Cyber Security Based on Artificial Intelligence for Cyber-Physical Systems


Hichem Sedjelmaci


Fateh Guenab


Sidi-Mohammed Senouci


Hassnaa Moustafa


Jiajia Liu


Shuai Han

Cyber-physical systems (CPSs) have become very complex, more sophisticated, intelligent and autonomous. Examples of CPS include smart grid in the energy sector, smart factory and industry 4.0, intelligent transportation systems, healthcare and medical systems, and robotic systems. CPSs offer very complex interaction between heterogeneous cyber and physical components; additionally to this complexity, they are exposed to important disturbances due to unintentional and intentional events which make the prediction of their behaviors (categorized as "Normal" or "Faulty") a very difficult task. Meanwhile, cyber security for CPS is attracting the attention of research scientists in both industry and academia since the number of cyber-attacks have increased and their behaviors have become more sophisticated, commonly known as zero-day threats.

Conventional cyber security mechanisms, such as intrusion detection and prevention systems (IDS/IPS), and access control do not have the capability to detect, prevent and block this category of cyber-attacks since the zero-day threats exhibit an unknown misbehavior that are not defined in signatures' database of the security systems. Recently, a new era of cyber security mechanisms based on artificial intelligence (AI) are under development to protect CPSs from these zero-day attacks. In the context of cyber security, machine learning technologies are used to manage a huge amount of heterogeneous data that come from different sources of information with a goal of generating automatically different attack patents and hence predicting accurately the future attackers' misbehavior. Game-theoretic approaches have been used in the context of cyber defense to solve the decision-making issues (i.e., the suspect device is an attacker or not) and attack prediction. In decision-making issues, the cyber security game is used to study the interaction between the security agents (e.g., IDS and IPS) and their opponents (e.g. attackers) with a goal to determine the optimal decision making of security agents to classify the suspected opponent as attacker or not.

Preventing the occurrence of zero-day attacks requires the collaboration between different AI systems including machine learning and game theory, as well as security expert intervention. In fact, human intervention in decision-making leads to an improvement in attack detection since the purpose of human-machine interaction is to reduce the number of false positives.

Another example to illustrate the migration of security solutions to use more intelligent principles and technologies is identity management & access control (IAM), which switches from simple login/password checking to voice and facial recognition.

This Special Issue (SI) aims to bring together researchers from academic and industry to share their vision of AI application in the cyber security context, and present challenges and recent works and advances related to AI-based cyber security applied to CPSs. In response to the Call for Papers, we received over 40 paper submissions. After a careful review process, 10 outstanding articles have been selected for this SI.

The articles in this SI are classified into two categories:

- AI-assisted cyber defense to detect attackers targeting CPS.
- Cyber protection based on machine learning for CPS.

In "BLCS: Brain-Like based Distributed Control Security in Cyber Physical Systems," the authors propose a distributed control security architecture for fog radio and optical networks in CPSs. They investigate the functional entities of the security architecture and interworking procedure in the insecure control mode. According to the experiment results, the authors proved that malicious CPS nodes are detected with high accuracy, while packet loss, latency and blocking probability are reduced.

In "An Intelligent Edge Computing-Based Method to Counter Coupling Problems in Cyber-Physical Systems," the authors propose an AI method based on an edge computing system to protect the CPS from coupling problems and optimize the utilization of sensors. Based on a machine learning algorithm and edge computing system, the authors develop two buffer queues to reduce the coupling degree of the system in parallel. The experiment results demonstrate that the AI method based on an edge computing system decreases the cost of scheduling, increases resource utilization, and prolongs the lifetime of the CPS.

In "Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement?" the authors propose a security provisioning approach based on an artificial intelligence (AI) algorithm to achieve fast authentication and progressive authorization in large-scale Internet of Things (IoT) networks. In the simulation results, they prove the effective protection of IoT wireless communication against the cyber-attacks.

In "Toward Integrated Virtual Emotion System with AI Applicability for Secure CPS-enabled Smart Cities: AI-based Research Challenges and Security Issues," the authors present an integrated virtual emotion system based on an AI algorithm that treats the virtual emotion barrier, virtual emotion map, and virtual emotion block for securing CPS-enabled smart cities. Future work related to the AI-enabled virtual emotion system is discussed in this research work.

In "Learning-Assisted Secure End-to-End Network Slicing for Cyber-Physical Systems," the authors highlight the security issues of network slicing, study the machine learning solution to secure the slices from network attacks, and analyze the robustness of their solution against Denial-of-Service (DoS) attacks. The experiment result shows that the learning-security solution reduces the occurrence of DoS attacks targeting network slicing.

In "Machine Learning based Side-Channel Leakage Detection

in Electronic System-Level Synthesis," the authors propose a machine learning algorithm based on a clustering approach to achieve faster and more effective leakage detection executed by cyber-attacks in a CPS network. According to their simulation results, the proposed clustering-based leakage detection system exhibits high accuracy detection against network attacks.

In "Federated Learning for Data Privacy Preservation in Vehicular Cyber-Physical Systems," the authors focus to protect vehicular cyber physical systems against data leakage attacks. The proposed security system is based on a federated learning mechanism, which relies on two security phases to ensure privacy preserving, data transformation and collaborative data leakage detection. Numerical results show that the proposed security system mitigates effectively cyber-attacks targeting vehicular CPSs.

In "Reinforcement Learning Empowered IDPS for Vehicular Networks in Edge Computing," the authors propose an intrusion detection framework based on reinforcement learning algorithms to secure the vehicles' network from internal and external attacks. The main purpose of this work is to improve over the time both attacks detection and prevention decision as demonstrated in the experiment results.

In "Artificial Intelligent-based Distributed Belief Propagation and Recurrent Neural Network Algorithm for Wide-Area Monitoring Systems," the authors propose an area monitoring mechanism based on distributed belief propagation and a bi-directional recurrent neural network to protect the CPS network against GPS spoofing attacks. The proposed monitoring mechanism authenticates each received power by analyzing and evaluating the GPS timing error to detect malicious GPS signals and hence detect spoofing attacks. In the simulation results, the authors prove that their mechanism exhibits fast detection time and low timing error estimation accuracy.

In "Pseudonym Limitation for Privacy in Cooperative Transport Systems," the authors present an experimental study of data-set messages exchanged between vehicles and they have shown, under some conditions, that it is possible to identify drivers' behavior based only on data correlation between collected data messages, and hence the track of drivers is possible even when they use pseudonym changes.

Biographies

Hichem Sedjelmaci is a senior research engineer in cyber security and Artificial Intelligence (AI), and a projects manager at Orange Labs. Before joining Orange Labs, he was a research specialist in cyber security and AI at the Institute of Technological Research (IRT) SystemX, Paris saclay. From 2013 to 2016 he was a postdoc at DRIVE Lab, University of Burgundy, France. He received the Ph.D. degree in telecommunication systems from Tlemcen University, Algeria in 2013, and the HDR (in the scope of AI and cyber security) from the University of Burgundy, France in 2019. His research interests include vehicular networks, wireless sensor networks, unmanned aerial vehicles, 5G networks, security issues, game theory and machine learning. He has published his work in major IEEE conferences (ICC, GLOBECOM) and premium journals (IEEE transactions). He serves as a Guest Editor of premium journals, such ADHOC, *IEEE Network*, IEEE VTM and IEEE JSAC. He holds a couple of international patents on the topics of cyber security and AI. He has participated or still participates in several national and European-wide research projects. He also participates in mounting and piloting the R&D projects related to cyber security and AI.

Fateh Guenab is Cybersecurity Project Manager at Alstom. He received his Ph.D. degree in automatic control – fault tolerant control systems in February 2007 from Nancy University – France, and his Master degree in diagnosis and fault tolerant control systems in September 2003 from INPG (National Polytechnic Institute of Grenoble) – France. He has been participating in several French and European research projects. His research interests include safety and cybersecurity of industrial control systems.

Sidi-Mohammed Senouci received his Ph.D. in computer science in October 2003 from the University of Paris 6 and his HDR from INP Toulouse, France. From December 2004 to August 2010 he was a researcher at France Telecom R&D (Orange Labs) Lannion. Since September 2010, he has been a professor at ISAT, a major French post-graduate school located in Nevers, France, and part of the University of Bourgogne. Since October 2017, he has been the director of the laboratory DRIVE EA 1859 collocated in ISAT Nevers. He has participated or still participates in several national and European-wide research projects. Among them FP7 FOTsis, ITEA CarCoDe, ITEA FUSE-IT and FUI PARFAIT. He holds seven international patents on these topics and has published his work in major IEEE conferences and renowned journals. He was co-chair of the AHSN Symposium at IEEE Globecom 2011 and co-chair of the NGN Symposium at IEEE ICC'2012 and IEEE ICC'2017. He was vice-chair of the SAC symposium at IEEE Globecom2010, co-chair of the VCT Symposium at IEEE WCMC2010, and TPC co-chair of the VehiCom2009 Workshop. He also acted or still acts as a TPC member of different IFIP, ACM or IEEE conferences and workshops. He was the Chair of the IEEE ComSoc IIN Technical Committee, TCIIN (2014-2016). He serves as a Guest Editor of premium journals, such ADHOC journal, *IEEE Network Magazine*, *IEEE Access*, *IEEE Vehicular Technology Magazine*, *IEEE AHSN TC Newsletter* and the French journal REE. He is also a Member of IEEE and the Communications Society and an Expert Senior of the French society SEE (Society of Electricity and Electronics).

Hassnaa Moustafa, is a principal engineer at Intel Corporation, USA. Currently she is working on edge AI solutions across IoT segments and network and edge infrastructure. Previously at Intel, Hassnaa led car-to-cloud solutions for connected/autonomous vehicles, and connectivity technologies across IoT segments. Before joining Intel, Hassnaa was a senior R&D engineer at France Telecom (Orange Labs) in France, where she contributed to low cost wireless network solutions for emerging countries and led engineering efforts on personalization and context-aware video and multimedia services within the NGN effort. Hassnaa obtained her tenure in computer science from the University of Paris XI, her Ph.D. in computer and networks from Telecom Paris Tech and her Master degree in distributed systems from the University of Paris XI. Her broad experience covers IoT E2E network and services infrastructure, media networks, video delivery optimization, services personalization and content adaptation. She also worked for many years on ad hoc and vehicular network routing and AAA solutions. She contributed to the IETF standardization for 10 years and she is a senior IEEE member. Hassnaa has over 80 publications in international conferences and journals including IEEE and ACM. She has co-authored books published by the CRC press, she is a regular guest editor for several journals, and she is an active member in TPCs for IEEE and ACM conferences. She is also a regular co-chair for several IEEE workshops and conferences symposiums. Hassnaa has been involved in several European projects with a technical lead role and she has served as a consultant for the European Commission (EU) from 2008 until 2012 and contributed to defining the research agenda for Future Internet and Media Networks published in EU white papers.

Jiajia Liu [S'11, M'12, SM'15] was a full professor at the School of Cyber Engineering, Xidian University, from 2013 to 2018, and was the director of the Internet of Things Security Research Center, Xidian University from 2016 to 2018. Since January 2019, he has been a full professor at the School of Cybersecurity, Northwestern Polytechnical University. He has published more than 180 peer-reviewed papers in many high quality publications, including prestigious IEEE journals and conferences. He received the IEEE VTS Early Career Award in 2019, IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award in 2017, IEEE ComSoc Asia-Pacific Outstanding Paper Award in 2019, Niwa Yasujiro Outstanding Paper Award in 2012, Best Paper Awards from many international conferences including IEEE flagship events, such as IEEE GLOBECOM in 2016 and 2019, IEEE WCNC in 2012 and 2014, IEEE WiMob in 2019, IEEE IC-NIDC in 2018. He was also a recipient of the Tohoku University President Award 2013. His research interests cover a wide range of areas including intelligent and connected vehicles, mobile/edge/cloud computing and storage, Internet of Things security, wireless and mobile ad hoc networks, and space-air-ground integrated networks. He has been actively involved in society activities, such as serving as associate editor for *IEEE Transactions on Wireless Communications* (May 2018–present), *IEEE Transactions on Computers* (October 2015–June 2017) and *IEEE Transactions on Vehicular Technology* (January 2016 – present), editor for *IEEE Network* (July 2015–present), editor for *IEEE Transactions on Cognitive Communications and Networking* (January 2019–present), guest editors of top ranking international journals such as *IEEE Transactions on Emerging Topics in Computing* (TETC), *IEEE Network Magazine*, *IEEE Internet of Things (IoT) Journal*, etc., and serving on technical program committees of numerous international conferences such as the leading symposium co-chair of the AHSN Symposium for GLOBECOM 2017, CRN Symposium for ICC 2018, and AHSN Symposium for ICC 2019. He is the Vice Chair of IEEE AHSN TC, and is a Distinguished Lecturer of the IEEE Communications Society.

Shuai Han [S'11, M'12, SM'17] is currently a professor in the Department of Electronics and Communication Engineering, Harbin Institute of Technology. His research interests include wireless sensor networks, wireless communications, the global navigation satellite system and indoor location. Over his academic career, his students and he have contributed in various fields in wireless networks and wireless positioning. His IEEE ICC2017 paper on wireless security was a candidate for best paper. His WiCON2017 paper on Full Duplex Decode-and-Forward Cooperative Relay System was the best paper. As PI, he has four national grants and more than 10 industrial grants on wireless networks and positioning. Also, he has participated in several major projects at the national level in China. He is an associate editor of *IEEE Access*, *Journal of Communications and Information Networks* (JCIN), and has served as a guest editor for many IEEE magazines and journals. He has served as a co-chair for technical symposia of international conferences such as Globecom 2019, ICC 2018, and VTC FALL 2016. He has also served as the TPC Chair for several international conferences, including the AICON2019 and MLICOM2018. He is the Vice Chair of the IEEE Harbin ComSoc Chapter and Vice Chair of the IEEE Harbin VTS Chapter.