REFERENCES

[1] Y. Lin, P. Wang, and M. Ma, “Intelligent Transportation System(ITS): Concept, Challenge and Opportunity,” in *2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, IEEE, May 2017, pp. 167–172. doi: 10.1109/BigDataSecurity.2017.50.

[2] K. N. Qureshi and A. H. Abdullah, “A survey on intelligent transportation systems,” *Middle East J Sci Res*, vol. 15, no. 5, pp. 629–642, 2013, doi: 10.5829/idosi.mejsr.2013.15.5.11215.

[3] S. H. An, B. H. Lee, and D. R. Shin, “A survey of intelligent transportation systems,” in *Proceedings - 3rd International Conference on Computational Intelligence, Communication Systems and Networks, CICSyN 2011*, 2011, pp. 332–337. doi: 10.1109/CICSyN.2011.76.

[4] Y. Wei, H. Lu, and Z. He, “Research of the digital communication system for CBTC based on 802.11,” in *Proceedings - 3rd International Conference on Multimedia Information Networking and Security, MINES 2011*, 2011, pp. 95–99. doi: 10.1109/MINES.2011.26.

[5] S. Soderi, D. Masti, and Y. Z. Lun, “Railway cyber-security in the era of interconnected systems: a survey,” Jul. 2022, doi: 10.1109/TITS.2023.3254442.

[6] H. Liang, H. Zhao, S. Wang, and Y. Zhang, “LTE-U based Train to Train Communication System in CBTC: System Desin and Reliability Analysis,” *Wirel Commun Mob Comput*, vol. 2020, 2020, doi: 10.1155/2020/8893631.

[7] S. Soderi, D. Masti, M. Hämäläinen, and J. Iinatti, “Cybersecurity Considerations for Communication Based Train Control,” *IEEE Access*, vol. 11, pp. 92312–92321, 2023, doi: 10.1109/ACCESS.2023.3309005.

[8] S. Kim, Y. Won, I. H. Park, Y. Eun, and K. J. Park, “Cyber-Physical Vulnerability Analysis of Communication-Based Train Control,” *IEEE Internet Things J*, vol. 6, no. 4, pp. 6353–6362, Aug. 2019, doi: 10.1109/JIOT.2019.2919066.

[9] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, “Machine Learning for Anomaly Detection: A Systematic Review,” 2021, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2021.3083060.

[10] R. W. Van Der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 779–811, Jan. 2019, doi: 10.1109/COMST.2018.2873088.

[11] S. Gyawali, Y. Qian, and R. Q. Hu, "Machine Learning and Reputation Based Misbehavior Detection in Vehicular Communication Networks," *IEEE Trans Veh Technol*, vol. 69, no. 8, pp. 8871–8885, Aug. 2020, doi: 10.1109/TVT.2020.2996620.

[12] S. Caton and C. Haas, "Fairness in Machine Learning: A Survey," *ACM Comput Surv*, vol. 56, no. 7, pp. 1–38, Jul. 2024, doi: 10.1145/3616865.

[13] A. Telikani, A. Tahmassebi, W. Banzhaf, and A. H. Gandomi, "Evolutionary Machine Learning: A Survey," Nov. 30, 2022, *Association for Computing Machinery*. doi: 10.1145/3467477.

[14] P. A. D. Amiri and S. Pierre, "An Ensemble-Based Machine Learning Model for Forecasting Network Traffic in VANET," *IEEE Access*, vol. 11, pp. 22855–22870, 2023, doi: 10.1109/ACCESS.2023.3253625.

[15] F. A. Ghaleb, M. A. Maarof, A. Zainal, B. A. Saleh Al-Rimy, A. Alsaeedi, and W. Boulila, "Ensemble-based hybrid context-aware misbehavior detection model for vehicular ad hoc network," *Remote Sens (Basel)*, vol. 11, no. 23, Dec. 2019, doi: 10.3390/rs11232852.

[16] L. Zhu, D. Yao, and H. Zhao, "Reliability Analysis of Next-Generation CBTC Data Communication Systems," *IEEE Trans Veh Technol*, vol. 68, no. 3, pp. 2024–2034, Mar. 2019, doi: 10.1109/TVT.2018.2870053.

[17] L. Zhu, Y. Li, F. R. Yu, B. Ning, T. Tang, and X. Wang, "Cross-Layer Defense Methods for Jamming-Resistant CBTC Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 11, pp. 7266–7278, Nov. 2021, doi: 10.1109/TITS.2020.3005931.

[18] A. Fakhereldine, M. Zulkernine, and D. Murdock, "TrainSec: A Simulation Framework for Security Modeling and Evaluation in CBTC Networks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer Science and Business Media Deutschland GmbH, 2023, pp. 22–39. doi: 10.1007/978-3-031-43366-5_2.

[19] A. Fakhereldine, M. Zulkernine, and D. Murdock, "CBTCset: A Reference Dataset for Detecting Misbehavior Attacks in CBTC Networks," in *Proceedings - 2023 IEEE 34th International Symposium on Software Reliability*

Engineering Workshop, ISSREW 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 57–62. doi: 10.1109/ISSREW60843.2023.00047.

[20] S. Erickson, “Plain Text & Character Encoding: A Primer for Data Curators,” *J Escience Librariansh*, vol. 10, no. 3, Aug. 2021, doi: 10.7191/jeslib.2021.1211.

[21] M. M. Ahsan, M. A. P. Mahmud, P. K. Saha, K. D. Gupta, and Z. Siddique, “Effect of Data Scaling Methods on Machine Learning Algorithms and Model Performance,” *Technologies (Basel)*, vol. 9, no. 3, Sep. 2021, doi: 10.3390/technologies9030052.

[22] I. Rail Transit Vehicle Interface Standards Committee of the IEEE Vehicular Technology Society, “IEEE Recommended Practice for Communications-Based Train Control (CBTC) System Design and Functional Allocations IEEE Vehicular Technology Society,” 2008.

[23] R. Transit Vehicle Interface Standards Committee of the IEEE Vehicular Technology Society, “IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements IEEE Vehicular Technology Society Sponsored by the Rail Transit Vehicle Interface Standards Committee IEEE Standards,” 2005.

[24] *IEEE Std 1474.2-2003 : IEEE Standard for User Interface Requirements in Communications-Based Train Control (CBTC) Systems*. IEEE, 2003.

[25] J. Farooq and J. Soler, “Radio Communication for Communications-Based Train Control (CBTC): A Tutorial and Survey,” Jul. 01, 2017, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/COMST.2017.2661384.

[26] Z. Wang and X. Liu, “Cyber security of railway cyber-physical system (CPS) – A risk management methodology,” *Communications in Transportation Research*, vol. 2, Dec. 2022, doi: 10.1016/j.commtr.2022.100078.

[27] S. Kolli, J. Lilly, and D. Wijesekera, “Positive train control security: An intrusion-detection system to provide cyber-situational awareness,” *IEEE Vehicular Technology Magazine*, vol. 13, no. 3, pp. 48–60, Sep. 2018, doi: 10.1109/MVT.2018.2848398.

[28] M. Burmester, E. Magkos, and V. Chrissikopoulos, “Modeling security in cyber-physical systems,” *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3–4, pp. 118–126, Dec. 2012, doi: 10.1016/j.ijcip.2012.08.002.

[29] B. Gao and B. Bu, “A Novel Intrusion Detection Method in Train-Ground Communication System,” *IEEE Access*, vol. 7, pp. 178726–178743, 2019, doi: 10.1109/ACCESS.2019.2958198.

[30] H. A. Idris, K. Ueda, B. Mokhtar, and S. A. Elsagheer Mohamed, “Machine Learning Based Misbehavior Detection System for False Data Injection Attack in Internet of Vehicles Using Neighbor Public Transport Vehicle Approach,” *International Journal of Computer Networks and Applications*, vol. 11, no. 2, pp. 159–176, Mar. 2024, doi: 10.22247/ijcna/2024/224442.

[31] “Information technology-Security techniques-Information security management systems-Requirements ISO/IEC 27001 INTERNATIONAL STANDARD(E) ii COPYRIGHT PROTECTED DOCUMENT.”

[32] “Using the ISA/IEC 62443 Standards to Secure Your Control Systems.”

[33] S. Park, D. Kim, and S. Lee, “Enhancing V2X Security Through Combined Rule-Based and DL-Based Local Misbehavior Detection in Roadside Units,” *IEEE Open Journal of Intelligent Transportation Systems*, 2024, doi: 10.1109/OJITS.2024.3479716.

[34] E. Mármol Campos, J. L. Hernandez-Ramos, A. González Vidal, G. Baldini, and A. Skarmeta, “Misbehavior detection in intelligent transportation systems based on federated learning,” *Internet of Things (Netherlands)*, vol. 25, Apr. 2024, doi: 10.1016/j.iot.2024.101127.

[35] E. Tufan, C. Tezcan, and C. Acartürk, “Anomaly-based intrusion detection by machine learning: A case study on probing attacks to an institutional network,” *IEEE Access*, vol. 9, pp. 50078–50092, 2021, doi: 10.1109/ACCESS.2021.3068961.

[36] Z. S. Lee, H. Guo, and L. Zhou, “Rail system anomaly detection via machine learning approaches,” in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 824–828. doi: 10.1109/TENCON50793.2020.9293809.

[37] S. B. Kotsiantis, I. D. Zaharakis, and P. E. Pintelas, “Machine learning: A review of classification and combining techniques,” *Artif Intell Rev*, vol. 26, no. 3, pp. 159–190, Nov. 2006, doi: 10.1007/s10462-007-9052-3.

[38] R. N. Behera, K. Das, B. Tech, and A. Professor, “A Survey on Machine Learning: Concept, Algorithms and Applications International Journal of Innovative Research in Computer and Communication Engineering A Survey on Machine Learning: Concept, Algorithms and Applications,” *Article in International Journal of Innovative Research in Computer and Communication Engineering*, 2017, doi: 10.15680/IJIRCCE.2017.

[39] B. Ghojogh and M. Crowley, “The Theory Behind Overfitting, Cross Validation, Regularization, Bagging, and Boosting: Tutorial,” May 2019, [Online]. Available: http://arxiv.org/abs/1905.12787

[40] R. Natras, B. Soja, and M. Schmidt, “Ensemble Machine Learning of Random Forest, AdaBoost and XGBoost for Vertical Total Electron Content Forecasting,” *Remote Sens (Basel)*, vol. 14, no. 15, Aug. 2022, doi: 10.3390/rs14153547.

[41] P. A. A. Resende and A. C. Drummond, “A survey of random forest based methods for intrusion detection systems,” Jul. 31, 2018, *Association for Computing Machinery*. doi: 10.1145/3178582.

[42] G. Tuysuzoglu and D. Birant, “Enhanced bagging (eBagging): A novel approach for ensemble learning,” *International Arab Journal of Information Technology*, vol. 17, no. 4, pp. 515–528, Jul. 2020, doi: 10.34028/iajit/17/4/10.

[43] I. Mahmoudi, J. Kamel, I. Ben-Jemaa, A. Kaiser, and P. Urien, “Towards a Reliable Machine Learning Based Global Misbehavior Detection in C-ITS: Model Evaluation Approach.” [Online]. Available: https://hal.science/hal-02353893v1

[44] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, “CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment,” *Sensors*, vol. 23, no. 13, Jul. 2023, doi: 10.3390/s23135941.

[45] Z. Li, Z. Yan, N. Bin, and J. Hailin, “Train-ground communication in CBTC based on 802.11b: Design and performance research,” in *Proceedings - 2009 WRI International Conference on Communications and Mobile Computing, CMC 2009*, 2009, pp. 368–372. doi: 10.1109/CMC.2009.93.

[46] D. Bashir, G. D. Montanez, S. Sehra, P. S. Segura, and J. Lauw, “An Information-Theoretic Perspective on Overfitting and Underfitting,” Oct. 2020, [Online]. Available: http://arxiv.org/abs/2010.06076

[47] H. Zhang, L. Zhang, and Y. Jiang, “Overfitting and Underfitting Analysis for Deep Learning Based End-to-end Communication Systems.”

[48] C. Aliferis and G. Simon, “Overfitting, Underfitting and General Model Overconfidence and Under-Performance Pitfalls and Best Practices in Machine Learning and AI,” 2024, pp. 477–524. doi: 10.1007/978-3-031-39355-6_10.

[49] G. Simon, “Health Informatics Artificial Intelligence and Machine Learning in Health Care and Medical Sciences Best Practices and Pitfalls.”

[50] S. Editor Wolfgang Walz, “Machine Learning for Brain Disorders.” [Online]. Available: http://www.springer.com/series/7657

[51] M. A. Amanullah, M. B. Chhetri, S. W. Loke, and R. Doss, “BurST-ADMA: Towards an Australian Dataset for Misbehaviour Detection in the Internet of Vehicles.”

[52] H. A. Idris *et al.*, “Explaining Machine Learning Based Speed Anomaly Detection System Using eXplainable Artificial Intelligence.” [Online]. Available: https://www.researchgate.net/publication/379025563

[53] Z. Shao, M. N. Ahmad, and A. Javed, “Comparison of Random Forest and XGBoost Classifiers Using Integrated Optical and SAR Features for Mapping Urban Impervious Surface,” *Remote Sens (Basel)*, vol. 16, no. 4, Feb. 2024, doi: 10.3390/rs16040665.

[54] K. M. Kahloot and P. Ekler, “Algorithmic Splitting: A Method for Dataset Preparation,” *IEEE Access*, vol. 9, pp. 125229–125237, 2021, doi: 10.1109/ACCESS.2021.3110745.

[55] Q. H. Nguyen *et al.*, “Influence of data splitting on performance of machine learning models in prediction of shear strength of soil,” *Math Probl Eng*, vol. 2021, 2021, doi: 10.1155/2021/4832864.