Table A: Selected studies in the review. Here ID denotes study identification number.

ID	Title	Authors	Venue	Year	Ref
S1	RF-Sensing: A New Way to Observe Surroundings	Khunteta, Shubham, Saikrishna, Pedamalli, Agrawal, Avani, Kumar, Ashwini, Chavva, Ashok Kumar Reddy	IEEE Access	2022	[1]
S2	Dynamic spectrum allocation following machine learning-based traffic predictions in 5G	Rony, Rakibul Islam, Lopez-Aguilera, Elena, Garcia-Villegas, Eduard	IEEE Access	2021	[2]
S3	Confidence aware deep learning driven wireless resource allocation in shared spectrum bands	Ganewattha, Chanaka, Khan, Zaheer, Latva-Aho, Matti, Lehtoma	IEEE Access	2022	[3]
S4	Secure Industrial IoT Systems via RF Fingerprinting Under Impaired Channels With Interference and Noise	Gul, Omer Melih, Kulhandjian, Michel, Kantarci, Burak, Touazi, Azzedine, Ellement, Cliff, D'amours, Claude	IEEE Access	2023	[4]
S5	GPDS: A multi-agent deep reinforcement learning game for anti-jamming secure computing in MEC network	Chen, Miaojiang, Liu, Wei, Zhang, Ning, Li, Junling, Ren, Yingying, Yi, Meng, Liu, Anfeng	Expert Systems with Applications	2022	[5]
S6	Generalized wireless adversarial deep learning	Restuccia, Francesco, D'Oro, Salvatore, Al-Shawabka, Amani, Rendon, Bruno Costa, Chowdhury, Kaushik, Ioannidis, Stratis, Melodia, Tommaso	Computer Networks	2020	[6]
S7	Cybertwin-driven resource allocation using deep reinforcement learning in 6G-enabled edge environment	Jain, Vibha, Kumar, Bijendra, Gupta, Aditya	Journal of King Saud University – Computer and Information Sciences	2022	[7]
S8	Online edge learning offloading and resource management for UAV-assisted MEC secure communications	Ding, Yu, Feng, Yunqi, Lu, Weidang, Zheng, Shilian, Zhao, Nan, Meng, Limin, Nallanathan, Arumugam, Yang, Xiaoniu	IEEE Journal of Selected Topics in Signal Processing	2022	[8]
S9	When deep reinforcement learning meets federated learning: Intelligent multi-timescale resource management for multi-access edge computing in 5G ultradense network	Yu, Shuai, Chen, Xu, Zhou, Zhi, Gong, Xiaowen, Wu, Di	IEEE Internet of Things Journal	2020	[9]
S10	Federated Reinforcement Learning-Based Resource Allocation for D2D-Aided Digital Twin Edge Networks in 6G Industrial IoT	Guo, Qi, Tang, Fengxiao, Kato, Nei	IEEE Transactions on Industrial Informatics	2022	[10]
S11	Reinforcement learning based latency minimization in secure NOMA-MEC systems with hybrid SIC	Wang, Kaidi, Li, Haodong, Ding, Zhiguo, Xiao, Pei	IEEE Transactions on Wireless Communications	2022	[11]
S12	Security Hardening of Intelligent Reflecting Surfaces Against Adversarial Machine Learning Attacks	Catak, Ferhat Ozgur, Kuzlu, Murat, Tang, Haolin, Catak, Evren, Zhao, Yanxiao	IEEE Access	2022	[12]

Continued on next page

Appendix A – continued from previous page

ID	Title	Authors	Venue	Year	Ref
S13	Beyond 5G for digital twins of UAVs	Lv, Zhihan, Chen, Dongliang, Feng, Hailing, Lou, Ranran, Wang, Huihui	Computer Networks	2021	[13]
S14	A variational autoencoder-based secure transceiver design using deep learning	Lin, Chia-Hung, Wu, Chao-Chin, Chen, Kuan-Fu, Lee, Ta-Sung	IEEE GLOBECOM	2020	[14]
S15	The Hexa-X project vision on Artificial Intelligence and Machine Learning-driven Communication and Computation co-design for 6G	Merluzzi, Mattia, Borsos, Tams, Rajatheva, Nandana, Benczr, Andrs A, Farhadi, Hamed, Yassine, Taha, Mu	IEEE Access	2023	[15]
S16	Multi-UAV-assisted computation offloading in DT-based networks: A distributed deep reinforcement learning approach	Shi, Junling, Li, Chunyu, Guan, Yunchong, Cong, Peiyu, Li, Jie	Computer Communications	2023	[16]
S17	Mitigating Jamming Attack in 5G Heterogeneous Networks: A Federated Deep Reinforcement Learning Approach	Sharma, Himanshu, Kumar, Neeraj, Tekchandani, Rajkumar	IEEE Transactions on Vehicular Technology	2022	[17]
S18	Exploring Practical Vulnerabilities of Machine Learning-based Wireless Systems	Liu, Zikun, Xu, Changming, Sie, Emerson, Singh, Gagandeep, Vasisht, Deepak	USENIX Symposium on Networked Systems Design and Implementation	2023	[18]
S19	Digital Twin-Aided Learning for Managing Reconfigurable Intelligent Surface-Assisted, Uplink, User-Centric Cell-Free Systems	Cui, Yingping, Lv, Tiejun, Ni, Wei, Jamalipour, Abbas	IEEE Journal on Selected Areas in Communications	2023	[19]
S20	mmecho: A mmwave-based acoustic eavesdropping method	Hu, Pengfei, Li, Wenhao, Spolaor, Riccardo, Cheng, Xiuzhen	IEEE Symposium on Security and Privacy	2023	[20]
S21	A D2D-Aided Federated Learning Scheme With Incentive Mechanism in 6G Networks	Fantacci, Romano, Picano, Benedetta	IEEE Access	2022	[21]
S22	Joint resource allocation to minimize execution time of federated learning in cell-free massive MIMO	Vu, Tung Thanh, Ngo, Duy Trong, Ngo, Hien Quoc, Dao, Minh Ngoc, Tran, Nguyen Hoang, Middleton, Richard H	IEEE Internet of Things Journal	2022	[22]
S23	Joint resource management for mobility supported federated learning in Internet of Vehicles	Wang, Ge, Xu, Fangmin, Zhang, Hengsheng, Zhao, Chenglin	Future Generation Computer Systems	2022	[23]
S24	Mitigating attacks on artificial intelligence-based spectrum sensing for cellular network signals	Catak, Ferhat Ozgur, Kuzlu, Murat, Sarp, Salih, Catak, Evren, Cali, Umit	IEEE GLOBECOM	2022	[24]
S25	Privacy-preserving federated k-means for proactive caching in next generation cellular networks	Liu, Yang, Ma, Zhuo, Yan, Zheng, Wang, Zhuzhu, Liu, Ximeng, Ma, Jianfeng	Journal of King Saud University – Computer and Information Sciences	2020	[25]

Continued on next page

Appendix A – continued from previous page

ID	Title	Authors	Venue	Year	Ref
S26	Resource allocation and device pairing for energy-efficient NOMA-enabled federated edge learning	Hu, Youqiang, Huang, Hejiao, Yu, Nuo	Computer Communications	2023	[26]
S27	Adaptive resource reservation to survive against adversarial resource selection jamming attacks in 5g nr-v2x distributed mode 2	Djaidja, Taki Eddine Toufik, Brik, Bouziane, Senouci, Sidi Mohammed, Ghamri-Doudane, Yacine	IEEE International Conference on Communications	2022	[27]
S28	Securing radio resources allocation with deep reinforcement learning for IoE services in next-generation wireless networks	Peng, Yuhuai, Xue, Xiaojing, Bashir, Ali Kashif, Zhu, Xiaogang, Al-Otaibi, Yasser D, Tariq, Usman, Yu, Keping	IEEE Transactions on Network Science and Engineering	2022	[28]
S29	A deep convolutional neural network based transfer learning method for non-cooperative spectrum sensing	Pati, Bipun Man, Kaneko, Megumi, Taparugssanagorn, Attaphongse	IEEE Access	2020	[29]
S30	Spectrum Sensing in Cognitive Radio Using CNN-RNN and Transfer Learning	Solanki, Surendra, Dehalwar, Vasudev, Choudhary, Jaytrilok, Kolhe, Mohan Lal, Ogura, Koki	IEEE Access	2022	[30]
S31	When attackers meet AI: Learning-empowered attacks in cooperative spectrum sensing	Luo, Zhengping, Zhao, Shangqing, Lu, Zhuo, Xu, Jie, Sagduyu, Yalin E	IEEE Transactions on Mobile Computing	2020	[31]
S32	Adversarial deep learning for over-the-air spectrum poisoning attacks	Sagduyu, Yalin E, Shi, Yi, Erpek, Tugba	IEEE Transactions on Mobile Computing	2019	[32]
S33	Channel-aware adversarial attacks against deep learning-based wireless signal classifiers	Kim, Brian, Sagduyu, Yalin E, Davaslioglu, Kemal, Erpek, Tugba, Ulukus, Sennur	IEEE Transactions on Wireless Communications	2021	[33]
S34	Deep learning driven physical layer security for a simultaneously wireless information and power transfer network	Li, Junxia, Zhao, Hui, Huang, Yiyun, Zhang, Miao, Lal, Sujesh P	Alexandria Engineering Journal	2022	[34]
S35	Threshold-free physical layer authentication based on machine learning for industrial wireless CPS	Pan, Fei, Pang, Zhibo, Wen, Hong, Luvisotto, Michele, Xiao, Ming, Liao, Run-Fa, Chen, Jie	IEEE Transactions on Industrial Informatics	2019	[35]
S36	Improving medium access efficiency with intelligent spectrum learning	Yang, Bo, Cao, Xuelin, Omotere, Oluwaseyi, Li, Xiangfang, Han, Zhu, Qian, Lijun	IEEE Access	2020	[36]
S37	Signal detection and classification in shared spectrum: A deep learning approach	Zhang, Wenhan, Feng, Mingjie, Krunz, Marwan, Abyaneh, Amir Hossein Yazdani	IEEE INFOCOM	2021	[37]
S38	A Radio Frequency Region-of-Interest Convolutional Neural Network for Wideband Spectrum Sensing	Olesiski, Adam, Piotrowski, Zbigniew	Sensors	2023	[38]

Continued on next page

Appendix A – continued from previous page

ID	Title	Authors	Venue	Year	Ref
S39	Charm: Nextg spectrum sharing through data-driven realtime o-ran dynamic control	Baldesi, Luca, Restuccia, Francesco, Melodia, Tommaso	IEEE INFOCOM	2022	[39]
S40	Learning the unknown: Improving modulation classification performance in unseen scenarios	Perenda, Erma, Rajendran, Sreeraj, Bovet, Gerome, Pollin, Sofie, Zheleva, Mariya	IEEE INFOCOM	2021	[40]
S41	A deep reinforcement learning framework for spectrum management in dynamic spectrum access	Song, Hao, Liu, Lingjia, Ashdown, Jonathan, Yi, Yang	IEEE Internet of Things Journal	2021	[41]
S42	End-to-end learning from spectrum data: A deep learning approach for wireless signal identification in spectrum monitoring applications	Kulin, Merima, Kazaz, Tarik, Moerman, Ingrid, De Poorter, Eli	IEEE Access	2018	[42]
S43	Deep learning-based spectrum prediction collision avoidance for hybrid wireless environments	Mennes, Ruben, Claeys, Maxim, De Figueiredo, Felipe AP, Jabandvz	IEEE Access	2019	[43]
S44	An ai-based incumbent protection system for collaborative intelligent radio networks	Camelo, Miguel, Mennes, Ruben, Shahid, Adnan, Struye, Jakob, Donato, Carlos, Jabandzic, Irfan, Giannoulis, Spilios, Mahfoudhi, Farouk, Maddala, Prasanthi, Seskar, Ivan, others	IEEE Wireless Communications	2020	[44]
S45	Optimizing primary user privacy in spectrum sharing systems	Clark, Matthew, Psounis, Konstantinos	IEEE/ACM Transactions on Networking	2020	[45]
S46	Pattern-aware intelligent anti-jamming communication: A sequential deep reinforcement learning approach	Liu, Songyi, Xu, Yifan, Chen, Xueqiang, Wang, Ximing, Wang, Meng, Li, Wen, Li, Yangyang, Xu, Yuhua	IEEE Access	2019	[46]
S47	"jam me if you can:" defeating jammer with deep dueling neural network architecture and ambient backscattering augmented communications	Van Huynh, Nguyen, Nguyen, Diep N, Hoang, Dinh Thai, Dutkiewicz, Eryk	IEEE Journal on Selected Areas in Communications	2019	[47]
S48	DeepFake: Deep dueling-based deception strategy to defeat reactive jammers	Van Huynh, Nguyen, Hoang, Dinh Thai, Nguyen, Diep N, Dutkiewicz, Eryk	IEEE Transactions on Wireless Communications	2021	[48]
S49	CyberSpec: Behavioral Fingerprinting for Intelligent Attacks Detection on Crowdsensing Spectrum Sensors	Celdrn, Alberto Huertas, Snchez, Pedro Miguel Snchez, Bovet, Gro	IEEE Transactions on Dependable and Secure Computing	2023	[49]
S50	Differential privacy and IRS empowered intelligent energy harvesting for 6G Internet of Things	Pan, Qianqian, Wu, Jun, Zheng, Xi, Yang, Wu, Li, Jianhua	IEEE Internet of Things Journal	2021	[50]

Continued on next page

Appendix A – continued from previous page

ID	Title	Authors	Venue	Year	Ref
S51	Federated learning for intelligent transmission with space-air-ground integrated network (SAGIN) toward 6G	Tang, Fengxiao, Wen, Cong, Chen, Xuehan, Kato, Nei	IEEE Network	2022	[51]
S52	Federated Multi-Agent Deep Reinforcement Learning (Fed-MADRL) for Dynamic Spectrum Access	Chang, Hao-Hsuan, Song, Yifei, Doan, Thinh T, Liu, Lingjia	IEEE Transactions on Wireless Communications	2023	[52]
S53	How effective is the artificial noise? Real-time analysis of a PHY security scenario	Goekceli, Selahattin, Cepheli, Oezge, Basaran, Semiha Tedik, Kurt, Guenes Karabulut, Dartmann, Guido, Ascheid, Gerd	IEEE GLOBECOM	2017	[53]
S54	Anomaly detection based on multidimensional data processing for protecting vital devices in 6G-enabled massive IIoT	Han, Guangjie, Tu, Juntao, Liu, Li, Martnez-Garca, Miguel, Peng, Yan	IEEE Internet of Things Journal	2021	[54]
S55	Self-Optimizing Data Offloading in Mobile Heterogeneous Radio-Optical Networks: A Deep Reinforcement Learning Approach	Shao, Sihua, Nazzal, Mahmoud, Khreishah, Abdallah, Ayyash, Moussa	IEEE Network	2022	[55]
S56	Defensive distillation-based adversarial attack mitigation method for channel estimation using deep learning models in next-generation wireless networks	Catak, Ferhat Ozgur, Kuzlu, Murat, Catak, Evren, Cali, Umit, Guler, Ozgur	IEEE Access	2022	[56]
S57	Data-augmentation-based cellular traffic prediction in edge-computing-enabled smart city	Wang, Zi, Hu, Jia, Min, Geyong, Zhao, Zhiwei, Wang, Jin	IEEE Transactions on Industrial Informatics	2020	[57]
S58	Federated learning for 5G base station traffic forecasting	Perifanis, Vasileios, Pavlidis, Nikolaos, Koutsiamanis, Remous-Aris, Efraimidis, Pavlos S	Computer Networks	2023	[58]
S59	A self-adaptive deep learning-based system for anomaly detection in 5G networks	Maim, Lorenzo Fernndez, Gmez, ngel Luis Perales, Clemente, Flix J Garca, Prez, Manuel Gil, Prez, Gregorio Martnez	IEEE Access	2018	[59]
S60	Anomaly detection approach for urban sensing based on credibility and time-series analysis optimization model	Zhang, Hong, Li, Zhanming	IEEE Access	2019	[60]
S61	Fault-tolerant event region detection on trajectory pattern extraction for industrial wireless sensor networks	Liu, Li, Han, Guangjie, He, Yu, Jiang, Jinfang	IEEE Transactions on Industrial Informatics	2019	[61]
S62	Context-and-social-aware online beam selection for mmwave vehicular communications	Li, Dapeng, Wang, Shichao, Zhao, Haitao, Wang, Xiaoming	IEEE Internet of Things Journal	2020	[62]

Continued on next page

Appendix A – continued from previous page

ID	Title	Authors	Venue	Year	Ref
S63	Machine learning enabling analog beam selection for concurrent transmissions in millimeter-wave V2V communications	Yang, Yang, Gao, Zhen, Ma, Yao, Cao, Biao, He, Dazhong	IEEE Transactions on Vehicular Technology	2020	[63]
S64	Computer vision aided mmWave beam alignment in V2X communications	Xu, Weihua, Gao, Feifei, Tao, Xiaoming, Zhang, Jianhua, Alkhateeb, Ahmed	IEEE Transactions on Wireless Communications	2022	[64]
S65	A deep learning-based low overhead beam selection in mmWave communications	Echigo, Haruhi, Cao, Yuwen, Bouazizi, Mondher, Ohtsuki, Tomoaki	IEEE Transactions on Vehicular Technology	2021	[65]
S66	Deep learning-based mmWave beam selection for 5G NR/6G with sub-6 GHz channel information: Algorithms and prototype validation	Sim, Min Soo, Lim, Yeon-Geun, Park, Sang Hyun, Dai, Linglong, Chae, Chan-Byoung	IEEE Access	2020	[66]
S67	Deep learning for mmWave beam and blockage prediction using sub-6 GHz channels	Alrabeiah, Muhammad, Alkhateeb, Ahmed	IEEE Transactions on Communications	2020	[67]
S68	LIDAR data for deep learning-based mmWave beam-selection	Klautau, Aldebaro, Gonzlez-Prelcic, Nuria, Heath, Robert W	IEEE Transactions on Communications	2019	[68]
S69	Deep scanning—beam selection based on deep reinforcement learning in massive mimo wireless communication system	Kim, Minhoe, Lee, Woongsup, Cho, Dong-Ho	Electronics	2020	[69]
S70	Fast specific absorption rate aware beamforming for downlink SWIPT via deep learning	Zhang, Juping, Zheng, Gan, Krikidis, Ioannis, Zhang, Rui	IEEE GLOBECOM	2020	[70]
S71	A two-step neural network based beamforming in MIMO without reference signal	Zhao, Yuyan, Liu, Yanan, Boudreau, Gary, Sediq, Akram Bin, Abou-zeid, Hatem, Wang, Xianbin	IEEE Transactions on Mobile Computing	2019	[71]
S72	Online Reinforcement Learning for Beam Tracking and Rate Adaptation in Millimeter-wave Systems	Krunz, Marwan, Aykin, Irmak, Sarkar, Sopan, Akgun, Berk	IEEE Access	2023	[72]
S73	Deep learning coordinated beamforming for highly-mobile millimeter wave systems	Alkhateeb, Ahmed, Alex, Sam, Varkey, Paul, Li, Ying, Qu, Qi, Tujkovic, Djordje	IEEE Transactions on Mobile Computing	2018	[73]
S74	A deep learning framework for beam selection and power control in massive MIMO-millimeter-wave communications	Nguyen, Ti Ti, Nguyen, Kim-Khoa	IEEE Transactions on Wireless Communications	2022	[74]
S75	A deep learning approach to location-and orientation-aided 3d beam selection for mmwave communications	Rezaie, Sajad, De Carvalho, Elisabeth, Manchn, Carles Navarro	IEEE Transactions on Wireless Communications	2022	[75]

Continued on next page

Appendix A – continued from previous page

ID	Title	Authors	Venue	Year	Ref
S76	Deep learning enabled optimization of downlink beamforming under per-antenna power constraints: Algorithms and experimental demonstration	Zhang, Juping, Xia, Wenchao, You, Minglei, Zheng, Gan, Lambotharan, Sangarapillai, Wong, Kai-Kit	IEEE Transactions on Wireless Communications	2020	[76]
S77	A Reinforcement Learning Approach for Energy Efficient Beamforming in NOMA Systems	Liu, Yuqin, Zhong, Ruikang, Jaber, Mona	IEEE GLOBECOM	2022	[77]
S78	Multi-agent deep reinforcement learning for distributed handover management in dense mmWave networks	Sana, Mohamed, De Domenico, Antonio, Strinati, Emilio Calvanese, Clemente, Antonio	IEEE International Conference on Acoustics, SpeechI and Signal Processing	2020	[78]
S79	Efficient codebook-based beamforming algorithm for millimeter-wave massive MIMO systems	Chen, Jung-Chieh	IEEE Transactions on Vehicular Technology	2017	[79]
S80	Clustering-based codebook design for MIMO communication system	Jiang, Jing, Wang, Xiaojing, Sidhu, Guftaar Ahmad Sardar, Zhen, Li, Gao, Runchen	IEEE International Conference on Communications	2019	[80]
S81	Trainable projected gradient detector for massive overloaded MIMO channels: Data-driven tuning approach	Takabe, Satoshi, Imanishi, Masayuki, Wadayama, Tadashi, Hayakawa, Ryo, Hayashi, Kazunori	IEEE Access	2019	[81]
S82	Machine learning-based beamforming in K-user MISO interference channels	Kwon, Hyung Jun, Lee, Jung Hoon, Choi, Wan	IEEE Access	2021	[82]
S83	Deep learning for distributed channel feedback and multiuser precoding in FDD massive MIMO	Sohrabi, Foad, Attiah, Kareem M, Yu, Wei	IEEE Transactions on Wireless Communications	2021	[83]
S84	On Assessing Vulnerabilities of the 5G Networks to Adversarial Examples	Zolotukhin, Mikhail, Miraghaei, Parsa, Zhang, Di, Ha	IEEE Access	2022	[84]
S85	mmspy: Spying phone calls using mmwave radars	Basak, Suryoday, Gowda, Mahanth	IEEE Symposium on Security and Privacy	2022	[85]
S86	mmTrack: Passive multi-person localization using commodity millimeter wave radio	Wu, Chenshu, Zhang, Feng, Wang, Beibei, Liu, KJ Ray	IEEE INFOCOM	2020	[86]
S87	m-activity: Accurate and real-time human activity recognition via millimeter wave radar	Wang, Yuheng, Liu, Haipeng, Cui, Kening, Zhou, Anfu, Li, Wensheng, Ma, Huadong	IEEE International Conference on Acoustics, Speech and Signal Processing	2021	[87]
S88	EarFisher: Detecting Wireless Eavesdroppers by Stimulating and Sensing Memory (EMR)	Shen, Cheng, Huang, Jun	USENIX Symposium on Networked Systems Design and Implementation	2021	[88]
S89	Deep reinforcement learning based blind mmwave MIMO beam alignment	Raj, Vishnu, Nayak, Nancy, Kalyani, Sheetal	IEEE Transactions on Wireless Communications	2022	[89]

Continued on next page

Appendix A – continued from previous page

ID	Title	Authors	Venue	Year	Ref
S90	Beyond Codebook-Based Analog Beamforming at mmWave: Compressed Sensing and Machine Learning Methods	Pezeshki, H., Massoli, F.V., Behboodi, A., Yoo, T., Kannan, A., Boroujeni, M.T., Li, Q., Luo, T. and Soriaga, J.B	IEEE GLOBECOM	2022	[90]
S91	Learning and data-driven beam selection for mmWave communications: An angle of arrival-based approach	Antn-Haro, Carles, Mestre, Xavier	IEEE Access	2019	[91]
S92	Physical-layer security via distributed beamforming in the presence of adversaries with unknown locations	Savas, Yagiz, Hashemi, Abolfazl, Vinod, Abraham P, Sadler, Brian M, Topcu, Ufuk	IEEE International Conference on Acoustics, Speech and Signal Processing	2021	[92]
S93	Channel estimation for cell-free mmWave massive MIMO through deep learning	Jin, Yu, Zhang, Jiayi, Jin, Shi, Ai, Bo	IEEE Transactions on Vehicular Technology	2019	[93]
S94	Evaluating adversarial evasion attacks in the context of wireless communications	Flowers, Bryse, et al.	IEEE Transactions on Information Forensics and Security	2019	[94]
S95	Robust adversarial attacks against DNN-based wireless communication systems	Bahramali, Alireza, et al.	ACM Symposium on Computer and Communications Security	2021	[95]
S96	Poison Neural Network-Based mmWave Beam Selection and Detoxification With Machine Unlearning	Zhang, Zhengming, et al.	IEEE Transactions on Communications	2022	[96]
S97	Data poisoning attacks and defenses in dynamic crowdsourcing with online data quality learning	Zhao, Yuxi, et al.	IEEE Transactions on Mobile Computing	2021	[97]
S98	Backdoor federated learning-based mmWave beam selection	Zhang, Zhengming, et al.	IEEE Transactions on Communications	2022	[98]
S99	A lightweight auction framework for spectrum allocation with strong security guarantees	Cheng, Ke, et al.	IEEE INFOCOM	2020	[99]
S100	Bayesian Inference-assisted Machine Learning for Near Real-Time Jamming Detection and Classification in 5G New Radio (NR)	Jere, Shashank, et al.	IEEE Transactions on Wireless Communications	2023	[100]
S101	Securing large-scale d2d networks using covert communication and friendly jamming	Feng, Shaohan, et al.	IEEE Transactions on Wireless Communications	2023	[101]
S102	A Defensive Strategy Against Beam Training Attack in 5G mmWave Networks for Manufacturing	Dinh-Van, Son, et al.	IEEE Transactions on Information Forensics and Security	2023	[102]
S103	A trust-centric privacy-preserving blockchain for dynamic spectrum management in IoT networks	Ye, Jingwei, et al.	IEEE Internet of Things Journal	2022	[103]
S104	An efficient privacy preserving spectrum sharing framework for internet of things	Wang, Xiaoyan, et al.	IEEE Access	2020	[104]

Continued on next page

Appendix A – continued from previous page

ID	Title	Authors	Venue	Year	Ref
S105	Detection and localization of the eavesdropper in MIMO systems	Ning, Lina, et al.	IEEE Access	2020	[105]
S106	Secrecy Rate Maximization in THz-Aided Heterogeneous Networks: A Deep Reinforcement Learning Approach	Sharma, Himanshu, et al.	IEEE Transactions on Vehicular Technology	2023	[106]
S107	On mitigation of pilot spoofing attack	Tugnait, Jitendra K	IEEE Intl. Conf. on Acoustics, Speech and Signal Processing	2017	[107]
S108	Physical layer spoofing attack detection in MmWave massive MIMO 5G networks	Li, Weiwei, et al.	IEEE Access	2021	[108]
S109	Exploiting beam features for spoofing attack detection in mmWave 60-GHz IEEE 802.11 ad networks	Wang, Ning, et al.	IEEE Transactions on Wireless Communications	2021	[109]
S110	Concurrent Spoofing-Jamming Attack in Massive MIMO Systems with a Full-Duplex Multi-Antenna Eavesdropper	Alageli, Mahmoud, et al.	IEEE Transactions on Vehicular Technology	2023	[110]

References

[1] S. Khunteta, P. Saikrishna, A. Agrawal, A. Kumar, and A. K. R. Chavva, "Rf-sensing: A new way to observe surroundings," *IEEE Access*, vol. 10, pp. 129653–129665, 2022.

[2] R. I. Rony, E. Lopez-Aguilera, and E. Garcia-Villegas, "Dynamic spectrum allocation following machine learning-based traffic predictions in 5g," *IEEE access*, vol. 9, pp. 143458–143472, 2021.

[3] C. Ganewattha, Z. Khan, M. Latva-Aho, and J. J. Lehtomaki, "Confidence aware deep learning driven wireless resource allocation in shared spectrum bands," *IEEE Access*, vol. 10, pp. 34945–34959, 2022.

[4] O. M. Gul, M. Kulhandjian, B. Kantarci, A. Touazi, C. Ellement, and C. D'amours, "Secure industrial iot systems via rf fingerprinting under impaired channels with interference and noise," *IEEE Access*, vol. 11, pp. 26289–26307, 2023.

[5] M. Chen, W. Liu, N. Zhang, J. Li, Y. Ren, M. Yi, and A. Liu, "Gpds: A multi-agent deep reinforcement learning game for anti-jamming secure computing in mec network," *Expert Systems with Applications*, vol. 210, p. 118394, 2022.

[6] F. Restuccia, S. D'Oro, A. Al-Shawabka, B. C. Rendon, K. Chowdhury, S. Ioannidis, and T. Melodia, "Generalized wireless adversarial deep learning," in *Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning*, pp. 49–54, 2020.

[7] V. Jain, B. Kumar, and A. Gupta, "Cybertwin-driven resource allocation using deep reinforcement learning in 6g-enabled edge environment," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5708–5720, 2022.

[8] Y. Ding, Y. Feng, W. Lu, S. Zheng, N. Zhao, L. Meng, A. Nallanathan, and X. Yang, "Online edge learning offloading and resource management for uav-assisted mec secure communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 17, no. 1, pp. 54–65, 2022.

[9] S. Yu, X. Chen, Z. Zhou, X. Gong, and D. Wu, "When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5g ultradense network," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2238–2251, 2020.

[10] Q. Guo, F. Tang, and N. Kato, "Federated reinforcement learning-based resource allocation for d2d-aided digital twin edge networks in 6g industrial iot," *IEEE Transactions on Industrial Informatics*, 2022.

[11] K. Wang, H. Li, Z. Ding, and P. Xiao, "Reinforcement learning based latency minimization in secure noma-mec systems with hybrid sic," *IEEE transactions on wireless communications*, vol. 22, no. 1, pp. 408–422, 2022.

[12] F. O. Catak, M. Kuzlu, H. Tang, E. Catak, and Y. Zhao, "Security hardening of intelligent reflecting surfaces against adversarial machine learning attacks," *IEEE Access*, vol. 10, pp. 100267–100275, 2022.

[13] Z. Lv, D. Chen, H. Feng, R. Lou, and H. Wang, "Beyond 5g for digital twins of uavs," *Computer Networks*, vol. 197, p. 108366, 2021.

[14] C.-H. Lin, C.-C. Wu, K.-F. Chen, and T.-S. Lee, "A variational autoencoder-based secure transceiver design using deep learning," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1–7, IEEE, 2020.

[15] M. Merluzzi, T. Borsos, N. Rajatheva, A. A. Benczur, H. Farhadi, T. Yassine, M. D. Muck, S. Barmpounakis, E. C. Strinati, D. Dampahalage, *et al.*, "The hexa-x project vision on artificial intelligence and machine learning-driven communication and computation co-design for 6g," *IEEE Access*, 2023.

[16] J. Shi, C. Li, Y. Guan, P. Cong, and J. Li, "Multi-uav-assisted computation offloading in dt-based networks: A distributed deep reinforcement learning approach," *Computer Communications*, vol. 210, pp. 217–228, 2023.

[17] H. Sharma, N. Kumar, and R. Tekchandani, "Mitigating jamming attack in 5g heterogeneous networks: A federated deep reinforcement learning approach," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2439–2452, 2022.

[18] Z. Liu, C. Xu, E. Sie, G. Singh, and D. Vasisht, "Exploring practical vulnerabilities of machine learning-based wireless systems," in *20th USENIX Symposium on Networked Systems Design and Implementation (NSDI 23)*, pp. 1801–1817, 2023.

[19] Y. Cui, T. Lv, W. Ni, and A. Jamalipour, "Digital twin-aided learning for managing reconfigurable intelligent surface-assisted, uplink, user-centric cell-free systems," *arXiv preprint arXiv:2302.05073*, 2023.

[20] P. Hu, W. Li, R. Spolaor, and X. Cheng, "mmecho: A mmwave-based acoustic eavesdropping method," in *Proceedings of the ACM Turing Award Celebration Conference-China 2023*, pp. 138–140, 2023.

[21] R. Fantacci and B. Picano, "A d2d-aided federated learning scheme with incentive mechanism in 6g networks," *IEEE Access*, vol. 11, pp. 107–117, 2022.

[22] T. T. Vu, D. T. Ngo, H. Q. Ngo, M. N. Dao, N. H. Tran, and R. H. Middleton, "Joint resource allocation to minimize execution time of federated learning in cell-free massive mimo," *IEEE Internet of Things Journal*, vol. 9, no. 21, pp. 21736–21750, 2022.

[23] G. Wang, F. Xu, H. Zhang, and C. Zhao, "Joint resource management for mobility supported federated learning in internet of vehicles," *Future Generation Computer Systems*, vol. 129, pp. 199–211, 2022.

[24] F. O. Catak, M. Kuzlu, S. Sarp, E. Catak, and U. Cali, "Mitigating attacks on artificial intelligence-based spectrum sensing for cellular network signals," in *2022 IEEE Globecom Workshops (GC Wkshps)*, pp. 1371–1376, IEEE, 2022.

[25] Y. Liu, Z. Ma, Z. Yan, Z. Wang, X. Liu, and J. Ma, "Privacy-preserving federated k-means for proactive caching in next generation cellular networks," *Information Sciences*, vol. 521, pp. 14–31, 2020.

[26] Y. Hu, H. Huang, and N. Yu, "Resource allocation and device pairing for energy-efficient noma-enabled federated edge learning," *Computer Communications*, vol. 208, pp. 283–293, 2023.

[27] T. E. T. Djaidja, B. Brik, S. M. Senouci, and Y. Ghamri-Doudane, "Adaptive resource reservation to survive against adversarial resource selection jamming attacks in 5g nr-v2x distributed mode 2," in *ICC 2022-IEEE International Conference on Communications*, pp. 3406–3411, IEEE, 2022.

[28] Y. Peng, X. Xue, A. K. Bashir, X. Zhu, Y. D. Al-Otaibi, U. Tariq, and K. Yu, "Securing radio resources allocation with deep reinforcement learning for ioe services in next-generation wireless networks," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 2991–3003, 2022.

[29] B. M. Pati, M. Kaneko, and A. Taparugssanagorn, "A deep convolutional neural network based transfer learning method for non-cooperative spectrum sensing," *IEEE Access*, vol. 8, pp. 164529–164545, 2020.

[30] S. Solanki, V. Dehalwar, J. Choudhary, M. L. Kolhe, and K. Ogura, "Spectrum sensing in cognitive radio using cnn-rnn and transfer learning," *IEEE Access*, vol. 10, pp. 113482–113492, 2022.

[31] Z. Luo, S. Zhao, Z. Lu, J. Xu, and Y. E. Sagduyu, "When attackers meet ai: Learning-empowered attacks in cooperative spectrum sensing," *IEEE Transactions on Mobile Computing*, vol. 21, no. 5, pp. 1892–1908, 2020.

[32] Y. E. Sagduyu, Y. Shi, and T. Erpek, "Adversarial deep learning for over-the-air spectrum poisoning attacks," *IEEE Transactions on Mobile Computing*, vol. 20, no. 2, pp. 306–319, 2019.

[33] B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Channel-aware adversarial attacks against deep learning-based wireless signal classifiers," *IEEE Transactions on Wireless Communications*, vol. 21, no. 6, pp. 3868–3880, 2021.

[34] J. Li, H. Zhao, Y. Huang, M. Zhang, and S. P. Lal, "Deep learning driven physical layer security for a simultaneously wireless information and power transfer network," *Alexandria Engineering Journal*, vol. 61, no. 9, pp. 7429–7439, 2022.

[35] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R.-F. Liao, and J. Chen, "Threshold-free physical layer authentication based on machine learning for industrial wireless cps," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6481–6491, 2019.

[36] B. Yang, X. Cao, O. Omotere, X. Li, Z. Han, and L. Qian, "Improving medium access efficiency with intelligent spectrum learning," *IEEE Access*, vol. 8, pp. 94484–94498, 2020.

[37] W. Zhang, M. Feng, M. Krunz, and A. H. Y. Abyaneh, "Signal detection and classification in shared spectrum: A deep learning approach," in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*, pp. 1–10, IEEE, 2021.

[38] A. Olesiński and Z. Piotrowski, "A radio frequency region-of-interest convolutional neural network for wideband spectrum sensing," *Sensors*, vol. 23, no. 14, p. 6480, 2023.

[39] L. Baldesi, F. Restuccia, and T. Melodia, "Charm: Nextg spectrum sharing through data-driven real-time o-ran dynamic control," in *IEEE INFOCOM 2022-IEEE Conference on Computer Communications*, pp. 240–249, IEEE, 2022.

[40] E. Perenda, S. Rajendran, G. Bovet, S. Pollin, and M. Zheleva, "Learning the unknown: Improving modulation classification performance in unseen scenarios," in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications*, pp. 1–10, IEEE, 2021.

[41] H. Song, L. Liu, J. Ashdown, and Y. Yi, "A deep reinforcement learning framework for spectrum management in dynamic spectrum access," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11208–11218, 2021.

[42] M. Kulin, T. Kazaz, I. Moerman, and E. De Poorter, "End-to-end learning from spectrum data: A deep learning approach for wireless signal identification in spectrum monitoring applications," *IEEE access*, vol. 6, pp. 18484–18501, 2018.

[43] R. Mennes, M. Claeys, F. A. De Figueiredo, I. Jabandžić, I. Moerman, and S. Latré, "Deep learning-based spectrum prediction collision avoidance for hybrid wireless environments," *IEEE Access*, vol. 7, pp. 45818–45830, 2019.

[44] M. Camelo, R. Mennes, A. Shahid, J. Struye, C. Donato, I. Jabandzic, S. Giannoulis, F. Mahfoudhi, P. Maddala, I. Seskar, *et al.*, "An ai-based incumbent protection system for collaborative intelligent radio networks," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 16–23, 2020.

[45] M. Clark and K. Psounis, "Optimizing primary user privacy in spectrum sharing systems," *IEEE/ACM Transactions on Networking*, vol. 28, no. 2, pp. 533–546, 2020.

[46] S. Liu, Y. Xu, X. Chen, X. Wang, M. Wang, W. Li, Y. Li, and Y. Xu, "Pattern-aware intelligent anti-jamming communication: A sequential deep reinforcement learning approach," *IEEE Access*, vol. 7, pp. 169204–169216, 2019.

[47] N. Van Huynh, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, ""jam me if you can:" defeating jammer with deep dueling neural network architecture and ambient backscattering augmented communications," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 11, pp. 2603–2620, 2019.

[48] N. Van Huynh, D. T. Hoang, D. N. Nguyen, and E. Dutkiewicz, "Deepfake: Deep dueling-based deception strategy to defeat reactive jammers," *IEEE Transactions on Wireless Communications*, vol. 20, no. 10, pp. 6898–6914, 2021.

[49] A. H. Celdrán, P. M. S. Sánchez, G. Bovet, G. M. Pérez, and B. Stiller, "Cyberspec: Behavioral fingerprinting for intelligent attacks detection on crowdsensing spectrum sensors," *IEEE Transactions on Dependable and Secure Computing*, 2023.

[50] Q. Pan, J. Wu, X. Zheng, W. Yang, and J. Li, "Differential privacy and irs empowered intelligent energy harvesting for 6g internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22109–22122, 2021.

[51] F. Tang, C. Wen, X. Chen, and N. Kato, "Federated learning for intelligent transmission with space-air-ground integrated network (sagin) toward 6g," *IEEE Network*, 2022.

[52] H.-H. Chang, Y. Song, T. T. Doan, and L. Liu, "Federated multi-agent deep reinforcement learning (fed-madrl) for dynamic spectrum access," *IEEE Transactions on Wireless Communications*, 2023.

[53] S. Goekceli, O. Cepheli, S. T. Basaran, G. K. Kurt, G. Dartmann, and G. Ascheid, "How effective is the artificial noise? real-time analysis of a phy security scenario," in *2017 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–7, IEEE, 2017.

[54] G. Han, J. Tu, L. Liu, M. Martínez-García, and Y. Peng, "Anomaly detection based on multidimensional data processing for protecting vital devices in 6g-enabled massive iiot," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5219–5229, 2021.

[55] S. Shao, M. Nazzal, A. Khreishah, and M. Ayyash, "Self-optimizing data offloading in mobile heterogeneous radio-optical networks: A deep reinforcement learning approach," *IEEE Network*, vol. 36, no. 2, pp. 100–106, 2022.

[56] F. O. Catak, M. Kuzlu, E. Catak, U. Cali, and O. Guler, "Defensive distillation-based adversarial attack mitigation method for channel estimation using deep learning models in next-generation wireless networks," *IEEE Access*, vol. 10, pp. 98191–98203, 2022.

[57] Z. Wang, J. Hu, G. Min, Z. Zhao, and J. Wang, "Data-augmentation-based cellular traffic prediction in edge-computing-enabled smart city," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4179–4187, 2020.

[58] V. Perifanis, N. Pavlidis, R.-A. Koutsiamanis, and P. S. Efraimidis, "Federated learning for 5g base station traffic forecasting," *Computer Networks*, vol. 235, p. 109950, 2023.

[59] L. F. Maimó, Á. L. P. Gómez, F. J. G. Clemente, M. G. Pérez, and G. M. Pérez, "A self-adaptive deep learning-based system for anomaly detection in 5g networks," *Ieee Access*, vol. 6, pp. 7700–7712, 2018.

[60] H. Zhang and Z. Li, "Anomaly detection approach for urban sensing based on credibility and time-series analysis optimization model," *IEEE Access*, vol. 7, pp. 49102–49110, 2019.

[61] L. Liu, G. Han, Y. He, and J. Jiang, "Fault-tolerant event region detection on trajectory pattern extraction for industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2072–2080, 2019.

[62] D. Li, S. Wang, H. Zhao, and X. Wang, "Context-and-social-aware online beam selection for mmwave vehicular communications," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 8603–8615, 2020.

[63] Y. Yang, Z. Gao, Y. Ma, B. Cao, and D. He, "Machine learning enabling analog beam selection for concurrent transmissions in millimeter-wave v2v communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9185–9189, 2020.

[64] W. Xu, F. Gao, X. Tao, J. Zhang, and A. Alkhateeb, "Computer vision aided mmwave beam alignment in v2x communications," *IEEE Transactions on Wireless Communications*, vol. 22, no. 4, pp. 2699–2714, 2022.

[65] H. Echigo, Y. Cao, M. Bouazizi, and T. Ohtsuki, "A deep learning-based low overhead beam selection in mmwave communications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 682–691, 2021.

[66] M. S. Sim, Y.-G. Lim, S. H. Park, L. Dai, and C.-B. Chae, "Deep learning-based mmwave beam selection for 5g nr/6g with sub-6 ghz channel information: Algorithms and prototype validation," *IEEE Access*, vol. 8, pp. 51634–51646, 2020.

[67] M. Alrabeiah and A. Alkhateeb, "Deep learning for mmwave beam and blockage prediction using sub-6 ghz channels," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5504–5518, 2020.

[68] A. Klautau, N. González-Prelcic, and R. W. Heath, "Lidar data for deep learning-based mmwave beam-selection," *IEEE Wireless Communications Letters*, vol. 8, no. 3, pp. 909–912, 2019.

[69] M. Kim, W. Lee, and D.-H. Cho, "Deep scanning—beam selection based on deep reinforcement learning in massive mimo wireless communication system," *Electronics*, vol. 9, no. 11, p. 1844, 2020.

[70] J. Zhang, G. Zheng, I. Krikidis, and R. Zhang, "Fast specific absorption rate aware beamforming for downlink swipt via deep learning," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 16178–16182, 2020.

[71] Y. Zhao, Y. Liu, G. Boudreau, A. B. Sediq, H. Abou-zeid, and X. Wang, "A two-step neural network based beamforming in mimo without reference signal," in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, 2019.

[72] M. Krunz, I. Aykin, S. Sarkar, and B. Akgun, "Online reinforcement learning for beam tracking and rate adaptation in millimeter-wave systems," *IEEE Transactions on Mobile Computing*, 2023.

[73] A. Alkhateeb, S. Alex, P. Varkey, Y. Li, Q. Qu, and D. Tujkovic, "Deep learning coordinated beamforming for highly-mobile millimeter wave systems," *IEEE Access*, vol. 6, pp. 37328–37348, 2018.

[74] T. T. Nguyen and K.-K. Nguyen, "A deep learning framework for beam selection and power control in massive mimo-millimeter-wave communications," *IEEE Transactions on Mobile Computing*, 2022.

[75] S. Rezaie, E. De Carvalho, and C. N. Manchón, "A deep learning approach to location-and orientation-aided 3d beam selection for mmwave communications," *IEEE Transactions on Wireless Communications*, vol. 21, no. 12, pp. 11110–11124, 2022.

[76] J. Zhang, W. Xia, M. You, G. Zheng, S. Lambotharan, and K.-K. Wong, "Deep learning enabled optimization of downlink beamforming under per-antenna power constraints: Algorithms and experimental demonstration," *IEEE Transactions on Wireless Communications*, vol. 19, no. 6, pp. 3738–3752, 2020.

[77] Y. Liu, R. Zhong, and M. Jaber, "A reinforcement learning approach for energy efficient beamforming in noma systems," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pp. 3827–3832, IEEE, 2022.

[78] M. Sana, A. De Domenico, E. C. Strinati, and A. Clemente, "Multi-agent deep reinforcement learning for distributed handover management in dense mmwave networks," in *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 8976–8980, IEEE, 2020.

[79] J.-C. Chen, "Efficient codebook-based beamforming algorithm for millimeter-wave massive mimo systems," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 9, pp. 7809–7817, 2017.

[80] J. Jiang, X. Wang, G. A. S. Sidhu, L. Zhen, and R. Gao, "Clustering-based codebook design for mimo communication system," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2019.

[81] S. Takabe, M. Imanishi, T. Wadayama, R. Hayakawa, and K. Hayashi, "Trainable projected gradient detector for massive overloaded mimo channels: Data-driven tuning approach," *IEEE Access*, vol. 7, pp. 93326–93338, 2019.

[82] H. J. Kwon, J. H. Lee, and W. Choi, "Machine learning-based beamforming in k-user miso interference channels," *IEEE Access*, vol. 9, pp. 28066–28075, 2021.

[83] F. Sohrabi, K. M. Attiah, and W. Yu, "Deep learning for distributed channel feedback and multiuser precoding in fdd massive mimo," *IEEE Transactions on Wireless Communications*, vol. 20, no. 7, pp. 4044–4057, 2021.

[84] M. Zolotukhin, P. Miraghaei, D. Zhang, and T. Hämäläinen, "On assessing vulnerabilities of the 5g networks to adversarial examples," *IEEE Access*, vol. 10, pp. 126285–126303, 2022.

[85] S. Basak and M. Gowda, "mmspy: Spying phone calls using mmwave radars," in *2022 IEEE Symposium on Security and Privacy (SP)*, pp. 1211–1228, IEEE, 2022.

[86] C. Wu, F. Zhang, B. Wang, and K. R. Liu, "mmtrack: Passive multi-person localization using commodity millimeter wave radio," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pp. 2400–2409, IEEE, 2020.

[87] Y. Wang, H. Liu, K. Cui, A. Zhou, W. Li, and H. Ma, "m-activity: Accurate and real-time human activity recognition via millimeter wave radar," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 8298–8302, IEEE, 2021.

[88] C. Shen and J. Huang, "Earfisher: Detecting wireless eavesdroppers by stimulating and sensing memory (emr)," in *18th USENIX Symposium on Networked Systems Design and Implementation (NSDI 21)*, pp. 873–886, 2021.

[89] V. Raj, N. Nayak, and S. Kalyani, "Deep reinforcement learning based blind mmwave mimo beam alignment," *IEEE Transactions on Wireless Communications*, vol. 21, no. 10, pp. 8772–8785, 2022.

[90] H. Pezeshki, F. V. Massoli, A. Behboodi, T. Yoo, A. Kannan, M. T. Boroujeni, Q. Li, T. Luo, and J. B. Soriaga, "Beyond codebook-based analog beamforming at mmwave: Compressed sensing and machine learning methods," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*, pp. 776–781, IEEE, 2022.

[91] C. Antón-Haro and X. Mestre, "Learning and data-driven beam selection for mmwave communications: An angle of arrival-based approach," *IEEE Access*, vol. 7, pp. 20404–20415, 2019.

[92] Y. Savas, A. Hashemi, A. P. Vinod, B. M. Sadler, and U. Topcu, "Physical-layer security via distributed beamforming in the presence of adversaries with unknown locations," in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 4685–4689, IEEE, 2021.

[93] Y. Jin, J. Zhang, B. Ai, and X. Zhang, "Channel estimation for mmwave massive mimo with convolutional blind denoising network," *IEEE Communications Letters*, vol. 24, no. 1, pp. 95–98, 2019.

[94] B. Flowers, R. M. Buehrer, and W. C. Headley, "Evaluating adversarial evasion attacks in the context of wireless communications," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1102–1113, 2019.

[95] A. Bahramali, M. Nasr, A. Houmansadr, D. Goeckel, and D. Towsley, "Robust adversarial attacks against dnn-based wireless communication systems," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pp. 126–140, 2021.

[96] Z. Zhang, M. Tian, C. Li, Y. Huang, and L. Yang, "Poison neural network-based mmwave beam selection and detoxification with machine unlearning," *IEEE Transactions on Communications*, vol. 71, no. 2, pp. 877–892, 2022.

[97] Y. Zhao, X. Gong, F. Lin, and X. Chen, "Data poisoning attacks and defenses in dynamic crowdsourcing with online data quality learning," *IEEE Transactions on Mobile Computing*, 2021.

[98] Z. Zhang, R. Yang, X. Zhang, C. Li, Y. Huang, and L. Yang, "Backdoor federated learning-based mmwave beam selection," *IEEE Transactions on Communications*, vol. 70, no. 10, pp. 6563–6578, 2022.

[99] K. Cheng, L. Wang, Y. Shen, Y. Liu, Y. Wang, and L. Zheng, "A lightweight auction framework for spectrum allocation with strong security guarantees," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications*, pp. 1708–1717, IEEE, 2020.

[100] S. Jere, Y. Wang, I. Aryendu, S. Dayekh, and L. Liu, "Bayesian inference-assisted machine learning for near real-time jamming detection and classification in 5g new radio (nr)," *IEEE Transactions on Wireless Communications*, 2023.

[101] S. Feng, X. Lu, S. Sun, D. Niyato, and E. Hossain, "Securing large-scale d2d networks using covert communication and friendly jamming," *IEEE Transactions on Wireless Communications*, 2023.

[102] S. Dinh-Van, T. M. Hoang, B. B. Cebecioglu, D. S. Fowler, Y. K. Mo, and M. D. Higgins, "A defensive strategy against beam training attack in 5g mmwave networks for manufacturing," *IEEE Transactions on Information Forensics and Security*, 2023.

[103] J. Ye, X. Kang, Y.-C. Liang, and S. Sun, "A trust-centric privacy-preserving blockchain for dynamic spectrum management in iot networks," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13263–13278, 2022.

[104] X. Wang, M. Umehira, B. Han, H. Zhou, P. Li, and C. Wu, "An efficient privacy preserving spectrum sharing framework for internet of things," *IEEE Access*, vol. 8, pp. 34675–34685, 2020.

[105] L. Ning, B. Li, C. Zhao, Y. Tao, and X. Wang, "Detection and localization of the eavesdropper in mimo systems," *IEEE Access*, vol. 8, pp. 94984–94993, 2020.

[106] H. Sharma, N. Kumar, I. Budhiraja, and A. Barnawi, "Secrecy rate maximization in thz-aided heterogeneous networks: A deep reinforcement learning approach," *IEEE Transactions on Vehicular Technology*, 2023.

[107] J. K. Tugnait, "On mitigation of pilot spoofing attack," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2097–2101, IEEE, 2017.

[108] W. Li, N. Wang, L. Jiao, and K. Zeng, "Physical layer spoofing attack detection in mmwave massive mimo 5g networks," *IEEE Access*, vol. 9, pp. 60419–60432, 2021.

[109] N. Wang, L. Jiao, P. Wang, W. Li, and K. Zeng, "Exploiting beam features for spoofing attack detection in mmwave 60-ghz ieee 802.11 ad networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 5, pp. 3321–3335, 2021.

[110] M. Alageli, A. Ikhlef, and J. Chambers, "Concurrent spoofing-jamming attack in massive mimo systems with a full-duplex multi-antenna eavesdropper," *IEEE Transactions on Vehicular Technology*, 2023.