Security and Communication Networks

Special Issue on

# Security Threats to Artificial Intelligence-Driven Wireless Communication Systems 2021

CALL FOR PAPERS

Due to the openness of wireless channels, wireless communication systems are extremely vulnerable to attacks, counterfeiting, and eavesdropping. With the widespread adoption of artificial intelligence (AI) technologies in fifth generation (5G) and beyond fifth generation (B5G) networks, AI-based attacks have emerged as new threats to wireless communication systems. Deep learning-based end-to-end communication systems are extremely susceptible to physical adversarial attacks which can cause a serious reduction in the accuracy of signal classification or radio modulation recognition.

Intelligent threats can utilise AI to attack future networks, related services, and applications that use deep learning algorithms where small disturbances can be easily designed and generated by attackers. However, researchers still need to consider how best to protect 5G and B5G networks from AI-related attacks. Furthermore, defense strategies of adversarial attacks for future communication systems are still underdeveloped and inefficient.

The aim of this Special Issue is to solicit original articles, as well as review articles, analysing the security threats, challenges, and mechanisms inherent in AI-driven wireless communication systems. Submissions discussing potential defense approaches, and strategies to combat intelligent attacks on such systems are particularly encouraged.

Potential topics include but are not limited to the following:

- Architectures, simulators, scenarios, and applications tuned to security and privacy issues for AI-driven wireless communication systems
- Adversarial attacks on AI-based signal classification or radio modulation recognition
- White-box or black-box-based attacks on signal/modulation classifiers
- Effective attacks detection and prediction based on deep learning techniques, e.g. autoencoder (AE), deep neural network (DNN), generative adversarial network (GAN) and deep reinforcement learning (DRL)
- Defense mechanisms and theories of adversarial attacks against end-to-end communication systems
- Adversarial modelling or adversarial deep learning for future wireless networks
- Security threats to 5G and B5G-based applications, services and IoT devices
- Defense strategies and solutions for AI-related attacks on wireless communication systems
- Robust algorithms to protect against AI-related attacks on wireless communication systems

Authors can submit their manuscripts through the Manuscript Tracking System at https://review.hindawi.com/submit?specialIssue=787821.

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

**Lead Guest Editor**
Huaming Wu, Tianjin University, Tianjin, China
*whming@tju.edu.cn*

**Guest Editors**
Xiaolong Xu, Nanjing University of Information Science and Technology, Nanjing, China
*njuxlxu@gmail.com*

Kaitai Liang, Delft University of Technology, Delft, Netherlands
*kaitai.liang@tudelft.nl*

Junqing Zhang, University of Liverpool, Liverpool, UK
*junqing.zhang@liverpool.ac.uk*

Yuan Yuan, Michigan State University, Michigan, USA
*yyuan@msu.edu*

**Submission Deadline**
Friday, 30 July 2021

**Publication Date**
December 2021