Guest Editorial: Special Issue on Internet of Things for Industrial Security for Smart Cities

MORE than half of the world's current population resides in urban areas to compare to just 30% in the 1950s. The process of urbanization leads to exurban sprawl, the formation of slums, scattered workplaces, and aging infrastructure. These may cause huge inefficiencies in energy use, traffic, governance, waste management, and pollution, among others. To overcome these social, economic, and environmental challenges, public and private sectors invest heavily in smart city technologies. However, the risks of using smart technologies due to security breaches and cyberattacks in critical sectors should be well addressed.

Attackers would set their sights on smart cities for a number of reasons. Malicious individuals may consider smart cities as playgrounds where they can test their hacking skills by toying with available technologies for personal satisfaction. For cybercriminals, the interconnectedness of devices and systems in a smart city could be manipulated for any possible unauthorized access of personal assets, sensitive data, and financial properties, causing loss/damage to the public. State-sponsored actors could also abuse the pervasiveness of smart city technologies to launch their own espionage or hacktivist campaigns. In some very extreme cases, smart implementations may even be exploited for acts of terror. Therefore, researchers and engineers should provide actionable solutions and methods to help local governments and urban developers design more secure smart cities.

The aim of this special issue is to foster novel and multidisciplinary approaches that improve industrial security for smart cities and networked infrastructure by taking into consideration various challenges faced by industrial applications.

The response to our call for this special issue was overwhelming, as we received in total 163 submissions from around the world. During the review process, each article was assigned to and reviewed by at least three experts in the field, with a rigorous multiround review process. Thanks to the great support from the Editor-in-Chief, Prof. Honggang Wang, and the dedicated work of numerous reviewers, we were able to accept 28 excellent articles covering various topics in industrial and smart city security. In the following, we will introduce these articles and highlight their main contributions.

In the first article "An efficient and secure multidimensional data aggregation for fog-computing-based smart grid," Merad-Boudia and Senouci proposed an efficient and secure multidimensional data aggregation scheme, named ESMA. Unlike existing schemes, the multidimensional data in ESMA is structured and then encrypted into a single Paillier ciphertext and the data are efficiently decrypted as well.

In the article "Partial-DF full-duplex D2D-NOMA systems for IoT with/without an eavesdropper," Duan *et al.* investigated a cooperative full-duplex device-to-device system with nonorthogonal multiple access (NOMA) and partial decode-and-forward (PDF).

In the article "AI and machine learning for industrial security with level discovery method," Jiang *et al.* proposed a level discovery method for employees extracted from their records using mobile phones, named LDME. The calling behavior between employees is expressed as several weighted directed complex networks, LDME represents edges in these weighted directed complex networks as vectors to exact both direction and weight information of the edges.

In the article "Privacy-preserving federated learning framework based on chained secure multiparty computing," Li *et al.* proposed a novel privacy-preserving federated learning framework based on an innovative chained secure multiparty computing technique, named Chain-PPFL.

In the article "Toward effective intrusion detection using log-cosh conditional variational autoencoder," Xu *et al.* proposed a novel deep-learning-based intrusion detection method, named log-cosh conditional variational autoencoder (LCVAE). This is an intelligent method to detect intrusion.

In the article "Recognizing influential nodes in social networks with controllability and observability," Huang *et al.* examined an intelligent way to automatically recognize the influence of such nodes. Motivated by the concepts of system controllability and observability from control theory, the authors introduced a novel method to evaluate nodes from two different aspects, namely: 1) the ability to "observe" information on the network (i.e., observability) and 2) the ability to propagate information to other nodes (i.e., controllability).

In the article "An architecture for IoT-enabled smart transportation security system: A geospatial approach," Zhang *et al.* applied geospatial modeling analyses to develop an architecture for smart transportation security systems (STSS).

In the article "SeizSClas: An efficient and secure Internet-of-Things-based EEG classifier," Singh *et al.* tried to bridge the gap and presented a privacy-preserving secure technique for brain signal classification.

Digital Object Identifier 10.1109/JIOT.2021.3067077

In the article "A survey on supply chain security: Application areas, security threats, and solution architectures," Hassija *et al.* discussed the supply chain's security-critical application areas and presented a detailed survey of the security issues in the existing supply chain infrastructure.

In the article "Intrusion detection for cyber–physical systems using generative adversarial networks in fog environment," Freitas de Araujo-Filho *et al.* proposed an encoder that accelerates the reconstruction loss computation for cyber–physical systems.

In the article "Voting-based decentralized consensus design for improving the efficiency and security of consortium blockchain," Sun *et al.* introduced the proof of assets and proof of reputation to design a voting-based decentralized consensus algorithm (VDC) for consortium blockchain.

In the article "Industrial security solution for virtual reality," Lv *et al.* proposed a class and sample weighted C-SVM algorithm (CSWC-SVM) to protect industrial safety.

In the article "A quantitative study of DDoS and E-DDoS attacks on WiFi smart home devices," Tushir *et al.* quantified the impact of Distributed Denial of Service (DDoS) and energy-oriented DDoS attacks on various smart home devices and explored comprehensive reasons for such impact from the attacker, WiFi access point (AP), and victim device perspectives.

In the article "Distributed variational Bayes-based in-network security for the Internet of Things," He *et al.* designed a machine-learning-based in-network DDoS detection framework. They implemented the lightweight variational Bayes algorithm in each switch to detect the anomaly traffic. Besides, considering the shortage of training data in each switch, a centralized platform was introduced to synchronize parameters.

In the article "Blockchain for secure-GaS: Blockchain-powered secure natural gas IoT system with AI-enabled gas prediction and transaction in smart city," Xiao *et al.* introduced artificial intelligence (AI) and blockchain technologies and constructed AI-enabled and blockchain-powered natural gas IoT in smart cities.

In the article "Covert communication in relay-assisted IoT systems," Gao *et al.* proposed two relay selection schemes: one is the random selection and another is the superior-link selection to provide ubiquitous wireless connectivity for smart cities.

In the article "Confused-modulo-projection-based somewhat homomorphic encryption—Cryptosystem, library, and applications on secure smart cities," Jin *et al.* designed and implemented a blind computing scheme of accelerated version based on batch processing technology to improve efficiency.

In the article "Adaptive square attack: Fooling autonomous cars with adversarial traffic signs," Li *et al.* proposed a novel attacking method dubbed adaptive square attack (ASA) that can detect black-box attacks.

In the article "Deep anomaly detection for time-series data in Industrial IoT: A communication-efficient on-device federated learning approach," Liu *et al.* proposed a new communication-efficient on-device federated learning-based deep anomaly detection framework for sensing time-series data in IIoT.

In the article "Enterprise integration patterns in SDN: A reliable, fault-tolerant communication framework," Rauf *et al.* demonstrated through simulations how the proposed integrated design can be helpful in improving the security, efficiency, and reliability aspects of the enterprise network. As proof of concept, the authors also discussed the deployment of the proposed framework in IoT-based smart cities.

In the article "Attribute-based access control for smart cities: A smart-contract-driven framework," Zhang *et al.* proposed a distributed and reliable access control framework for smart cities by combining the blockchain smart contract technology and the attribute-based access control (ABAC) model.

In the article "Secrecy enhancing of SSK systems for IoT applications in smart cities," Huang *et al.* proposed a secrecy-enhancing space shift keying (SSK) scheme for IoT applications by applying security technologies in the physical layer wherein the number of transmit antennas is arbitrary rather than the value of power of two.

In the article "Industrial Internet of Things security enhanced with deep learning approaches for smart cities," Magaia *et al.* presented an IIoT concept and applications for smart cities, while also presenting security challenges faced by this emerging area.

In the article "Enabling drones in the Internet of Things with decentralized blockchain-based security," Yazdinejad *et al.* introduced a secure authentication model with low latency for drones in smart cities that leverages blockchain technology.

In the article "Hierarchical prediction based on network-representation-learning-enhanced clustering for bike-sharing system in smart city," Yang *et al.* proposed a hierarchical model for sharing bike prediction, which can predict the number of rents/returns of each bike-sharing station to achieve resource redistribution.

In the article "Efficient and traceable patient health data search system for hospital management in smart cities," Zhou *et al.* proposed a new traceable patient health data search system for hospital management in smart cities.

In the article "ATTDC: An active and traceable trust data collection scheme for industrial security in smart cities," Shen *et al.* proposed an active and traceable trust-based data collection scheme to collect trust data in Internet of Things.

In the article "I-SEE: Intelligent, secure, and energy-efficient techniques for medical data transmission using deep reinforcement learning," Allahham *et al.* proposed a practical secrecy metric, namely, the secrecy outage probability (SOP), along with the adaptive compression at the edge for providing a secure solution for health monitoring applications.

We would like to express our sincere gratitude to all the authors for submitting their papers and to the reviewers for their valuable comments and suggestions that significantly enhanced the quality of these articles. We are also grateful to Prof. H. Wang, the Editor-in-Chief of IEEE INTERNET OF THINGS JOURNAL, for his great support throughout the whole review and publication process of this special issue, and, of course, all the editorial staff. We hope that this special issue will serve as a useful reference for researchers, scientists, engineers, and academics in the field of industrial security of smart cities

HUIMIN LU, *Guest Editor*
School of Engineering
Kyushu Institute of Technology
Kitakyushu 804-8550, Japan

PIN-HAN HO, *Guest Editor*
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, ON N2L 3G1, Canada

MOHSEN GUIZANI, *Guest Editor*
College of Engineering
Qatar University
Doha, Qatar