AI/Machine Learning for Internet of Dependable and Controllable Things

Houbing Herbert Song, Ph.D., IEEE Fellow
University of Maryland, Baltimore County
Baltimore, USA
h.song@acm.org

ABSTRACT

The Internet of Things (IoT) has the potential to enable a variety of applications and services. However, it also presents grand challenges in security, safety, and privacy. Therefore, there is a need for moving from IoT to Internet of Dependable Things, which is defined as Internet of Things which is designed, built, deployed and operated in a highly trustworthy manner, and Internet of Controllable Things, which is defined as Internet of Things which is operated in a highly controllable manner. A massive resurgence of artificial intelligence (AI) and machine learning (ML) presents tremendous opportunities for Internet of Dependable and Controllable Things and as well as significant challenges to Internet of Dependable and Controllable Things. In this lecture, I will present the state of the art by reviewing and classifying the existing literature, evaluate the opportunities and challenges, and identify trends by evaluating what needs to be done to enable AI/Machine Learning for Internet of Dependable and Controllable Things.

CCS CONCEPTS

• **Computing methodologies** → **Artificial intelligence**; *Machine learning*; • **Computer systems organization** → Dependable and fault-tolerant systems and networks.

KEYWORDS

Artificial intelligence, Machine learning, Internet of Things

ACM Reference Format:
Houbing Herbert Song, Ph.D., IEEE Fellow. 2023. AI/Machine Learning for Internet of Dependable and Controllable Things. In *Proceedings of the 2023 Workshop on Advanced Multimedia Computing for Smart Manufacturing and Engineering (AMC-SME '23), November 2, 2023, Ottawa, ON, Canada.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3606042.3616460

BIOGRAPHY

Houbing Herbert Song (M'12–SM'14-F'23) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in August 2012.

He is currently a Professor, the Director of the NSF Center for Aviation Big Data Analytics (Planning), the Associate Director for Leadership of the DOT Transportation Cybersecurity Center for Advanced Research and Education (Tier 1 Center), and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us), University of Maryland, Baltimore County (UMBC), Baltimore, MD. Prior to joining UMBC, he was a Tenured Associate Professor of Electrical Engineering and Computer Science at Embry-Riddle Aeronautical University, Daytona Beach, FL. He serves as an Associate Editor for IEEE Transactions on Artificial Intelligence (TAI) (2023-present), IEEE Internet of Things Journal (2020-present), IEEE Transactions on Intelligent Transportation Systems (2021-present), and IEEE Journal on Miniaturization for Air and Space Systems (J-MASS) (2020-present). He was an Associate Technical Editor for IEEE Communications Magazine (2017-2020). He is the editor of eight books[4, 5, 7, 20, 21, 24–26], the author of more than 100 articles [1–3, 6, 8–19, 27–33] and the inventor of 2 patents [22, 23]. His research interests include cyber-physical systems/internet of things, cybersecurity and privacy, and

AMC-SME '23, November 2, 2023, Ottawa, ON, Canada
© 2023 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0273-0/23/11.
https://doi.org/10.1145/3606042.3616460

AI/machine learning/big data analytics. His research has been sponsored by federal agencies (including National Science Foundation, National Aeronautics and Space Administration, US Department of Transportation, and Federal Aviation Administration, among others) and industry. His research has been featured by popular news media outlets, including IEEE GlobalSpec's Engineering360, Association for Uncrewed Vehicle Systems International (AUVSI), Security Magazine, CXOTech Magazine, Fox News, U.S. News & World Report, The Washington Times, and New Atlas.

Dr. Song is an IEEE Fellow (for contributions to big data analytics and integration of AI with Internet of Things), and an ACM Distinguished Member (for outstanding scientific contributions to computing). He is an ACM Distinguished Speaker (2020-present), an IEEE Vehicular Technology Society (VTS) Distinguished Lecturer (2023-present) and an IEEE Systems Council Distinguished Lecturer (2023-present). Dr. Song has been a Highly Cited Researcher identified by Clarivate™ (2021, 2022). Dr. Song received Research.com Rising Star of Science Award in 2022, 2021 Harry Rowe Mimno Award bestowed by IEEE Aerospace and Electronic Systems Society, and 10+ Best Paper Awards from major international conferences, including IEEE CPSCom-2019, IEEE ICII 2019, IEEE/AIAA ICNS 2019, IEEE CBDCom 2020, WASA 2020, AIAA/ IEEE DASC 2021, IEEE GLOBECOM 2021 and IEEE INFOCOM 2022.

ACKNOWLEDGMENTS

This work was supported in part by the U.S. National Science Foundation under Grant No. 2309760 and Grant No. 2317117.

REFERENCES

[1] Kamal Acharya, Waleed Raza, Carlos Dourado, Alvaro Velasquez, and Houbing Herbert Song. 2023. Neurosymbolic Reinforcement Learning and Planning: A Survey. *IEEE Transactions on Artificial Intelligence* (2023), 1–14. https://doi.org/10.1109/TAI.2023.3311428

[2] Muhammad Adil, Jehad Ali, Muhammad Mohsin Jadoon, Sattam Rabia Alotaibi, Neeraj Kumar, Ahmed Farouk, and Houbing Song. 2023. COVID-19: Secure Healthcare Internet of Things Networks, Current Trends and Challenges with Future Research Directions. *ACM Trans. Sen. Netw.* 19, 3, Article 54 (may 2023), 25 pages. https://doi.org/10.1145/3558519

[3] Ismail Butun, Patrik Österberg, and Houbing Song. 2020. Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys Tutorials* 22, 1 (2020), 616–644. https://doi.org/10.1109/COMST.2019.2953364

[4] Guido Dartmann, Anke Schmeink, Volker Lücken, Houbing Song, Martina Ziefle, and Giovanni Prestiflippo. 2022. *Smart Transportation: AI Enabled Mobility and Autonomous Driving* (1st ed.). CRC Press.

[5] Guido Dartmann, Houbing Song, and Anke Schmeink. 2019. *Big Data Analytics for Cyber-Physical Systems: Machine Learning for the Internet of Things* (1st ed.). Elsevier.

[6] Aurora González-Vidal, José Mendoza-Bernal, Shuteng Niu, Antonio F. Skarmeta, and Houbing Song. 2023. A Transfer Learning Framework for Predictive Energy-Related Scenarios in Smart Buildings. *IEEE Transactions on Industry Applications* 59, 1 (2023), 26–37. https://doi.org/10.1109/TIA.2022.3179222

[7] Sabina Jeschke, Christian Brecher, Houbing Song, and Danda Rawat. 2017. *Industrial Internet of Things: Cybermanufacturing Systems* (1st ed.). Springer Cham.

[8] Bin Jiang, Jianqiang Li, Guanghui Yue, and Houbing Song. 2021. Differential Privacy for Industrial Internet of Things: Opportunities, Applications, and Challenges. *IEEE Internet of Things Journal* 8, 13 (2021), 10430–10451. https://doi.org/10.1109/JIOT.2021.3057419

[9] Yu Jiang, Houbing Song, Yixiao Yang, Han Liu, Ming Gu, Yong Guan, Jiaguang Sun, and Lui Sha. 2018. Dependable Model-Driven Development of CPS: From Stateflow Simulation to Verified Implementation. *ACM Trans. Cyber-Phys. Syst.* 3, 1, Article 12 (aug 2018), 31 pages. https://doi.org/10.1145/3078623

[10] Yongxin Liu, Jian Wang, Jianqiang Li, Shuteng Niu, and Houbing Song. 2021. Class-Incremental Learning for Wireless Device Identification in IoT. *IEEE Internet of Things Journal* 8, 23 (2021), 17227–17235. https://doi.org/10.1109/JIOT.2021.3078407

[11] Yongxin Liu, Jian Wang, Jianqiang Li, Shuteng Niu, and Houbing Song. 2022. Machine Learning for the Detection and Identification of Internet of Things Devices: A Survey. *IEEE Internet of Things Journal* 9, 1 (2022), 298–320. https://doi.org/10.1109/JIOT.2021.3099028

[12] Yongxin Liu, Jian Wang, Jianqiang Li, Shuteng Niu, Lei Wu, and Houbing Song. 2022. Zero-Bias Deep-Learning-Enabled Quickest Abnormal Event Detection in IoT. *IEEE Internet of Things Journal* 9, 13 (2022), 11385–11395. https://doi.org/10.1109/JIOT.2021.3126819

[13] Yongxin Liu, Jian Wang, Jianqiang Li, Houbing Song, Thomas Yang, Shuteng Niu, and Zhong Ming. 2021. Zero-Bias Deep Learning for Accurate Identification of Internet-of-Things (IoT) Devices. *IEEE Internet of Things Journal* 8, 4 (2021), 2627–2634. https://doi.org/10.1109/JIOT.2020.3018677

[14] Zhihan Lv, Ranran Lou, Jinhua Li, Amit Kumar Singh, and Houbing Song. 2021. Big Data Analytics for 6G-Enabled Massive Internet of Things. *IEEE Internet of Things Journal* 8, 7 (2021), 5350–5359. https://doi.org/10.1109/JIOT.2021.3056128

[15] Zhihan Lv, Houbing Song, Pablo Basanta-Val, Anthony Steed, and Minho Jo. 2017. Next-Generation Big Data Analytics: State of the Art, Challenges, and Future Research Topics. *IEEE Transactions on Industrial Informatics* 13, 4 (2017), 1891–1899. https://doi.org/10.1109/TII.2017.2650204

[16] Shuteng Niu, Yushan Jiang, Bowen Chen, Jian Wang, Yongxin Liu, and Houbing Song. 2021. Cross-Modality Transfer Learning for Image-Text Information Management. *ACM Trans. Manage. Inf. Syst.* 13, 1, Article 5 (oct 2021), 14 pages. https://doi.org/10.1145/3464324

[17] Shuteng Niu, Meryl Liu, Yongxin Liu, Jian Wang, and Houbing Song. 2021. Distant Domain Transfer Learning for Medical Imaging. *IEEE Journal of Biomedical and Health Informatics* 25, 10 (2021), 3784–3793. https://doi.org/10.1109/JBHI.2021.3051470

[18] Shuteng Niu, Yongxin Liu, Jian Wang, and Houbing Song. 2020. A Decade Survey of Transfer Learning (2010–2020). *IEEE Transactions on Artificial Intelligence* 1, 2 (2020), 151–166. https://doi.org/10.1109/TAI.2021.3054609

[19] Justus Renkhoff, Wenkai Tan, Alvaro Velasquez, William Yichen Wang, Yongxin Liu, Jian Wang, Shuteng Niu, Lejla Begic Fazlic, Guido Dartmann, and Houbing Song. 2022. Exploring Adversarial Attacks on Neural Networks: An Explainable Approach. In *2022 IEEE International Performance, Computing, and Communications Conference (IPCCC)*. 41–42. https://doi.org/10.1109/IPCCC55026.2022.9894322

[20] Houbing Song, Glenn A. Fink, and Sabina Jeschke. 2017. *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications* (1st ed.). Wiley-IEEE Press.

[21] Houbing Song, Kenneth Hopkinson, Tomaso De Cola, Tom Alexandrovich, and Dahai Liu. 2021. *Aviation Cybersecurity: Foundations, Principles, and Applications* (1st ed.). IET Press.

[22] Houbing Song, Yongxin Liu, and Jian Wang. 2021. UAS Detection and Negation. https://patents.google.com/patent/US20210197967A1/en

[23] Houbing Song, Yongxin Liu, and Jian Wang. 2021. UAS Detection and Negation. https://patents.google.com/patent/WO2020236328A3/en

[24] Houbing Song, Danda B. Rawat, Sabina Jeschke, and Christian Brecher. 2016. *Cyber-Physical Systems: Foundations, Principles and Applications* (1st ed.). Academic Press, Inc., USA.

[25] Houbing Song, Ravi Srinivasan, Tamim Sookoor, and Sabina Jeschke. 2017. *Smart Cities: Foundations, Principles, and Applications* (1st ed.). Wiley Publishing.

[26] Yunchuan Sun and Houbing Song. 2017. *Secure and Trustworthy Transportation Cyber-Physical Systems* (1st ed.). Springer Singapore.

[27] Yunchuan Sun, Houbing Song, Antonio J. Jara, and Rongfang Bie. 2016. Internet of Things and Big Data Analytics for Smart and Connected Communities. *IEEE Access* 4 (2016), 766–773. https://doi.org/10.1109/ACCESS.2016.2529723

[28] Wenkai Tan, Justus Renkhoff, Alvaro Velasquez, Ziyu Wang, Lusi Li, Jian Wang, Shuteng Niu, Fan Yang, Yongxin Liu, and Houbing Song. 2023. NoiseCAM: Explainable AI for the Boundary Between Noise and Adversarial Attacks. In *2023 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE 2023)*.

[29] Jian Wang, Yongxin Liu, and Houbing Song. 2021. Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends. *IEEE Aerospace and Electronic Systems Magazine* 36, 3 (2021), 4–29. https://doi.org/10.1109/MAES.2020.3015537

[30] Jiachen Yang, Chenguang Wang, Bin Jiang, Houbing Song, and Qinggang Meng. 2021. Visual Perception Enabled Industry Intelligence: State of the Art, Challenges and Prospects. *IEEE Transactions on Industrial Informatics* 17, 3 (2021), 2204–2219. https://doi.org/10.1109/TII.2020.2998818

[31] Zhenhua Yu, Hongxia Gao, Xuya Cong, Naiqi Wu, and Houbing Herbert Song. 2023. A Survey on Cyber-Physical Systems Security. *IEEE Internet of Things Journal* (2023), 1–1. https://doi.org/10.1109/JIOT.2023.3289625

[32] Xuejun Yue, Yongxin Liu, Jian Wang, Houbing Song, and Huiru Cao. 2018. Software Defined Radio and Wireless Acoustic Networking for Amateur Drone Surveillance. *IEEE Communications Magazine* 56, 4 (2018), 90–97. https://doi.org/10.1109/MCOM.2018.1700423

[33] Yuan Zhang, Limin Sun, Houbing Song, and Xiaojun Cao. 2014. Ubiquitous WSN for Healthcare: Recent Advances and Future Prospects. *IEEE Internet of Things Journal* 1, 4 (2014), 311–318. https://doi.org/10.1109/JIOT.2014.2329462