Sidi-Mohammed Senouci, Hichem Sedjelmaci, Jiajia Liu, Mubashir Husain Rehmani, and Elias Bou-Harb

AI-Driven Cybersecurity Threats to Future Networks

Future-generation networks (5G and beyond 5G) will include a variety of services for various verticals, such as enhanced mobile broadband, health monitoring, Industry 4.0, smart energy distribution, and automotive networks. These vertical services and the critical components that comprise 5G architecture (e.g., radio access and edge and core networks) exhibit several cybersecurity vulnerabilities that attract attackers to use all their capabilities to exploit and hence shut down these networks.

Recently, a new generation of smart threats, defined as *artificial intelligence* (*AI*) *attacks*, has appeared. These smart attacks either turn AI into weapons to attack 5G services or hack the AI algorithms used by 5G components. In the first misbehavior, attackers take advantage of AI's improved ability to launch lethal and stealthy threats against attractive targets, e.g., autonomous vehicles, drones, or manufacturing machinery. In the second misbehavior, attackers hack machine learning (ML) algorithms by modifying, for instance, the labels of the ML classification functions and altering the training data, causing a decrease in the accuracy of the classification rate.

Digital Object Identifier 10.1109/MVT.2020.3007981
Date of current version: 14 August 2020

THESE SMART ATTACKS EITHER TURN AI INTO WEAPONS TO ATTACK 5G SERVICES OR HACK THE AI ALGORITHMS USED BY 5G COMPONENTS.

A new era of cyberdefense approaches based on robust AI algorithms is under development to protect future networks from AI attacks. These AI security algorithms rely on human–ML (classification) interactions to accurately detect current and future smart AI attacks. Despite the accuracy detection exhibited by human–machine interaction, the network constraint of 5G architectures (such overhead, latency, energy, and bandwidth consumption) should be taken account during the deployment of AI cyberdefense techniques.

The special issue (SI) in this edition of *IEEE Vehicular Technology Magazine* aims to bring together researchers from academia and industry to share their vision of AI applications in a cybersecurity context and to present challenges and recent works and advances related to AI-based cybersecurity as applied to future networks. In response to the call for papers, we received over nine submissions. After a careful review process, two outstanding articles were selected for this SI, with the acceptance ratio lower than 25%. In addition, two additional open call articles in the area of security have been included. The articles in this SI are classified into two categories:

- AI-assisted cyber detection systems for future networks
- cyber protection based on ML for future networks.

The first article, "Physical-Layer Security for Vehicle-to-Everything Networks" by Rice et al., analyzes how physical layer security can help make vehicle-to-infrastructure and vehicle-to-vehicle networks more secure against eavesdropping. The article showcases a set of vehicle-to-everything experiments that demonstrate how finite block-length physical-layer security coding increases security while maintaining reliable communications. The authors also discuss fundamental tradeoffs in achieving both reliability and security through physical-layer efforts.

Vehicles are being transformed into information and computer technology-oriented machines. This helps expand vehicular applications and functionalities but also poses unforeseen challenges in a sector where safety is the priority. One of these challenges is security. "Protecting In-Vehicle Services: Security-Enabled SOME/IP Middleware" by Iorio et al. presents a framework

AI SECURITY ALGORITHMS RELY ON HUMAN–ML (CLASSIFICATION) INTERACTIONS TO ACCURATELY DETECT CURRENT AND FUTURE SMART AI ATTACKS.

to improve security for applications executed in vehicles based on the principle of defining exactly who can talk to whom. The proposed framework targets in-vehicle Ethernet-based communications and is integrated within the emerging scalable service-oriented middleware over IP (SOME/IP) middleware for in-vehicle communications. The authors validate the proposal in a proof of concept.

In "Detecting Fake Mobile Crowdsensing Tasks: Ensemble Methods Under Limited Data," Simsek et al. develop a security solution against fake tasks based on ML algorithms provided to a mobile crowdsensing system. Among the learning algorithms used to detect fake tasks are adaptive boosting for binary classification, gentle adaptive boosting, and random undersampling boosting. According to simulation results, GentleBoost-based ensemble learning can achieve high accuracy classification against fake tasks submitted to a crowdsensing system.

Finally, in "Artificial Intelligence Security in 5G Networks," Qiu et al. propose two approaches for adversarial examples based on a spatial–temporal estimation task. These adversarial examples include both white-box and black-box attacks. According to their experimental results, the authors prove that, in the 5G context, adversarial examples can successfully attack the security model based on deep learning algorithms.

Author Information

Sidi-Mohammed Senouci received his Ph.D. degree in computer science from the University of Paris XI and his HDR from the National Polytechnic Institute of Toulouse, France. From 2004 to 2010, he was a researcher with France Telecom R&D (Orange Labs), Lannion, France. Since 2010, he has been a professor at the Institut supérieur de l'automobile et des transports, Nevers, France, where he directs the DRIVE Laboratory. He holds seven international patents and has published his work in major conference proceedings and renowned journals.

Hichem Sedjelmaci is a senior research engineer in cybersecurity and artificial intelligence (AI) and project manager at Orange Labs, Lannion, France. He received his Ph.D. degree in telecommunication systems from Tlemcen University, Algeria, in 2013 and his HDR (in the scope of AI and cybersecurity) from the University of Burgundy, France, in 2019. He has published his work in major conference proceedings and premium journals. He holds eight international patents on topics related to cybersecurity and AI.

Jiajia Liu is a full professor with the School of Cybersecurity, Northwestern Polytechnical University, Xi'an, Shaanxi, China. He received the IEEE Vehicular Technology Society's Early Career Award in 2019, the IEEE Communications Society's Asia-Pacific Outstanding Young Researcher Award in 2017, and the IEEE Communications Society's Asia-Pacific Outstanding Paper Award in 2019. He is a Distinguished Lecturer of the IEEE Communications Society and the IEEE Vehicular Technology Society.

Mubashir Husain Rehmani received his B.Eng. degree in computer systems engineering from Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2004, his M.S. degree from the University of Paris XI in 2008, and his Ph.D. degree from the University Pierre and Marie Curie, Paris, in 2011. He is currently an assistant lecturer in the Department of Computer Science, Cork Institute of Technology, Ireland. He is a Member of the IEEE.

Elias Bou-Harb is currently associate director of the Cyber Center for Security and Analytics with the University of Texas at San Antonio (UTSA), where he leads university-wide innovative cybersecurity research, development, and training initiatives. He is also an associate professor in UTSA's Department of Information Systems and Cybersecurity, specializing in operational cybersecurity and data science as applicable to national security challenges. He received his Ph.D. degree from Concordia University, Montreal, Canada, and conducted postdoctoral training at Carnegie Mellon University, Pittsburgh, Pennsylvania.

VT