Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Survey on Machine Learning in Network Exploring

Marwa Qatawneh

Master degree, Computer science ,artificial intelligence, Mutah University, Jordan-alkarak, Marwaqatawneh95@gmail.com

Modern communication systems and networks produce an extensive and diverse volume of traffic data. Conventional methods of network management encounter various challenges and problems, such as ensuring accuracy and efficiently processing large volumes of real-time data for monitoring and data analytics. Additionally, the network traffic pattern exhibits highly intricate behavior due to a multitude of factors, including network heterogeneity. Machine learning has proven to be highly effective in the application of Techniques for Network Optimization, Traffic Prediction, Anomaly Detection, and Intelligent Network Management for pattern recognition. Researchers in the networking field utilize machine learning techniques for tasks such as Network Traffic Monitoring, Network Optimization, Traffic Prediction, Anomaly Detection, and Intelligent Network Management. This comprehensive review paper provides an extensive analysis of the current research landscape in Machine Learning in Network. It encompasses recent advancements, significant challenges, and areas of ongoing research. Additionally, it conducts a meticulous evaluation of existing literature, including research papers. The paper also emphasizes the crucial gap in research papers that impedes the advancement of Machine Learning in Network development. Furthermore, it underscores the significance of addressing open research areas to fully harness the potential of this technology. Individuals such as researchers, engineers, policymakers, and those interested in the future of Machine Learning in Network will find this paper to be an invaluable resource.

Keywords: Machine Learning (ML), Artificial intelligence (AI), Deep learning (DL) Intelligent Network Management, Network Traffic Prediction, Network Anomaly Detection.

1. Introduction

The expanding network plays a crucial role in enhancing the efficiency and convenience of

our life, while also increasing the need for superior service quality. Despite the increasing complexity of network use cases and the growing data processing requirements of network devices, users anticipate faster response times. The heightened focus of internet serves providers on accurate user traffic profiling in order to provide customized services, along with the surge in the quantity of connected users and internet of things devices, are key factors driving this demand.

In order to establish an effective network infrastructure for the transfer and management of large amounts of data, a variety of techniques have been implemented. These techniques are primarily aimed at preventing network faults and inefficiencies, ensuring Quality of Service (QoS), and enhancing security measures. The quality of service is not only influenced by the type of network infrastructure, but also by the efficiency of data routing and the capability of routing devices to assess real-time network conditions for making dynamic adjustments and allocation decisions. Network Traffic Monitoring and Analyzing (NTMA) techniques have been introduced to monitor network performance, provide valuable insights for network analysis, and propose solutions to overcome challenges without requiring human intervention [1].

Networks like the Internet and mobile telecommunications networks play a crucial role as the central hub of contemporary human societies, around which the different aspects of modern life revolve. As networks continue to evolve, becoming more dynamic, diverse, and intricate, the task of managing these networks has become more challenging. The success of Artificial intelligence (AI) and ML techniques in various fields, including computer vision, can be largely attributed to two factors: The remarkable progress in unsupervised ML techniques, particularly deep learning and the abundance of unstructured raw data that can be easily processed by unsupervised learning algorithms.

The research question is what are the most effectives AI technique used in network exploring. This study aims to propose a new structure to describe the general concept of machine learning techniques for network optimization. This document outlines a study on traffic network prediction. This document outlines a study on anomaly detection and intelligent network management and explores insights from various research fields. These survey contributions are to propose a new review about machine learning techniques for network optimization in details.

The rest of the paper is organized as follows section one is introduction, section two is related work, section three is survey on ML, section four is dissection, section five and finally is conclusion.

2. Related work

The expansion of communication technology has led to the diversification of access environments and the creation of distributed networks. As a result, a wide range of data, originating from different domains like sensors, computers, and the Internet of Things (IoT), is now being communicated through network systems. The capacity of these systems has also been enhanced to ensure the reliable processing of such data. The ML has experienced a remarkable increase in its applications, contributing to problem solving and automation in

various fields.

This survey [2] explains a comprehensive examination of the various applications of machine learning and artificial intelligence in future mobile communication systems. It presents an overview of different types of machine learning and artificial intelligence to provide a deeper understanding of intelligent methodologies. Furthermore, the paper engages in discussions based on the reviewed papers, focusing on artificial intelligence and machine learning concepts. Also, the paper provides a classification of the pertinent research. Additionally, the paper discusses various obstacles faced by machine learning applications in mobile communications-enabled systems and offers insights into potential research avenues.

This paper in [3] Arzoo Miglani et al, provide a comprehensive review of the current state-of-the-art in the collaboration between machine learning (ML) and blockchain. They present an overview of blockchain technology and discuss how this decentralized approach can address privacy concerns in ML. Additionally; they provide insights into ML technology and examine its key applications, as well as the applicability of blockchain features in ML. The literature review reveals that collaborative applications between blockchain and ML are still in their early stages, and there are numerous research challenges that need to be addressed.

In this review article Moussa Aboubakar et al in [4], they have explored the cutting-edge strategies for managing IoT low power networks. They have outlined key criteria for effectively managing IoT low power networks and categorized current solutions into five groups: network management protocols, SDN-based frameworks, Cloud-based frameworks, Semantic-based frameworks, and machine learning based frameworks. Additionally, they have conducted a thorough comparative evaluation of existing solutions for managing IoT low power networks based on various criteria. The deficiencies in current solutions for managing IoT low power networks underscore the need for further research to develop efficient solutions that can support scalability, optimize resource utilization, address the diversity of IoT networks, and ensure security and privacy.

Raouf Boutaba et al In [5] this study, they have gathered the academic articles published in Springer, Elsevier, IEEE, and ACM, focusing on the topics of SDN and ML from 2016 to 2023. These research papers have been categorized based on the proposed solutions, evaluation criteria, and testing environments, aiming to assist individuals involved in SDN and ML in enhancing both functional and non-functional parameters. The analysis of these research papers will enable us to extract the solutions, evaluation criteria, and environments, which will then be organized into clusters within this review paper. Furthermore, this work will also highlight the research gaps and provide insights into future research directions. This comprehensive survey proves to be invaluable for individuals engaged in SDN, as it offers valuable insights on leveraging machine learning techniques to enhance both functional and non-functional parameters.

Sahar Faezi1et al in [6] there is multiple surveys available on machine learning for specific networking areas or technologies. This particular survey stands out for its originality, as it covers a wide range of machine learning techniques applied in various important networking areas across different technologies. Readers will gain valuable insights from a thorough discussion on different learning paradigms and machine learning techniques

used to address fundamental networking issues such as traffic prediction, routing and classification, congestion control, resource and fault management, QoS and QoE management, and network security. Additionally, this survey highlights the limitations, provides insights, identifies research challenges, and outlines future opportunities for advancing machine learning in networking. As a result, this survey makes a timely contribution to understanding the impact of machine learning on networking, pushing the boundaries of autonomic network operation and management.

Table 1 years and gap are compared in various use cases.

Ref	Year	Gap
İbrahim Yazici et al [2]	2022	data privacy and security
Moussa Aboubakar et al [4]	2023	Need to investigate on hybrid solutions (solutions that encompass at least two types of approaches for IoT low power networks management mentioned in this paper).
Raouf Boutaba et al [5]	2018	Needed that can evaluate the performance of the proposed ML techniques in real networks and with real data.
Sahar Faezi1et al [6]	2023	Existing ML approaches should be extended or re architected to take into account the notion of multi tenancy in multi layer networks.

1. Survey on Machine learining in Network

In [7], the study involved utilizing deep reinforcement learning (DRL) to determine the optimal offloading ratio, while the allocation of transmission power and computational capability was managed by a centralized optimizer (CO). Furthermore, a deep Q-network (DQN) was employed to make offloading strategy decisions, followed by the use of convex optimization for the allocation of transmission power and computational capability based on the offloading ratio determined by the DQN. In [8], the objective of the study was to enhance data transmission rate to guarantee physical-layer security. DDPG was implemented to improve system performance by learning and executing resource allocation and task offloading decisions for MEC network to minimize latency and energy consumption costs. In [9] this article introduces an AI-based Trust-aware and Privacy-preserving System (ATPS) designed to safeguard the privacy of vehicular data providers and enhance the quality of data collections in VANETs.

Furthermore, this research paper provides a comprehensive analysis of the current state of IoT security, with a specific focus on machine learning and deep learning approaches. It not only categorizes recent studies on security issues but also emphasizes the opportunities, advantages, and limitations of ML/DL solutions in this domain [10]. Conversely, in another publication [11], they propose an energy-efficient scheme that prioritizes secrecy in a two-tier heterogeneous network (HetNet), comprising a sub-6 GHz macrocell and multiple millimeter wave (mmWave) picocells.

On a different note, thier paper introduces a novel met averse network intrusion detection model that leverages the underlying technology of met averse, the Internet of Things. By combining deep auto encoder and random forest algorithms with GAN, they construct a hybrid abnormal traffic detection model [12]. Additionally, in [13], their study aims to develop a security framework for addressing the vulnerabilities in smart cities' sustainability edge computing. This framework utilizes Petri Net and Genetic Algorithm-Based Reinforcement Learning (GARL) to enhance the overall security of these cities.

Table 2 methods, ml task, and results are compared in various use cases.

Ref	Year	Methods	ML Task	Results
L. Chen, S . Tang et al [7]	2022	DQN	RL	Simulations show that the DRCO method can outperform other approaches that are commonly used, and can decrease the latency of the MEC system by 32.5% even under up to 15 colluding eavesdroppers
L. Zhang et al [8]	2022	DDPG	RL	The computing powers at CAP and each user are W and 0.2 W, respectively.
T.Li,s.et al[9]	2022	GAN	Classification	extensive experiments conducted on the real-world datasets demonstrates efficiency of they ATPS in terms of improving the data quality by 45.76% to 52.57%, reducing the malicious vehicle participants by 15.48% to 16.95%, preserving privacy of vehicles, and guaranteeing data availability.
R.Fu,x. et al[10]	2022	DDQN, CNN + LSTM	RL+ Classification	The experimental findings verified the effectiveness of the suggested method over the status quo of deep learning models for attack detection.
H.Sharma[11]	2023	Dueling double DQN	RL	Simulation results demonstrated that the proposed SecBoost scheme achieves 14.7%, 8.33%, 30%, and 69% better average SEE in comparison to MARL, MA-DQN, JBF-SEEM, and O-EDT schemes, respectively, which reveals its effectiveness in improving SEE of picocells.
S.Ding et al[12]	2023	GAN + DAE + RF	Classification	As per obtained results in the paper, the proposed method outperformed the compared methods.
L.A.Ajao et al[13]	2023	Q-learning	RL	The proposed approach outperformed the compared approaches in terms of F1-measure, precision, and sensitivity.

A. Artificial intelligence(AI) and Machine Learning (ML)

Artificial intelligence, commonly referred to as AI, denotes the technology enabling computers and machines to replicate human intelligence and problem-solving abilities. Artificial intelligence is closely linked with machine learning and deep learning. These fields involve the creation of AI algorithms that mimic the decision-making processes of the human brain, enabling them to 'learn' from data and improve their accuracy in classifications or predictions over time. Machine learning and deep learning are branches of artificial intelligence. Both machine learning and deep learning utilize neural networks to analyze extensive datasets. These neural networks are designed to mimic the decision making processes of the human brain. The key difference between machine learning and deep learning lies in the neural network structures used and the level of human involvement. The following figure shows the relationship between artificial intelligence in machine learning;

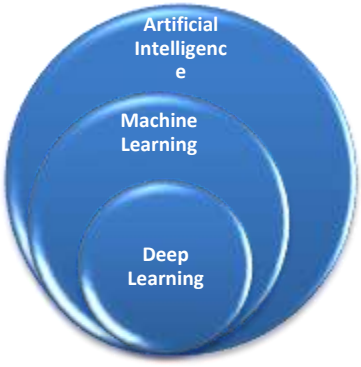

Figure 1.1 relationships between AI, ML and DL

In this paper [14], they have concentrated on various strategies for implementing AI and ML tools in 6G networking and optimizing resource management. They have demonstrated the use of intelligent terahertz techniques, such as AI-/ML-enabled terahertz channel estimation and spectrum management, which are considered groundbreaking in achieving ultra-broadband transmission. Additionally, they have introduced AI/ML applications in energy management, particularly for large-scale energy-harvesting networks. Furthermore, they have discussed AI-/ML-based security enhancement mechanisms, including authentication, access control, and attack detection, for advanced IoT systems. Moreover, they have presented efficient mobility and handover management strategies based on DRL, DL, and Q-learning to establish ultra-reliable and stable transmission links and address the high dynamics in 6G. Lastly, they have identified intelligent resource allocation technologies, such as traffic, storage, and computing offloading mechanisms, to meet the demands of ultra-reliability and low latency in 6G services.

Machine learning is endeavoring to establish its worth in various domains, one of which is anomaly detection, a practical application that garners significant interest. ML, as a statistical-based analytical tool, has garnered significant attention and implementation across diverse domains. Its ability to analyze and interpret vast amounts of data enables it to alleviate the burden of data processing, making it a valuable asset in exploring intricate scenarios [15]. [16] In this research, various OL strategies are examined and contrasted to offer data stream analytics for the networking sector. Throughout their investigation into the advantages of traffic data analytics, they concentrated on not just the advantages of online learning in this domain but also its drawbacks, including concept drift and imbalanced classes. Additionally, they explored the compatibility of these frameworks and tools with existing data processing frameworks. To evaluate the effectiveness of OL methods, an empirical investigation on ensemble- and tree-based network traffic categorization algorithms was carried out.

In other side, this study [17], a novel machine learning ensemble technique is proposed for the categorization of Intrusion Detection (ID). Making corrections to the training dataset can greatly aid in class identification, particularly for uncommon attacks like R2L (Root to Local attacks) and U2R (User to Root attacks). When compared to existing methodologies, the proposed approach offers several advantages. Firstly, it introduces two methods for classifying intrusions on the most widely used datasets using machine learning models. Secondly, the KDD Cup99 and NSL-KDD datasets are rebalanced through data augmentation. Additionally, a three-step approach is provided for enhancing intrusion detection by utilizing a Multi Layer Perceptron (MLP) in a cascaded structure. Specialized cascaded meta-specialized classifier architecture has been developed to accurately classify each class. Moreover, all meta-specialists evaluate the dataset's non-flagged connections. This approach has demonstrated a significant increase in detection quality, achieving a classification accuracy of 89.32% and a false positive rate (FPR) of 1.95%.On the NSL-KDD dataset, this approach achieves a high accuracy of 87.63% and a low FPR of 1.68%.

In this document [18], the authors introduce Machine Learning-Network Selector (ML-NetSel), a fully automated ML-driven method for choosing the optimal base station within an LTE setting. The proposed technique focuses on offloading video traffic at the base station level during periods of high traffic to fulfill the Quality of Service (QoS) demands of

diverse applications. By combining QoS requirements for users' applications and user behavior, a hybrid approach is employed to train the ML model for selecting the most suitable base stations for these applications. Results from simulations demonstrate that ML-NetSel achieves superior prediction accuracy, as measured by the Mean Absolute Percentage Error (MAPE), and increased throughput when compared to an existing solution. Furthermore, it leads to reduced delay and packet loss ratio. The concept of blockchain was initially introduced by Satoshi Nakamoto in 2008 [19].

This research paper [20], delves into the potential of machine learning in enhancing the detection of cyber threats by analyzing behavioral patterns in network traffic. The authors provide an overview of various machine learning techniques, explaining how they can effectively model complex patterns in network traffic data that cannot be discerned by traditional rules. The methodology employed encompasses supervised, unsupervised, and hybrid machine learning algorithms, such as neural networks, support vector machines, random forests, self-organizing maps, k-means clustering, and isolation forests. Performance evaluation is based on metrics like detection rate, false positive rate, accuracy, precision, recall, and f1-score. The results clearly demonstrate that machine learning significantly enhances detection rates compared to conventional techniques, while still maintaining a manageable number of false positives. This research [21], examines the recent utilization of ML algorithms in networking, encompassing various applications such as congestion control, predictive network modeling, intrusion detection systems, route and path allocation, QoS enhancement, and resource management. However, these approaches do have certain limitations. They require manual configurations with a fixed matrix, possess limited computing capacity, exhibit long execution times with high overhead load, and respond slowly to network changes. This research presents a summary of simulation and experimental results that demonstrate the superiority of ML-based algorithms compared to conventional approaches.

There is an urgent need for data analytic methods that can process network data in real-time as new data arrives. Online machine learning (OL) techniques offer a promising solution for such data analytics. In the study conducted by the team [22], they delve into and contrast various online learning techniques that enhance the analysis of data streams within the networking domain, they present the open issues and future directions in the analysis of traffic data streams. This technical study provides valuable insights and a forward-looking perspective for the network research community when addressing the requirements and objectives of online data stream analytics and learning in the networking domain [22].

In this section, they describe applications of machine learning in intrusion detection within different network domains. In [23] the approach suggested combines reinforcement learning with the traffic reduction method. A significant aspect of this approach is the network traffic reduction strategy, which allows for a reduction of input packets by approximately 50%. they proposed method achieves a detection rate of 98.30% and a low FPR of 0.010% with a time-window size of 60 seconds. information security and object technology (ISOT) dataset, The second dataset comprises of four authorized P2P applications, namely Vuze, uTorrent, Frostwire, and eMule, along with the traffic generated by three P2P Botnets, namely Zeus, Storm, and Waledac. The dataset is offered by the Information Security Centre of Excellence (ISCX). Furthermore, they proposed bot detection

approach has demonstrated a commendable accuracy rate and the ability to detect new bots. However, there are still several challenges that must be tackled. For instance, cybercriminals will persist in finding new methods to evade detection, such as utilizing rootkits. Furthermore, botnets evolve constantly through updates, leading to potential changes in their operations across different life cycle phases.

The deep learning, a subset of ML, aims to replicate the functions of the human brain. It is considered the next paradigm in enhancing user experience and has garnered significant attention from networking researchers due to its capability to manage the challenges posed by the rapid growth of traffic and complexity. The utilization of DL in reducing communication overhead has also been explored by researchers. DL imitates the biological nervous system and conducts computations through multi-layer transformations, as illustrated in Fig. 1 One of the key advantages of DL compared to traditional ML is its ability to automatically extract features, eliminating the need for costly hand-crafted feature engineering. In contrast, traditional supervised ML is effective only when there is a sufficient amount of labeled data available. However, many current systems generate unlabeled or semi-labeled data. DL offers a solution by extracting valuable patterns from unlabeled data [24][25][26][27].

Table 3 published in, years and methodology are compared in various use cases.

References	Published in	Year	Methodology
D. Haripriya et al [16]	international journal of intelligent systems and applications in engineering	2024	OL paradigm
İbrahim Yazici et al [2]	Engineering Science and Technology, an International Journal	2023	Machine learning and artificial intelligence applications for different use cases enabled by future mobile communication systems.
Arindam Sarkar et al [17]	Springer nature	2023	classifying intrusions on the two most widely used datasets using ML models
Devanshu Anand et al [18]	IEEE	2021	ML-based approach for selecting the best base station in a LTE environment.
Fatima Boucham et al [20]	International Journal of Business Intelligence and Big Data Analytics	2024	methodology utilizes supervised, unsupervised, and hybrid machine learning algorithms, including neural networks, support vector machines, random forests, self-organizing maps, k-means clustering, and isolation forests.
M. A. Ridwan et al [21]	IEEE	2024	the recent trends in the application of ML models in communication networks for prediction, intrusion detection, route and path assignment, Quality of Service improvement, and resource management.
Amin Shahraki et al [22]	Engineering Science and Technology, an International Journal	2022	compare the OL techniques that facilitate data stream analytics in the networking domain

B. Internet of Things (IoT)

The advancements in machine learning (ML) and deep learning (DL) techniques have made them reliable tools for tackling security concerns in internet of things (IoT) devices. In this study [28], a thorough examination of IoT security research is conducted with a specific emphasis on ML/DL strategies. The paper further organizes recent investigations on security problems according to ML/DL methodologies, shedding light on their benefits, drawbacks,

and potential. These findings offer valuable guidance for addressing upcoming research obstacles. Combining GNN with other data set classifiers can significantly enhance operational accuracy. Additionally, the AdaBoost mechanism greatly improves overall accuracy in voting and classifiers. SGDM and ADAM are utilized for training classification weights, enabling quick determination of classifier size and weight, yielding desired results. These algorithms rely on gradient descent and chaotic behavior.

Additionally, in [29] a pioneering method for detecting intrusions in electric vehicle charging stations (EVCS) based on the Internet of Things (IoT) has been introduced. This approach integrates Convolutional neural network (CNN), long short-term memory (LSTM), and gated recurrent unit (GRU) models, offering a groundbreaking solution. To tackle the complex challenges faced by IoT-based EVCS, a comprehensive real-world cyber security dataset specifically designed for IoT and IIoT applications was utilized. The researchers conducted extensive testing in both binary and multiclass scenarios, yielding remarkable results. These accomplishments highlight the effectiveness of the CNN-LSTM-GRU ensemble architecture in developing a resilient and adaptable intrusion detection system (IDS) for IoT infrastructures. The ensemble algorithm, which can be accessed on GitHub, represents a significant advancement in safeguarding IoT-based EVCS against a wide range of cyber security threats. On other side, in [30] they presented a method for detecting intrusions on the Internet of Things (IoT) and created a hybrid deep learning model to tackle the various security threats that IoT devices may face. XGBoost feature selection was implemented to minimize redundancy in the IoT dataset. Through the integration of CNN and GRU, they successfully achieved thorough and efficient feature learning. Additionally, a comprehensive performance evaluation was carried out by comparing their model with cutting-edge classification models.

Furthermore, in [31] the authors of this study introduce a method for identifying attacks on IoT networks by combining two Convolutional neural networks (CNN-CNN). The initial CNN model is employed to pinpoint the key features that aid in detecting IoT attacks from the raw network traffic data. The second CNN then uses these features to construct a reliable detection model that can accurately identify IoT attacks. Additionally, comparisons with other deep learning algorithms and feature selection techniques demonstrate that this proposed approach surpasses the performance of these alternative methods. However, in [32] a novel approach to network intrusion detection in the realm of the Internet of Things is presented, utilizing a deep learning algorithm. Initially, an intrusion detection model specific to the Internet of Things is constructed by incorporating edge computing. This model incorporates the concept of gated convolution to enhance the convolution neural network model. The effectiveness of the proposed algorithm is demonstrated through experimental evaluation using the KDD99 data set. This approach effectively caters to the requirements of intrusion detection in the context of the Internet of Things. Table 1 shows Comparison of ML methods, ML task, dataset and accurate in use cases.

Table 4 ML methods, ML tasks, datasets, and accuracy are compared in various use cases.

References	Methods	Year	ML task	Dataset	Results
Ali Ghaffari et al [28]	SGDM and ADAM	2024	IoT security research focusing on ML/DL approaches	-----	SGDM and ADAM are both effective methods for training the weight of classifications. By utilizing these two techniques, it is possible to swiftly determine the size and weight of the classifiers,

					resulting in accurate and reliable outcomes.
Dusmurod Kilichev et al [29]	CNN, LSTM, GRU	2024	intrusion detection for IoT-based electric vehicle charging (stations (EVCS	dataset specifically designed for IoT	The results are remarkable, demonstrating a perfect 100% accuracy in binary classification, an impressive 97.44% accuracy in six-class classification, and 96.90% accuracy in fifteen-class .classification
Zhaolian Wang et al [30]	CNN, GRU	2023	detecting intrusions in the Internet of Things ((IoT	N-BaIoT	the proposed CNN-GRU model outperforms other models in terms of accuracy, F1-score, precision, and recall, achieving 99.78%, 99.59%, 99.52%, and 99.68% ..respectively
Basim Ahmad Alabsi et al [31]	CNN-CNN	2023	detecting attacks on IoT	the BoT IoT 2020 dataset	The results reveal that the proposed approach achieves 98.04% detection accuracy, 98.09% precision, 99.85% recall, 98.96% recall, and a 1.93% (false positive rate (FPR
Yulin Wang et al [32]	DL	2023	IoT intrusion detection algorithm based on deep learning in edge computing environment	KDD99	The results show that the accuracy, precision, recall, and F1 values are 92.14%, 95.97%, 90.89%, and 90.03%, which are better than other comparison .algorithms

3. Discussion and Recommendation

The objective of this study is to present a novel framework for explaining the overall idea of machine learning methods in network optimization. This paper provides an overview of a research conducted on predicting traffic patterns in networks. Additionally, it delves into the realms of anomaly detection and intelligent network management, drawing insights from diverse research domains. The primary aim of these survey findings is to offer a comprehensive analysis of machine learning techniques for network optimization. These recommendations stem from the observations we made by analyzing the data presented in the tables of this survey.

The tables provided above offer a comprehensive comparison of the key features and technologies in machine learning for networks. It is clear that each study has made significant advancements in methods, ML tasks, and results. Table number 1 highlights the research gap in areas such as data privacy and security, as discussed in the paper by İbrahim Yazici et al. This paper also provides an overview of different types of machine learning and artificial intelligence to enhance our understanding of intelligent methodologies. Furthermore, it addresses the challenges faced by machine learning applications in mobile communications systems and suggests potential research directions. On other hand Moussa Aboubakar et al, They focused on cutting-edge strategies for managing low power networks in the Internet of Things (IoT). They have identified key criteria for effective management and categorized current solutions into five groups. However, there is still a need to investigate hybrid solutions that combine multiple approaches for managing low power networks in the IoT, as mentioned in this paper.

Raouf Boutaba and colleagues conducted a comprehensive study where they compiled academic articles from Springer, Elsevier, IEEE, and ACM focusing on SDN and ML topics from 2016 to 2023. The research papers were categorized based on proposed solutions, evaluation criteria, and testing environments to aid individuals in improving functional and non-functional parameters in SDN and ML. However, there is a need for an evaluation of the performance of proposed ML techniques in real networks and with real data. Furthermore,

Sahar Faezi and team's survey highlights limitations, provides insights, identifies research challenges, and outlines future opportunities for advancing machine learning in networking. This survey contributes to understanding the impact of machine learning on networking, pushing the boundaries of autonomic network operation and management. Despite the usefulness of all this work, there is a gap in existing ML approaches that should be addressed by considering the notion of multi-tenancy in multi-layer networks.

In Table No. 2, we present the findings of 5 studies that utilized RL as an ML task using different methods, resulting in varying outcomes. L. Chen et al employed the DQN method and demonstrated through simulations that the DRCO method surpasses commonly used approaches, reducing the latency of the MEC system by 32.5% even in the presence of up to 15 colluding eavesdroppers. Conversely, L. Zhang et al employed the DDPG method and reported that the computing powers at CAP and each user were 0.1 W and 0.2 W, respectively. H. Sharma's work utilized the Dueling double DQN method, and the simulation results showcased that the proposed SecBoost scheme achieved superior average SEE compared to MARL, MA-DQN, JBF-SEEM, and O-EDT schemes, with improvements of 14.7%, 8.33%, 30%, and 69%, respectively, thereby highlighting its effectiveness in enhancing SEE of picocells.

On the other hand, L.A. Ajao et al employed Q-learning as a method and found that the proposed approach outperformed the compared approaches in terms of F1-measure, precision, and sensitivity. Additionally, three studies focused on classification as an ML task using different methods, yielding diverse results. T. Li et al utilized the GAN method and reported that extensive experiments conducted on real-world datasets demonstrated the efficiency of their ATPS in terms of improving data quality by 45.76% to 52.57%, reducing malicious vehicle participants by 15.48% to 16.95%, preserving privacy of vehicles, and ensuring data availability. On the other hand, S. Ding et al employed GAN, DAE, and RF methods, and based on the obtained results, the proposed method outperformed the compared methods.

Furthermore, this study combined RL and classification as an ML task, utilizing the DDQN, CNN, and LSTM methods. The experimental findings validated the effectiveness of the suggested method in comparison to existing deep learning models for attack detection.

Table No. 3 provided an in-depth analysis of the methodologies utilized in the years 2021, 2022, 2023, and 2024. It also shed light on the journals where these methodologies were published. These studies can be valuable resources for researchers delving into machine learning in networks, offering convenient access to aid in various research endeavors.

Table number 4, on the other hand, delves into ML methods, ML tasks, datasets, and the comparison of accuracy across different use cases. Within this table, it was discovered that three studies employed the CNN method and yielded varying results. Dusmurod Kilichev et al. utilized the CNN, LSTM, and GRU methods for intrusion detection in IoT-based electric vehicle charging stations (EVCS) as an ML task. Their findings were remarkable, showcasing a perfect 100% accuracy in binary classification, an impressive 97.44% accuracy in six-class classification, and a 96.90% accuracy in fifteen-class classification. These results were obtained using a dataset specifically designed for IoT.

Furthermore, Zhaolian Wang et al. employed the CNN and GRU methods for detecting intrusions in the Internet of Things (IoT) as an ML task. Their proposed CNN-GRU model outperformed other models in terms of accuracy, F1-score, precision, and recall, achieving 99.78%, 99.59%, 99.52%, and 99.68% respectively. They utilized the N-BaIoT dataset for their analysis. Lastly, Basim Ahmad Alabsi et al. focused on detecting attacks on IoT as an ML task. Their approach yielded impressive results, with a detection accuracy of 98.04%, precision of 98.09%, recall of 99.85%, and a false positive rate (FPR) of 1.93%. These findings were obtained using the BoT IoT 2020 dataset.

Ali Ghaffari and colleagues employed SGDM and ADAM methods in their IoT security research, focusing on ML/DL approaches for machine learning tasks. The study found that both SGDM and ADAM were effective in training classification weights. By utilizing these techniques, researchers were able to quickly determine the size and weight of classifiers, leading to accurate and reliable results. In contrast, Yulin Wang and team utilized a DL method and IoT intrusion detection algorithm based on deep learning in an edge computing environment for a machine learning task using the KDD99 dataset. The results indicated that the accuracy, precision, recall, and F1 values were 92.14%, 95.97%, 90.89%, and 90.03%, respectively, outperforming other comparison algorithms.

4. Conclusion

Modern communication systems and networks generate a vast and varied amount of traffic data. Conventional network management methods face numerous challenges and issues when dealing with such networks, including the need to accurately and efficiently process large volumes of real-time data for monitoring and data analytics. Moreover, the network traffic pattern displays complex behavior due to various factors, such as network heterogeneity. This comprehensive review paper provides an extensive analysis of the current research landscape in Machine Learning in Network. It encompasses recent advancements, significant challenges, and areas of ongoing research. Additionally, it conducts a meticulous evaluation of existing literature, including research papers, patents, and technical reports. The paper also emphasizes the crucial gap in research papers that impedes the advancement of Machine Learning in Network development. Furthermore, it underscores the significance of addressing open research areas to fully harness the potential of this technology. Individuals such as researchers, engineers, policymakers, and those interested in the future of Machine Learning in Network will find this paper to be an invaluable resource.

References

[1] Iraj Lohrasbinasab et al, “rom statistical- to machine learning-based network traffic prediction”, 2021.

[2] İbrahim Yazici et al , “A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems”, 2023.

[3] Arzoo Miglani et al , “Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review”, 2021.

[4] Moussa Aboubakar et al, “A review of IoT network management: Current status and

perspectives", 2022.
[5] Raouf Boutaba et al , A comprehensive survey on machine learning for networking: evolution,applications and research opportunities,2018.
[6] Sahar Faezi1et al, A comprehensive survey on machine learning for networking: evolution, applications and research opportunities, 2023
[7] L. Chen, S. Tang, V. Balasubramanian, J. Xia, F. Zhou, L. Fan Physical-layer security based mobile edge computing for emerging cyber physical systems
[8] L. Zhang, S. Lai, J. Xia, C. Gao, D. Fan, J. Ou Deep reinforcement learning based IRS-assisted mobile edge computing under physical-layer security Phys. Commun., 55 (2022).
[9] T. Li, S. Xie, Z. Zeng, M. Dong, A. Liu ATPS: An AI based trust-aware and privacy-preserving system for vehicle managements in sustainable VANETs IEEE Trans. Intell. Transp. Syst., 23 (10) (2022).
[10] R. Fu, X. Ren, Y. Li, Y. Wu, H. Sun, M.A. Al-Absi Machine Learning-Based UAV Assisted Agricultural Information Security Architecture and Intrusion Detection IEEE Internet Things J. (2023) .
[11] H. Sharma, N. Kumar, R.K. Tekchandani SecBoost: Secrecy-Aware Deep Reinforcement Learning Based Energy-Efficient Scheme for 5G HetNets IEEE Trans. Mob. Comput. (2023).
[12] S. Ding, L. Kou, T. Wu A GAN-based intrusion detection model for 5G enabled future metaverse Mob. Networks Appl., 27 (6) (2022).
[13] L.A. Ajao, S.T. Apeh Secure edge computing vulnerabilities in smart cities sustainability using petri net and genetic algorithm-based reinforcement learning Intell. Syst. with Appl. (2023).
[14] SONG WANG et al, "Machine Learning in Network Anomaly Detection: A Survey", 2021.
[15] jun du et al, " machine learining for 6G wirless networks carrying forword enhanced bandwidth, massive acsess, and utareilble/ low latency services",2022.
[16] D. Haripriya et al, "A Comparative Study on Online Machine Learning Techniques for Network Traffic Streams Analysis", 2024.
[17] Arindam Sarkar et al, "A supervised machine learning-based solution for efficient network intrusion detection using ensemble learning based on hyper parameter optimization", 2022.
[18] Devanshu Anand et al, "A Machine Learning Solution for Automatic Network Selection to Enhance Quality of Service for Video Delivery", 2021.
[19] Raynor de Best et al, "Blockchain - statistics & facts", 2024.
[20] Fatima Bouchama et al, "Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns", 2024.
[21] M. A. Ridwan et al, "Applications of Machine Learning in Networking: A Survey of Current Issues and Future Challenges", 2021.
[22] Amin Shahraki et al , "A comparative study on online machine learning techniques for network traffic streams analysis", 2022.
[23] M. Alauthman et al, ``An ef_cient reinforcement learning-based botnet detection approach," J. Netw. Comput. Appl., vol. 150, Jan. 2020, Art. no. 102479.
[24] C. Zhang, P. Patras and H. Haddadi, "Deep learning in mobile and wireless networking: A survey", IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2224-2287, 3rd Quart. 2019.
[25] A. Géron et al, Hands-On Machine Learning With Scikit-Learn Keras and TensorFlow: Concepts Tools and Techniques to Build Intelligent Systems, Canada:O'Reilly Media, 2019.
[26] F. Chollet et al, Deep Learning With Python, Shelter Island, NY, USA:Manning Publications, 2017.
[27] Y. LeCun, Y. Bengio and G. Hinton, "Deep learning", Nature, vol. 521, pp. 436-444, May 2015.
[28] Ali Ghaffari et al, "Securing internet of things using machine and deep learning methods: a survey", 2024.
[29] Dusmurod Kilichev et al, "Next–Generation Intrusion Detection for IoT EVCS: Integrating CNN, LSTM, and GRU Models", 2024.

[30] Zhaolian Wang et al , “IoT Intrusion Detection Model based on CNN-GRU”, 2023.
[31] Basim Ahmad Alabsi et al , “CNN-CNN: Dual Convolutional Neural Network Approach for Feature Selection and Attack Detection on Internet of Things Networks”, 2023.
[32] Yulin Wang et al, “Network Intrusion Detection Method Based on Improved CNN in Internet of Things Environment”, 2022.