



Artificial Intelligence in Computer Networks: An Organized Overview of Uses, Methods, Difficulties, and Prospects

DOI: <https://doi.org/10.5281/zenodo.23163045>

Yash D. Turkey

***Corresponding Author:** Research Student, M.Sc. Computer Science, R.A. Arts, Shri M.K. Commerce and Shri S.R. Rath Science College, Washim 444505, Maharashtra, India.

yasht.1702@gmail.com

ORCID: 0009-0001-5685-5089

ABSTRACT

Artificial Intelligence (AI) is increasingly becoming an integral part of the modern computer network design, management, and optimisation. Whereas traditional systems rely on rules set by hand, AI based systems can adapt to operational data and make decisions based on changing network conditions. The paper introduces a systematic review of the AI and machine-learning (ML) techniques presented in the networking literature, and primarily based on peer-reviewed journal articles, IEEE survey papers and conference proceedings published between 2015 and 2024. The methods studied are supervised learning, unsupervised learning, reinforcement learning, deep learning, graph-based learning, federated learning and AI-based 5G/6G networking. The review also discusses the key applications such as traffic classification and prediction, adaptive routing, software-defined networking, network security and intrusion detection, resource allocation, edge computing, network slicing, intelligent wireless networking, and quality-of-service management. In all these facets, common challenges are the lack of representative labeled data, limited data interpretability for learned decisions, computational limitations on time-sensitive inferences, susceptibility to adversarial data manipulation, and scalability issues when the network is heterogeneous. The paper specifies the following directions for future research: explainable AI, privacy-preserving federated learning, digital-twin-based network management, and more autonomous network architectures. In summary, the evidence suggests that AI has the potential to enhance network security, flexibility, and efficiency, but there are still challenges to be addressed, particularly in terms of interoperability, trust, standardisation, and the ability to process large quantities of real-time telemetry.

KEYWORDS: 6G Wireless Networks, Reinforcement Learning, Federated Learning, Artificial Intelligence, Machine Learning, Computer Networks, Deep Learning, Software-Defined Networking, Network Security, and Systematic Review.

1. OVERVIEW

The goals of throughput, latency, reliability, and security are all critical for modern computer networks, and must be met simultaneously, in a network that spans widely distributed and heterogeneous infrastructures. Requirements cover the cloud, edge, wired and wireless. Despite the promise of programmable architectures like Software-Defined Networking (SDN), a lot of operational tasks are still being performed by manually written protocols, heuristic rules and frequent manual intervention by network operators. The volume, diversity, and temporal variability of these services and systems, such as cloud-based applications, Internet of Things (IoT) devices, and advanced mobile networks, will only increase and make these approaches more difficult to maintain [1].

Patterns can be extracted from network telemetry, traffic measurements and operational log files using AI, and specifically machine learning (ML) to help with prediction and adaptive control [2]. There have been multiple technical advancements that have brought AI and networking together. First, the use of deep learning can be used to effectively learn from high-dimensional data, minimizing the need for hand-crafted features [3]. Second, programmable architectures, such as SDN in particular, isolate the control functions from the packet forwarding functions and provide interfaces for the deployment of learned policies. Third, reinforcement learning (RL) is a framework for sequential decision making in an uncertain environment. Decision processes can be defined as functions whose agent engages with the network environment to optimize the network policy and which can be formulated as networking functions like routing and congestion control [4].

The goals of this review are: (i) to determine which AI/ML techniques are most commonly used for networking problems; (ii) to correlate the different techniques with the major networking applications; (iii) to summarize technical and operational restrictions reported in the literature; and (iv) to point out interesting directions for future research.

2. CONTRIBUTION OF PAPER

- I. The paper is a systematic literature review of how AI and ML are used in computer networks. It covers peer-reviewed journals, IEEE surveys and conference papers from 2015 to 2024. It follows a defined search strategy (IEEE Xplore, ACM Digital Library, SpringerLink and arXiv), with set inclusion and exclusion criteria.
- II. The paper maps AI/ML techniques to networking applications in a two-dimensional scheme (Table I). The techniques are supervised, unsupervised, reinforcement, deep and graph-based learning, and federated learning. The applications include traffic classification and prediction, adaptive routing, SDN/KDN, intrusion detection, QoS and resource management, network slicing and edge computing, 5G/6G wireless networking, and blockchain–AI convergence.
- III. The paper identifies the main obstacles to adoption: scarce labeled data, limited interpretability, real-time computation limits, adversarial vulnerability, weak generalization across topologies and traffic, and lack of standards. From these it sets out future research directions: explainable

AI, privacy-preserving federated learning, digital-twin networks, autonomous networks, AI-native 6G architectures, and adversarially robust, secure model pipelines.

3. RESEARCH METHODS

The systematic literature review (SLR) was carried out along three main phases: planning SLR, searching the literature and choosing the studies, synthesizing and reporting the results of the literature review. The procedure was modified to suit the nature of networking and AI research, allowing a comparison of the studies selected not only in terms of the networking goal, but also in terms of the learning approach.

A. Search Strategy

The search terms used for finding relevant literature were "machine learning," "deep learning," "reinforcement learning," "computer networks," "software-defined networking," "network security," "routing," and "wireless networks. The search was performed in IEEE Xplore, the ACM Digital Library, SpringerLink and arXiv, and the timeframe of the publications is from 2015 to 2024. Survey articles were given more weight since they combine the evidence from a very large number of primary articles, and specifically from IEEE Communications Surveys & Tutorials. Original studies were cited extensively and where they also contributed to the technical aspects.

B. General Inclusion and Exclusion Criteria

The study was included if it met the following conditions: (i) it used an AI or ML technique for a networking problem; (ii) it offered adequate methodological detail to enable the evaluation of the networking application; and (iii) it was published in a peer reviewed venue or a widely cited preprint with an explicit engineering contribution. The studies that did not relate to the networked domain, did not sufficiently describe the methodology, or were primarily built on results of an existing survey in the networked domain were excluded.

C. Synthesis Method

The selected studies were categorized into two types: (1) type of networking application, and (2) AI/ML technique used. The two-dimensional coding scheme is applied to the operational networking functions and learning paradigms in the short summary of Table I. The resulting organization is consistent with the perspective of surveys of broader networking [1].

TABLE I: LINKING NETWORKING APPLICATION DOMAINS TO AI/ML TECHNIQUES

AI/ML Technique	Representative Networking Applications	Key References
Supervised Learning (SVM, Random Forest, kNN)	Traffic classification, malware/intrusion detection, fault diagnosis	[11], [13], [14]
Unsupervised Learning	Anomaly detection, traffic-pattern	[5], [15]

(clustering, autoencoders)	discovery, network profiling	
Reinforcement Learning	Adaptive routing, dynamic resource allocation, congestion control	[4], [26]
Deep Learning / Graph Neural Networks	Network modeling, KPI prediction, encrypted-traffic analysis	[3], [8], [9], [25]
Federated Learning	Privacy-preserving edge intelligence, distributed model training	[6], [22]

4. AI/ML METHODS USED IN NETWORKING

AI/ML techniques used in networking vary in terms of the type of data that they need, how they learn, and the types of decisions they can support. The literature reviewed reveals the following to be the main paradigms.

A. Supervised Learning

Supervised learning is commonly used for networks where labels are available for network observations. Several methods like Support Vector Machines (SVMs), decision trees, random forest, k-nearest neighbors have been used for various applications including traffic classification and intrusion detection [11]. These methods can produce decision structures that are fairly easy to understand and in many cases can require relatively little training. They are only effective if the training data they use to label is representative, high quality, and up-to-date.

B. Unsupervised Learning

When it is costly or impractical to get reliable labels for observations of networks, unsupervised learning can be useful. For telemetry anomaly detection, traffic profiling and dimensionality reduction, clustering techniques like k-means and SOMs have been investigated, as well as representation-learning techniques like autoencoders. The methods are especially useful for identifying previously unknown or changing anomalies in a network [5] without prior labels for each abnormal state.

C. Reinforcement Learning

Reinforcement learning (RL) is a technique for sequential decision making that enables an agent to learn a policy from experience by exploring an environment and based on the rewards received from its actions. This formulation has been studied for adaptive routing, congestion control, bandwidth allocation, and context-aware wireless resource management, among others, in networking. By learning how to adjust control policies in response to network changes instead of relying solely on precomputed policies, RL and deep RL can adapt to changes in the network [26].

D. Graph Based Networks and Deep Learning

Since deep neural networks can learn hierarchical representations directly from raw or minimally processed input data, they are well suited to complex networking data [3]. Networks are of particular interest as they can be naturally modeled as a graph of nodes and links, making Graph Neural Networks

(GNNs) relevant. For instance, when using RouteNet, the system learns the relationships between topology, routing, and traffic conditions in order to estimate per-flow delay, jitter, and packet loss, minimizing the need for packet-level simulation, which is expensive in terms of computation [8]. Later studies have focused on more extensive and complicated network structures, such as traffic that is not Markovian [9].

E. Federated Learning

Federated learning (FL) is a paradigm that allows multiple users or network nodes to cooperatively learn a shared model without sharing their individual observations with a central server. This distributed configuration is desirable in privacy-restricted environments at the edge since it can restrict the space for sensitive telemetry [6]. In networking, FL has been proposed for drones network, vehicles network, and 5G edge intelligence. Several methods integrate FL with blockchain technologies to improve coordination and trust in the participating nodes [22].

5. AI APPLICATIONS IN COMPUTER NETWORKS

A. Theory and application of traffic engineering, traffic prediction and classification.

Traffic forecasting and traffic classification are fundamental to Quality of Service (QoS) provisioning, capacity planning and anomaly detection. If content of payloads is not accessible using encryption, other machine learning (ML) classifiers based on statistical features of packets or flows may provide an alternative to port-based classification and deep packet inspection (DPI) [11]. Time-series methods or recurrent or graph-based neural models may also be used to forecast traffic conditions, which could then enable resource or route adjustments ahead of time before congestion or demand reaches critical levels [12].

B. Concise explanation for the topic: Adaptive and Intelligent Routing.

Road or shortest path routing usually depends on the predefined metrics and procedure. AI-based routing can instead take into account application needs, traffic congestion, and predicted traffic conditions on links when choosing routing. RL agents may be used to learn such policies in an SDN environment where users have objectives to consider such as latency, throughput, and load distribution, while models based on GNNs can provide performance estimates to inform these decisions [9].

C. Knowledge-Defined and Software-Defined Networking

Separation of control and data planes in SDN allows for network management through AI. A centralized controller's role is to keep a global state of the network and provide programmable mechanisms for enforcing learned policies [2]. Knowledge-Defined Networking (KDN) builds on this by adding a knowledge plane which uses network telemetry to extract knowledge and then pass back to SDN management functions. It is a closed-loop system which can cause the network to be more autonomous and self-optimizing [10].

D. Network Security and Intrusion Detection.

One significant application is network security, where AI-driven methods are employed to enhance

security protocols and combat cyber threats. While relying on pre-defined signatures, ML based intrusion detection systems (IDSs) can learn the statistical properties of both benign and malicious traffic, thus they can detect attack variants that were not explicitly coded beforehand [13]. Another public intrusion-detection dataset, which consists of raw or partially processed traffic, has also been used to test deep learning [14]. The extended visibility of the network by the SDN controller can also be utilized as a tool to identify volumetric and distributed attacks like DDoS events [15]. The vulnerabilities of centralized, programmable SDN control have also been exploited using AI technologies [16].

E. Quality of Service, Resource and Fault Management

QoS and fault management can be facilitated with the help of AI, as it can detect service degradation before it becomes a visible failure and can facilitate automated diagnosis and recovery. Using ML-based resource management techniques, bandwidth, computing power, and queueing resources can be dynamically assigned based on the demand prediction. This flexibility in allocation can lessen the need for worst case provisioning techniques [12].

F. Network Slicing and Edge Computing

The greater proximity of inference and, in some cases, model training to sources of network data, with the help of AI and edge computing. This can help decrease response latency and the amount of traffic directed to centralized infrastructure. AI can then be used to dynamically allocate virtualized resources to logically separate services sharing a common physical infrastructure, to efficiently utilize available resources while meeting the performance requirements of each network slice [19].

G. AI in Wireless Networks and 5G/6G

AI is now seen as a fundamental element of 5G and 6G wireless technology, where it has been used for spectrum management, beamforming and mobility control [7]. Large-scale traffic analysis [23], mobile multimedia and physical-layer processing [23] have been explored in several layers of the wireless stack in the context of deep learning. In the context of intelligent transportation networks and vehicles, the application of ML in connected mobility in future 6G environments has also been thoroughly explored [17]. AI-based network management is essential for the future for the healthcare-IoT and industrial-IoT systems, which have other requirements such as low latency, reliability, and device heterogeneity.

H. Convergence of Blockchain and AI for Network Management

Another area of study explores how blockchain can be integrated with AI to enhance security, coordination, and trust in decentralized networking systems. This pairing has drawn interest in limited space, safety-critical environments like drone networks and B5G edge devices. While federated learning allows for model development among all participating nodes without the need to expose their raw data, blockchain can provide tamper-resistant coordination. Other applications of AI in networking include industrial and manufacturing applications, such as cyber-physical systems [28].

6. CHALLENGES

A. The reliability and availability of data.

For supervised learning, traffic data should be sufficiently large and be properly labeled. These labels are expensive to create, and there may be a lack of relevance of datasets due to changing traffic patterns and attack methods. Furthermore, it can be challenging to get operational data from private industrial networks. The restrictions encourage other research into unsupervised and semi-supervised learning techniques [5].

B. Interpretability and Operator Confidence

There are many deep learning models that make predictions and don't explain the reasoning behind every single prediction. This transparency is particularly important for operational networking because a wrong automated response, for instance rerouting traffic or closing a flow, may have safety and/or economic implications. Network operators need systems that enable the audit, explanation and, if needed, override of AI generated actions.

C. Computational and Real-Time Limitations

Some functions of a network need to be performed in less than a few milliseconds or microseconds. Inference of deep models or GNNs can then come with a computational price that could be incompatible with the time sensitivity or line-rate requirements for operations. Possible solutions are model compression, dedicated hardware acceleration and hybrid architectures where learned models are used to make decisions where it is not necessary for per-packet inference [9].

D. Robustness and Security of AI models

The integration of AI in network infrastructure adds another layer of security risks as the learning components can also be potential targets for attack. Adversarial inputs can lead to subpar intrusion detection performance by ML, and manipulated training data can lead to compromised federated-learning aggregation and ML model. It is therefore important to have strong learning algorithms and data-handling protocols for reliable deployment [13, 14].

E. The generalizations and transferability of the experience.

A model trained at one topology, traffic distribution or data set might not be as effective when it is used in another topology, traffic distribution or data set. The problem can be partially addressed by explicitly encoding topology and routing interaction, as in the GNN-based approaches, which can enhance predictions on large topologies or topologies that have never been seen before. However, the generalization to very different traffic regimes is still not solved [9].

F. System Integration and Data Standardization.

Lack of common data sets, interfaces, and protocols for assessments makes it hard to consistently compare different AI-based networking solutions. It also makes research prototypes hard to integrate into the current network-management tools. To enable the deployment of AI networking ideas and research from proof-of-concept demonstrations to actual operations, it is therefore crucial to create

standards and reproducible evaluation environments that are interoperable [2].

7. FUTURE RESEARCH DIRECTIONS

Literature research has identified challenges that can be used to prioritize research areas for AI-enabled networking.

Future systems should generate explanations of network-control decisions, either interpretable or post-hoc, to enable operators to review, validate, audit and, if needed, alter automated decisions.

2) Federated and privacy-preserving edge intelligence: FL can facilitate the collaborative learning process on the edge and IoT devices with the privacy of raw data. In addition, non-independent and non-identically distributed data (non-IID) among the participating nodes needs to be considered and poisoning threats [22] need to be dealt with in future work.

3) Digital twin networks: AI based digital copies of network infrastructure can be used to enable what if analyses, predictive planning, and proactive remediation. A constantly synchronised digital representation enables potential issues to be assessed and mitigated before measures are put in place to address traffic in production.

4) Autonomous and self-driving networks: GNN-based network models, RL controllers and the knowledge-driven feedback mechanisms could form an end-to-end network that would be increasingly able to handle routine network-management tasks autonomously [8] [10].

5) AI-native 6G architectures: Future architectures can be designed with AI as an integral part of the wireless system, instead of considering it as an additional application on top of the existing stack [7].

6) Adversarial training, anomaly-aware monitoring, and secure model aggregation: Research is required to make sure that the adversarial training and anomaly-aware monitoring and secure model aggregation pipelines for intrusion detection can be resilient against deliberate manipulation by AI [13] [14].

8. CONCLUSION

This systematic review focused on the use of AI and ML in computer networking, exploring the primary learning paradigms, the applications areas where the technologies have been used, the challenges encountered and new research avenues. Based on the literature reviewed, there is a high degree of relevance of deep learning, reinforcement learning, and graph-based learning to traffic engineering, routing, security, resource management, and wireless networking. However, the practical adoption is limited by the lack of data collection, lack of model interpretability, computational requirements for realtime, lack of generalisation, vulnerability to adversarial inputs and lack of common standards. For the network infrastructure to become more autonomous, advances in machine learning, distributed systems, network engineering, and security will be necessary. Specifically, digital-twin based validation, privacy-preserving distributed learning, and explainable decision making are important research directions.

9. REFERENCES

- [1] R. Boutaba, M. A. Salahuddin, N. Shahriar, F. Estrada-Solano, N. Limam, S. Ayoubi, and O. "A

- comprehensive survey on machine learning for networking: Evolution, applications and research opportunities," by M. Caicedo, *Journal of Internet Services and Applications*, vol. 9, no. 1, 2018, p. 16.
- [2] J. Xie, J. Liu, C. Wang, F. R. Yu, T. Huang, R. Xie, and Y. Liu, "A survey of machine learning techniques applied to software defined networking (SDN): Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, 2019, pp. 393–430.
- [3] Y. Bengio, Y., LeCun, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, 436–444, 2015.
- [4] R. Sutton, S. and A. Reinforcement Learning: An Introduction, G. Barto, 2nd ed. MIT Press, Cambridge, MA, USA, 2018.
- [5] M. Usama, J. Qadir, A. Raza, H. Arif, Y. Elkhatib, A. Hussain, K.-L. A. Yau, and A. Al-Fuqaha, "Unsupervised machine learning for networking: Techniques, applications and research challenges," *arXiv preprint, arXiv:1709.06599*, 2017.
- [6] H. B. McMahan, E. Moore, S. Hampson, D. Ramage, and B. An A. Arcas, "Communication-efficient learning of deep networks from decentralized data," *Proc. 20th International. Conf. 1273–1282 in Artificial Intelligence and Statistics (AISTATS)*, 2017.
- [7] K. W. Chen, Y. Shi, J. Zhang, B. Letaief, and Y.-J. "The roadmap to 6G: AI empowered wireless networks," A. Zhang, *IEEE Communications Magazine*, vol. 57, no. 8, 2019, pp. 84–90.
- [8] K. Rusek, P. Almasan, P. Barlet-Ros, J. Suárez-Varela, and A. "RouteNet: Leveraging graph neural networks for network modeling and optimization in SDN," *Cabellos-Aparicio, IEEE Journal on Selected Areas in Communications*, vol. 38, no. 10, 2260–2270, 2020.
- [9] M. Ferriol-Galmés, J. Paillisse, J. Suárez-Varela, K. Rusek, S. Xiao, X. Shi, X. Cheng, P. Barlet-Ros, and A. "RouteNet-Fermi: Network modeling with graph neural networks," *Cabellos-Aparicio, IEEE/ACM Transactions on Networking*, vol. 31, no. 6, 2023, pp. 3080–3095.
- [10] Mestres, A. Rodriguez-Natal, J. Carner, P. Barlet-Ros, E. Alarcón, M. Solé, V. Muntés-Mulero, D. Meyer, S. Barkai, M. J. Hibbett, G. Estrada, K. Ma'ruf, F. Coras, V. Ermagan, H. Latapie, C. Cassar, J. Evans, F. Maino, J. Walrand, and A. Cabellos-Aparicio, "Knowledge-defined networking," *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 3, 2017, pp. 2–10.
- [11] F. Pacheco, J., M. Gineste, C. Baudoin, and E. Exposito. Aguilar, "Towards the deployment of machine learning solutions in network traffic classification: A systematic survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, 2019, pp. 1988–2014.
- [12] Y. Sun, M. Peng, Y. Huang, Y. Zhou, and S. Mao, "Application of machine learning in wireless networks: Key techniques and open issues," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, 2019, pp. 3072–3108.
- [13] Buczak, L., and E. "A survey of data mining and machine learning methods for cyber security

- intrusion detection," Guven, IEEE Communications Surveys & Tutorials, vol. 18, no. 2, 2016, pp. 1153–1176.
- [14] R. Vinayakumar, A. Al-Nemrat, P. Poornachandran, K. P. Soman, M. Alazab, and S. "Deep learning approach for intelligent intrusion detection system," Venkatraman, IEEE Access, vol. 7, 2019, pp. 41525–41550.
- [15] N. Sultana, W. Peng, N. Chilamkurti, and R. Alhadad, "Survey on SDN based network intrusion detection system using machine learning approaches," Peer-to-Peer Networking and Applications, vol. 12, no. 2, 2019, pp. 493–501.
- [16] I. Ahmad, M. Ylianttila, S. Namal, and A. Gurtov, "Security in software defined networks: A survey," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, 2015, pp. 2317–2346.
- [17] F. Tang, N. Kato, Y. Kawamoto, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," IEEE Proceedings, vol. 108, no. 2, 2020, pp. 292–307.
- [18] Y. Y. B. Zikria, A. V. Vasilakos, A. Qadri, A. Nauman, and S. W. Kim, "The future of healthcare internet of things: A survey of emerging technologies," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, 2020, pp. 1121–1167.
- [19] M. Li, J. Gao, X. S. Shen, C. Zhou, and W. Zhuang, "Slicing-based artificial intelligence service provisioning on the network edge: Balancing AI service performance and resource consumption of data management," IEEE Vehicular Technology Magazine, vol. 16, no. 4, 2021, pp. 16–26.
- [20] X. Wang, Y. Han, X. Yan, D. Niyato, V. C. M. Leung, and X. Chen, "Convergence of edge computing and deep learning: A thorough survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, 869–904, 2020.
- [21] Y. "Blockchain and machine learning for communications and networking systems," Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, IEEE Communications Surveys & Tutorials, vol. 22, no. 2, 2020, pp. 1392–1431.
- [22] S. A. Hawbani, A. V. Shvetsov, B. Lee, H. Alsamhi, F. A. Almalki, F. Afghah, and H. Song, "Drones' edge intelligence over smart environments in B5G: Blockchain and federated learning synergy," IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, 2022, pp. 295–312.
- [23] M. H.-P. Tan, Z., S. Lin, D. Niyato, and A. Alsheikh. Han, "Mobile big data analytics using deep learning and Apache Spark," IEEE Network, vol. 30, no. 3, 2016, pp. 22–29.
- [24] K. Ota, V. Mezaris, M. S. Dao, and F. "Deep learning for mobile multimedia: A survey," G. De Natale, ACM Transactions on Multimedia Computing, Communications, and Applications, vol. 13, no. 3s, 2017, p. 34.
- [25] Q. Hu, F. Mao, and Q. Hao, "Deep learning for intelligent wireless networks: A



- comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, 2595–2621, 2018.
- [26] K.-L. P. Komisarczuk, A. Yau, and P. D. Teal, "Reinforcement learning for context awareness and intelligence in wireless networks: Review, new features and open issues," Journal of Network and Computer Applications, vol. 35, no. 1, 2012, pp. 253–267.
- [27] T. G. F. Riley, R. Henderson, M. Lacage, C. Dowell, and J. Kopena, "Network simulations with the ns-3 simulator," Proc. 2008 ACM SIGCOMM Demo.
- [28] C. D. and Martínez-García. Li, "Artificial-intelligence-driven customized manufacturing factory: Key technologies, applications, and challenges," IEEE Proceedings vol. 109, no. 4, 377-398, 2021.