and must adhere to IEEE VTM guidelines: **http://ieee-vtm.org/submission.php**

Authors should submit their PDF manuscripts to **http://mc.manuscriptcentral.com/vtm-ieee**