Guest Editorial
IoT Systems for Extreme Environments

THE DEPLOYMENT of Internet of Things (IoT) systems spans a large variety of applications, each with unique requirements. Many of these applications relate to the management of various cyber–physical systems, including road and rail traffic, electricity, water, food/goods transportation and storage, smart building management, crime/safety management, underwater systems, etc. Within this context, a growing concern is the deployment of IoT systems in extreme environments which may occur either because of the nature of the application or due to external factors. Some prominent examples of the former are 1) the IoT deployments in hazardous environments such as management of chemical or nuclear plants, management of underwater oil/gas infrastructure, mining operations, etc.; 2) IoT systems deployed specifically to manage accidents and disasters; and 3) IoT systems deployed in arctic/antarctic regions where they routinely experience extreme levels of changes in terms of temperature, wind conditions, sunlight availability, compression, etc. Such IoT systems generally are designed to specifically operate in the challenging environment they must operate in, and thus may be expected to be rather robust. However, the IoT systems designed to manage the physical infrastructures such as those in urban settings may also need to handle unprecedented and unexpected stresses due to the worldwide phenomena of aging physical infrastructure, demand that far exceeds the designed capacity, and increasingly extreme operating conditions due to climate change. This special issue covers all such scenarios and thus represents a vast and rich area for innovations.

The IoT systems being deployed around the world in smart cities and other environments should anticipate and plan for operation in stressed environments. The robustness/resilience scenarios of interest in such environments are usually neither catastrophic nor random but may suffer from varying degrees of area damage relatively frequently. Thus, the key challenge is to assess damage effectively and with minimal manual involvement and accordingly configure or augment the system before, during, and after the event, to minimize service degradation, maximize coverage, and optimize the services offered. Collaboration across IoT systems potentially owned, and operated by different parties can help address this issue but must cope with issues of privacy, security, interoperability, and cross-party visibility. Furthermore, the situational understanding, which is increasingly based on video and other types of rich monitoring, is essential to assess the damage, dispatch work crews as needed, provide acceptable service and coverage, avoid conflicts and other undesirable behavior, and handle tradeoff between the information sharing and the privacy/security needs. Finally, both direct and side-channel attacks enabled by increasingly automated control and operation continue to make the security, privacy, and resilience of IoT systems even more important, especially in extreme environments.

We received a total of 56 original submissions from various institutions worldwide. Following a rigorous review process, 20 articles have been accepted and are included in this special issue of the IEEE INTERNET OF THINGS JOURNAL. These papers cover a broad range of issues and topic areas. We roughly divided them into the following four categories: 1) data collection and curation challenges; 2) network operations and management; 3) management of specific cyber–physical Systems; and 4) ensuring security and privacy in extreme environments. In the following, we introduce the articles in each area and highlight their main contributions.

I. DATA COLLECTION AND CURATION

This category consists of five articles on various aspects of data collection and curation for extreme environments and includes the issues of data imputation, data balancing, and data restoration. The article by Adhikari et al. [A1] discusses the challenge of imputing missing data in multivariate time-series data generated by IoT systems, especially in cases of extreme missing gaps and rates. The proposed solution utilizes techniques, such as multivariate variables, correlation, data fusion, regression, and multiple imputations. Extensive experiments with extreme missing gaps and rates ranging from 10% to 90% on sensor-generated data demonstrate that the proposed technique outperforms baseline techniques in preserving pattern, structure, and trend, even in scenarios with 90% extreme missing gaps and missing rates.

The article by Chen and Wu [A2] proposes collaborative filtering based on scaled lifted augmented half quadratic functions to address the problem of excessive sensitivity of traditional norms to outliers. The approach introduces auxiliary variables to absorb varying levels of data corruption and scaled reweighting forms to enhance resilience against oversensitivity. Experiments on open datasets demonstrate that the proposed method achieves better recoverability than baselines under different data corruption conditions, confirming its effectiveness.

The article by Cui et al. [A3] addresses the challenge of ensuring the stable operation of IoT systems in extreme environments, particularly in infrastructures like energy, aerospace,

Digital Object Identifier 10.1109/JIOT.2023.3339396

and healthcare. It highlights the vulnerability of resource-constrained devices to malware due to complex operating conditions and infrequent maintenance, posing risks of system failure or information leakage. To tackle these issues, the article utilizes a many-objective evolutionary algorithm to balance data space in different dimensions, including category and architectural distribution. Experimental results on IoT malware datasets demonstrate that MODSC effectively improves cross-architectural generalization while maintaining high confidence levels compared to popular data processing methods.

The article by Fu et al. [A4] discusses sparse mobile crowdsensing (SMCS) as a solution for large-scale data sensing in IoT systems by incorporating area constraints, truthful worker recruitment, and sensing map recovery. The scheme emphasizes the importance of areas based on historical data differences, identifies trustworthy workers using the truthful upper confidence bound algorithm, and employs the deep matrix factorization algorithm to infer unsensed data. Experimental results based on the China air quality dataset confirm the effectiveness of the proposed scheme in improving the platform's total profit.

The article by Li et al. [A5] discusses challenges in restoring imagery captured in extreme underwater environments, such as blurred details and color distortion. Existing restoration techniques often oversimplify by using static attenuation coefficients, leading to inconsistent results. To address this, the article introduces scene-depth fusion that dynamically considers the spectral decay of light underwater, providing a refined attenuation coefficient tailored to the specific scene. The method employs quadtree decomposition and depth mapping for precise localization, resulting in a more accurate transmission map. Experimental results demonstrate the system's effectiveness in addressing issues like blurred details and chromatic anomalies, outperforming existing methodologies in finesse and accuracy in challenging underwater conditions.

II. Network Operation and Management

This category contains five articles on such topics as multicasting, routing, offloading, threat detection, and management of distributed workflows. The article by Chen et al. [A6] discusses the challenges in transmitting large volumes of sensing data in maritime environments, highlighting issues with satellite links and traditional unicast transmission. It proposes BOOM, a bottleneck-aware opportunistic multicast strategy for efficient data delivery in maritime scenarios. BOOM considers the influence of bottleneck nodes and broadcasting rates, with adaptability to extreme conditions like storms and typhoons. Real-world experiments show that BOOM significantly reduces transmission latency, up to 59% in dense sensor scenarios. Simulation results demonstrate BOOM's superiority over other algorithms in completion time, particularly in sparse and dense sensor environments, with improvements of up to 49%.

The article by Verma et al. [A7] introduces AGRIC, an AI-based green routing system designed for industrial cyber–physical systems. It employs a novel AI-inspired extended spotted hyena Levy flight optimization (ESHLFO) algorithm for the election of cluster heads (CHs) in cluster-based routing. To address the energy hole problem, the study incorporates four energy-unlimited data collection nodes at the network periphery. The experimental results showcase that AGRIC improves network longevity and performance, with notable enhancements in stability, throughput, and remaining energy, serving as crucial performance indicators.

The article by Adil et al. [A8] discusses improved routing protocol for ad hoc networks by integrating destination-sequenced distance-vector (DSDV), which is used for routing information updates, and deep Q-learning for next-hop selection based on reward functions. This approach aims to minimize packet loss, congestion, end-to-end delay, and communication cost while improving Quality of Service (QoS) in extreme environments. Simulations indicate significant improvements in performance metrics compared to existing schemes.

The article by Kim et al. [A9] explores the use of unmanned aerial vehicle (UAV)-mounted intelligent reflecting surfaces (IRSs) in mmWave and THz communication systems. The focus is on establishing secure offloading systems for ground users through the assistance of the UAV-mounted IRS. The goal is to minimize the total energy consumption of battery-limited ground user devices while ensuring secure offloading and operability of the UAV-mounted IRS. The optimization involves adjusting the transmit power, trajectory, and phase shift matrix of the UAV-mounted IRS, as well as the offloading ratio between local execution and edge computing using successive convex approximation (SCA) algorithms. Numerical results indicate significant energy savings compared to local execution and partial optimizations.

The article by Amjad et al. [A10] highlights the challenge of efficiently utilizing IoT resources considering factors like location and battery life for comprehensive situational understanding, particularly in emergencies. The proposed dynamic approach orchestrates and manages distributed workflow applications across cloud data centers, servers, and IoT devices at the network edge. Specifically designed for adaptive and knowledge-driven business process workflows, the approach proves effective and resilient to situational changes, as demonstrated in a comprehensive empirical evaluation.

III. Management of Specific Cyber–Physical Systems

This category also consists of six articles on the important topics of landslide detection, aquatic ecosystem monitoring, flood risk evaluation, bearing fault diagnosis, soil stability prediction, and prediction of power generation. The article by Gidon et al. [A11] introduces a bidirectional long short-term memory (LSTM) model for landslide detection, focusing on Mawiongrim, Meghalaya, India, an active landslide zone. The bidirectional LSTM captures temporal patterns from various landslide-related characteristics, including topography, rainfall, hydrological, and soil properties. Results indicate that the proposed model achieves higher accuracy and lower error rates compared to other models, offering real-time warning capabilities for early landslide detection. The research also

highlights the significance of prediction models for matric suction and groundwater level in determining slope stability.

The article by de Araújo et al. [A12] introduces the OpenBoat system architecture for AI-enabled sailboats with autonomous environment monitoring and presents the F-Boat, a fully functional prototype built with commercial off-the-shelf components. F-Boat includes low-level control strategies, communication infrastructure, edge computing with AI acceleration, and modular support for application-specific monitoring systems. Field experiments in Guanabara Bay, Brazil, demonstrate the prototype's functionalities and the AI capabilities of the proposed architecture under extreme conditions.

The article by Ahmed et al. [A13] develops DeepLab, an algorithm for deep learning (DL) from satellite images for flood detection. DeepLab uses a convolutional neural network and is trained on extensive satellite images with ground truth labels, achieving a high accuracy of 87% in segmentation, outperforming state-of-the-art methods. The proposed system combines AI-based flood detection with meteorological forecasts and ground-based sensors, offering comprehensive flood monitoring for early warning and effective emergency response.

The article by Hu et al. [A14] discusses the challenges in bearing fault diagnosis models related to small sample sizes of faulty data in extreme environments. To address this, a real-time bearing fault diagnosis model, named RBFDSCA, is proposed, by making use of a Siamese network and convolutional autoencoder. The model is designed to learn effectively from limited faulty data. Utilizing an Industrial IoT (IIoT) platform for data collection and analysis, RBFDSCA constructs a Siamese convolutional autoencoder with positive and negative feature extraction networks. The model achieves high performance on a real bearing dataset, confirming its effectiveness in addressing the challenges of small sample sizes in bearing fault diagnosis.

The article by Nandy et al. [A15] addresses the need to continuously analyze slope stability, considering changing geospatial and geotechnical parameters. To monitor immediate changes, it uses a Fusion-Based Bag-of-Neural Network (FuBoNN) model for predicting the Factor of Safety (FoS). The relationship between environmental parameters and FOS is acknowledged as nonlinear and complex. The FuBoNN model, utilizing a rich dataset created by fusing laboratory data, demonstrates a 0.3% error in predicting multiple categories of FOS. Compared to standard machine learning models, the proposed approach exhibits a 2.5% improved prediction accuracy, highlighting its efficiency in addressing slope stability challenges.

The article by Satpathy et al. [A16] proposes quantum algorithms to forecast daily power generation, aiding energy organizations in making real-time decisions to save energy and costs in IoT-extreme environments. Quantum computers, leveraging properties like superposition and entanglement, offer superior computational performance with lower energy consumption than conventional computers. The article explores various quantum machine learning algorithms on datasets related to IoT extreme environments, showing that they outperform classical methods in accuracy.

IV. Ensuring Security in Extreme Environments

This category contains four articles concerning security issues for satellite communications (Satcoms), Internet of Vehicles (IoV), energy-constrained IoT devices, and data collection in disaster scenarios. The article by Salim et al. [A17] highlights the vulnerability of Satcoms to cyberattacks and the lack of equipped policies to address these challenges. In response, the article proposes a comprehensive deep federated learning (DFL)-based threat detection model for proactive intrusion recognition in Satcoms networks. The model incorporates a data-level preprocessing (DLP) mechanism to conceal original data and executes Federated Learning rounds on a deep autoencoder. Experimental results show that the proposed model surpasses classic/centralized learning versions in terms of protecting local data privacy and achieving optimal accuracy for attack detection. Additionally, the model, using differential privacy-based DLP, demonstrates high accuracy and enhanced privacy over the training data.

The article by Xu et al. [A18] discusses the challenges in implementing a ranked search system for IoV communication using searchable encryption (SE) over cloud infrastructure. The paper presents a search scheme that uses an encrypted index tree structure for multikeyword ranked retrieval and dynamic updating in IoV, along with a greedy breadth-first search for efficient sublinear search. The authors show via security analysis and experimental simulation that their system ensures user privacy and acceptable efficiency.

The article by Zhang et al. [A19] proposes to combine blockchain and DL to enhance IoT security. It introduces a Zero-Knowledge Proof-of-Learning (ZPoL) consensus approach, which replaces the traditional Proof of Work (PoW) with the training of a DL model. Additionally, the paper proposes an incentive mechanism based on a two-stage Stackelberg game to encourage resource-constrained IoT devices to participate in improving the quality of learning. The effectiveness of the mechanism in reducing communication, computation, and storage costs is shown through simulations and experiments.

The article by Jiang et al. [A20] proposes mobile crowdsourcing-assisted IoT systems for real-time data collection in disaster scenarios. It suggests a re-encryption mechanism for access authorization and encrypted task distribution through the cloud. It also proposes a mechanism to enhance the verifiability and reputability of reencrypted ciphertext under an untrusted cloud setting.

While these 20 accepted papers represent significant contributions to various aspects of IoT systems operating in extreme environments, numerous challenges persist, given the vast scope of the problem. We also believe that as the stress on existing physical infrastructures increases and newer, more complex infrastructures are deployed, many issues related to handling extreme situations—such as harsh operating environments, the necessity to continue operating aging infrastructures

due to economic limitations, usage beyond designed capacity due to increasing urban populations, heightened stresses due to climate change, and sophisticated attacks facilitated by increasingly automated IoT systems—will become even more critical in the future. We hope that the articles in this special issue will inspire further exploration of these complex problems.

Finally, as guest editors, we would like to convey our appreciation to all of the authors who submitted their work to this special issue and congratulate those whose work appears here. Our gratitude extends to a large number of anonymous reviewers whose insightful feedback not only assisted authors in enhancing their work but also facilitated our informed selection of the accepted articles. We would like to particularly thank Prof. Nei Kato, the Editor-in-Chief (EiC) of the IEEE INTERNET OF THINGS JOURNAL and his staff, for constant support and advice in making this special issue possible. We would also like to thank the former EiC Prof. Honggang Wang for providing us the opportunity to organize this special issue.

APPENDIX: RELATED ARTICLES

[A1] D. Adhikari et al., "A lightweight-window-portion-based multiple imputation for extreme missing gaps in IoT systems," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3676–3689, Feb. 1, 2024.

[A2] B.-W. Chen and Y.-H. Wu, "Partially observed visual IoT data reconstruction based on robust half-quadratic collaborative filtering," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3690–3701, Feb. 1, 2024.

[A3] Z. Cui, Z. Zhang, Z. Zhang, W. Zhang, and J. Chen, "MODSC: Many-objective-optimization-driven data-balancing strategy in cross-architectural malware classification for extreme IoT," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3702–3710, Feb. 1, 2024.

[A4] X. Fu, A. Liu, N. N. Xiong, T. Wang, and S. Zhang, "ATWR-SMR: An area-constrained truthful-worker-recruitment-based sensing map recovery scheme for sparse MCS in extreme-environment Internet of Things," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3711–3724, Feb. 1, 2024.

[A5] Y. Li, X. Zhu, Y. Zheng, H. Lu, J. Li, and Z. Shen, "Underwater visibility enhancement IoT system in extreme environment," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3725–3732, Feb. 1, 2024.

[A6] X. Chen et al., "BOOM: Bottleneck-aware opportunistic multicast strategy for cooperative maritime sensing," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3733–3748, Feb. 1, 2024.

[A7] S. Verma, S. Kaur, S. Garg, A. K. Sharma, and M. Alrashoud, "AGRIC: Artificial-intelligence-based green routing for industrial cyber–physical system pertaining to extreme environment," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3749–3756, Feb. 1, 2024.

[A8] M. Adil, M. Usman, M. A. Jan, H. Abulkasim, A. Farouk, and Z. Jin, "An improved congestion-controlled routing protocol for IoT applications in extreme environments," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3757–3767, Feb. 1, 2024.

[A9] D. Kim, S. Jeong, and J. Kang, "Energy-efficient secure offloading system designed via UAV-mounted intelligent reflecting surface for resilience enhancement," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3768–3778, Feb. 1, 2024.

[A10] S. Amjad et al., "Orchestration and management of adaptive IoT-centric distributed applications," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3779–3791, Feb. 1, 2024.

[A11] J. S. Gidon, J. Borah, S. Sahoo, S. Majumdar, and M. Fujita, "Bidirectional LSTM model for accurate and real-time landslide detection: A case study in Mawiongrim, Meghalaya, India," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3792–3800, Feb. 1, 2024.

[A12] A. P. D. Araújo et al., "General system architecture and COTS prototyping of an AIoT-enabled sailboat for autonomous aquatic ecosystem monitoring," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3801–3811, Feb. 1, 2024.

[A13] I. Ahmed, M. Ahmad, G. Jeon, and A. Chehri, "An Internet of Things and AI-powered framework for long-term flood risk evaluation," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3812–3819, Feb. 1, 2024.

[A14] H.-X. Hu, C. Cao, Q. Hu, Y. Zhang, and Z.-Z. Lin, "A real-time bearing fault diagnosis model based on Siamese convolutional autoencoder in Industrial Internet of Things," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3820–3831, Feb. 1, 2024.

[A15] S. Nandy, M. Adhikari, A. Ray, R. Rai, and T. N. Singh, "Edge-centric intelligent early warning system for residual soil stability prediction in slope," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3832–3839, Feb. 1, 2024.

[A16] S. K. Satpathy, V. Vibhu, B. K. Behera, S. Al-Kuwari, S. Mumtaz, and A. Farouk, "Analysis of quantum machine learning algorithms in noisy channels for classification tasks in the IoT extreme environment," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3840–3852, Feb. 1, 2024.

[A17] S. Salim, N. Moustafa, M. Hassanian, D. Ormod, and J. Slay, "Deep-federated-learning-based threat detection model for extreme satellite communications," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3853–3867, Feb. 1, 2024.

[A18] D. Xu, C. Peng, W. Wang, K. Dev, S. A. Khowaja, and Y. Tian, "Multikeyword-ranked search scheme supporting extreme environments for Internet of Vehicles," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3868–3880, Feb. 1, 2024.

[A19] H. Zhang, J. Wu, X. Lin, A. K. Bashir, and Y. D. Al-Otaibi, "Integrating blockchain and deep learning into extremely resource-constrained IoT: An energy-saving zero-knowledge PoL approach," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3881–3895, Feb. 1, 2024.

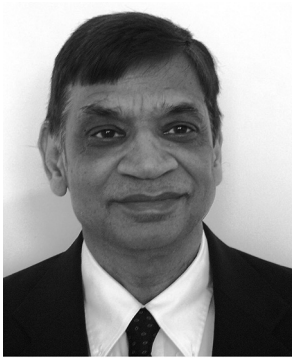
[A20] L. Jiang, M. Alazab, and Z. Qin, "Secure task distribution with verifiable re-encryption in mobile-crowdsensing-assisted emergency IoT system," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3896–3908, Feb. 1, 2024.

KRISHNA KANT, *Guest Editor*
Department of Computer and Information Sciences
Temple University
Philadelphia, PA 19122 USA

ALIREZA JOLFAEI, *Guest Editor*
College of Science and Engineering
Flinders University
Tonsley, SA 5042, Australia

KLAUS MOESSNER, *Guest Editor*
Communications Engineering Department
University of Technology Chemnitz
09111 Chemnitz, Germany

Institute for Communication Systems
University of Surrey
GU2 7XH Guildford, U.K.



Krishna Kant (Fellow, IEEE) received the Ph.D. degree in mathematical sciences from the University of Texas at Dallas, Richardson, TX, USA, in 1981.

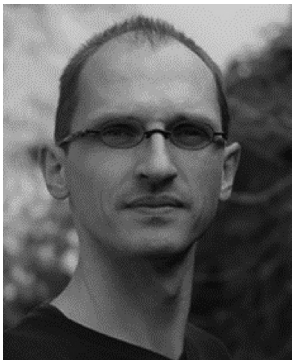
He is currently a Professor with the Computer and Information Science Department, Temple University, Philadelphia, PA, USA, where he directs the IUCRC Center on Intelligent Storage. Earlier, he was a Research Professor with the Center for Secure Information Systems, George Mason University, Fairfax, VA, USA. From 2008 to 2013, he served as a Program Director of NSF, where he managed the Computer Systems Research Program and was instrumental in the development and running of NSF-wide sustainability initiative named science, engineering, and education for sustainability. Prior to NSF, he served in industry for 18 years (at Intel, Hillsboro, OR, USA; Bellcore, Red Bank, NJ, USA; and Bell Labs, Murray Hill, NJ, USA) and 10 years in academia (at The Pennsylvania State University, State College, PA, USA, and Northwestern University, Evanston, IL, USA). He carries a combined 42 years of experience in academia, industry, and government. He has published in a wide variety of areas in computer science, authored a graduate textbook on performance modeling of computer systems. His research interests span a wide range, including energy efficiency, robustness, and security in cyber and cyber–physical systems.

Prof. Kant is an IEEE Distinguished Visitor.

Alireza Jolfaei (Senior Member, IEEE) received the Ph.D. degree.

He is an Associate Professor of Cybersecurity and Networking with the College of Science and Engineering, Flinders University, Tonsley, SA, Australia. His main research interest is in cyber–physical systems security, where he investigates the hidden interdependencies in industrial communication protocols and aims to provide fundamentally new methods for security-aware modeling, analysis, and design of safety-critical cyber–physical systems in the presence of cyber-adversaries.

Dr. Jolfaei received the prestigious IEEE Australian Council Award for his research article published in the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He is the Chair of the Security and Privacy Technical Committee of the IEEE Consumer Technology Society and the Editor-in-Chief of the IEEE Consumer Technology Society's World Newsletter. He has served as an Associate Editor for several IEEE journals and transactions, including the IEEE TRANSACTIONS ON CONSUMER TECHNOLOGY and the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS. He has served as the Program Co-Chair and a Technical Program Committee Member for major conferences, including IEEE ICCCN. He is a Distinguished Speaker of ACM on the topic of Cybersecurity.



Klaus Moessner (Senior Member, IEEE) received the Ph.D. degree.

He is a Professor of Communications Engineering with the University of Technology Chemnitz, Chemnitz, Germany, and also a Professor of Cognitive Networks with the Institute for Communication Systems and the 5G Innovation Centre, University of Surrey, Guildford, U.K. He was involved in more than 25 projects in the cognitive communications, service provision, and IoT areas. He was responsible for the work on cognitive decision-making mechanisms in the CR project ORACLE, led the work on radio awareness in the ICT FP7 project QoSMOS, and led the Speed5G, iKaaS, IoT.est, and SocIoTal projects. He is leading a research group investigating algorithms and mechanisms to gain knowledge and understanding of situations in and around autonomous vehicles. His research interests include cognitive networks, IoT deployments and sensor data-based knowledge generation, as well as reconfiguration and resource management.

Dr. Moessner was the Founding Chair of the IEEE DYSPAN Working Group (WG6) on Sensing Interfaces for future and cognitive communication systems.