DOI: 10.21917/ijct.2022.0419

IMPROVED RESOURCE ALLOCATION IN 5G USING DEEP LEARNING

P. Sachidhanandam[1], V. Amirtha Preeya[2], B.H. Impa[3] and M. Ranjith Kumar[4]

[1]Department of Information Technology, Knowledge Institute of Technology, India
[2,3]Department of Computer Science and Engineering, Presidency University, India
[4]Department of Computer Science and Business Systems, Knowledge Institute of Technology, India

Abstract

All wireless equipment, including terminals, base stations, and phones, functions as a component of a single interconnected system, it is subject to attacks from a wide variety of different forms of cyber threats. This elucidates the relevance of considering the aforementioned attacks in order to prevent them from finally acquiring control of the complete system environment. The term cybersecurity refers to the set of preventative measures that are implemented to safeguard an information technology infrastructure against being corrupted or destroyed. The results of a performance evaluation that was carried out on the DRL at several different node densities. When there is a requirement to analyze a network in terms of its throughput, delivery ratio, and latency, NS2 is the tool that is utilized. In this article, a comparison and contrast between the Lagrange Duality Method technique is presented.

Keywords:

Wireless Equipment, Cybersecurity, Resource Allocation, Deep Learning

1. INTRODUCTION

With the advent of fifth-generation (5G) networks, the typical length of time needed to set up a service will be reduced from ninety hours to just a few minutes [2]. Around 7 trillion different gadgets and things will be connected to these networks. This is the next step that should be taken in the evolution of 4G mobile communication technologies, which have already made it possible to satisfy the expectations of widespread broadband access. This is the next step that should be taken in the evolution of 4G mobile communication technologies. With this security architecture, which extends the ideas of 3G and 4G security architectures to serve the emerging 5G environment [1], networks will be able to efficiently handle a wide variety of service types.

The technology that enables multiple access, such as that which is made possible by non-orthogonal multiple access, will serve as the basis for future wireless network architectures (5G). We are able to make more efficient use of the power domain to serve multiple users at the same time when we combine NOMA with the technologies that make it possible to have 5G. This opens up interesting paths for study into enhancing user fairness, mass connection, extended coverage area, reduced latency, enhanced data rates, better capacity gains, and improved efficiency performances. Among other things, these are all areas that could benefit from research. The priority should be placed on the security that is provided by NOMA when it comes to the planning and implementation of 5G wireless networks. As a direct result of this, we place an extremely high focus on ensuring the safety of 5G networks that make use of NOMA [4].

The degree to which people rely on the Internet is directly correlated to the amount of attempts that hackers make to take advantage of it [3]. These attempts typically involve the use of ever-evolving methods to cause damage. It is possible for a wide variety of attacks, such as packet sniffing, unauthorized access, injection, session hijacking, distributed denial of service (DDOS), flooding, and dropping, to target the systems that make up wireless network environments [5]. There have been a significant number of investigations carried out in this area, some of the more noteworthy of which are [6].

A vast number of algorithmic and technological solutions have been conceived of and put into practice with the purpose of achieving the goal of ensuring that computer networks are secure. Utilizing machine learning and artificial intelligence (AI), which enables the creation of self-improving systems by training them on labeled datasets and allowing them to hone their accuracy over the course of time in response to patterns of behavior [7], is one strategy that is effective. This is because machine learning and AI enable the creation of self-improving systems.

2. LITERATURE REVIEW

Researchers have been focusing their efforts on developing approaches that make use of both deep learning and machine learning as a result of the disturbingly high rate at which hostile attacks are being launched against network infrastructure. Other researchers in the academic world have also made efforts to model 5G networks and evaluate the extent to which these networks are susceptible to being attacked. In order to generate an accurate depiction of the network, they made use of a number of modeling applications, including Omne++, Ns2, and Ns3.

The authors of the paper [8] built a 5G environment with the assistance of the OMNeT++ Simulator so that they could test out a variety of software-defined networking configurations that could be used in a variety of different types of intrusion detection scenarios. In order to do this, the authors used the OMNeT++ Simulator. In addition to the application, there is a notion that provides an explanation of the potential part that SDN could play in ensuring the safety of 5G networks. The findings indicate that it is possible to construct security components for 5G networks using software-defined networking (SDN) application frameworks. This is demonstrated by the findings.

Previous studies [9] have placed a significant amount of emphasis on the relevance of preventing unwanted access to 5G networks. Mina Malekzadeh and colleagues [10] assert that they built and implemented OMNeT++-based simulation modules that accurately reflect real-world wireless denial of service attacks. This is according to what they have to say about it. As an illustration of one possible way for comparing the results of simulations, take into consideration the latency from beginning to conclusion, as well as the packet loss ratio. They are now in a position as a direct result of this to test OMNeT++ and the reliability of the simulation results in relation to wireless denial of

service attacks. This paves the way for recognizing and preventing attacks of this sort within wireless networks, which opens up new possibilities. The authors of the paper [5] provide a network-centric intrusion detection system that is able to distinguish between malicious and benign activities taking place on a network. By applying this method, they were able to discern between three distinct types of jamming. Additionally, they were able to reduce the number of false alarms and enhance the number of successful detections. The OMNet++ simulation building tool was utilized during the development of their prototype by the group.

The authors of [11] investigate the capability of unsupervised learning that DL possesses as well as its potential application in the detection of network vulnerabilities. We investigate both the benefits and drawbacks of utilizing DL for the purpose of conducting intrusion detection. They developed a model that was comprised of many layers of neural networks, and it had a degree of accuracy that was 99%. They, unfortunately, relied on the KDD99 Dataset, which has been out of date for the past twenty years and does not adequately reflect the most recent state of network security.

In the most recent investigations carried out in this subject, a variety of diverse studies have taken use of machine learning. In [12], a novel authentication method that is based on machine-learning algorithms is proposed. This technique attempts to produce more effective security in 5G wireless networks by boosting the intelligence in the authentication layer by exploiting the features of the physical layer. Specifically, this strategy will increase the number of attributes that can be exploited. In order to recognize potential cyber threats and attacks on 5G mobile networks working on the development of a network security system. There have been a number of studies conducted with the objective of evaluating whether or not deep learning frameworks are effective in identifying instances of this kind of attack. The purpose of this activity is to determine which participant is capable of carrying out the greatest number of computations in the least amount of time. They perform their tasks with a very high degree of precision [8]. Analyzed the simulated network flows of both typical and unusual traffic patterns.

In this setting, every single wireless device is linked to every other wireless device in the area. Hackers may target a wide variety of devices to disrupt a wireless network. These devices may include wireless terminals and cell phones, in addition to access points and even more. This sheds light on the danger of these attacks and the required steps that need to be taken to prevent them from capturing complete control of the system.

Cybersecurity is the process of safeguarding a network or computer system from being penetrated or attacked with another computer network or the Internet. This approach is also known as network or computer system defense. Machine learning is one of the many algorithms and technologies that have been developed for the purpose of improving cyber security; nonetheless, it is one of the most successful. The field of artificial intelligence known as machine learning is responsible for the development of self-improving systems. This is accomplished by first instructing machines to recognize patterns in data, and then continuously enhancing their capabilities over the course of their use. The field of cyber security has also seen the development of other algorithms and technologies.

After successfully attracting attention to the development of 5G wireless communication systems, non-orthogonal multiple access, also known as NOMA, is an essential component of 5G communications. The most notable benefit of 5G networks is the improvement in speed, which might be one hundred times faster than that of 4G networks. Wireless intrusion detection systems are an essential component of any system that is connected to the Internet. This is because the network is subject to an increasing number of attacks, both internal and external, which can come from a variety of sources.

In addition, the data transfer rate as well as the level of security that is utilized will need to undergo significant development to be compatible with 5G. Concerns raised regarding the safety of 5G networks as well as NOMA deployments were discussed, and potential solutions were offered. By employing a simulated Noma and the specified attack dropping attack, we were able to obtain the data that was necessary for assessing which solutions would best secure the safety of the network while also preserving its high performance and quality. Because of this, we were able to evaluate which potential solutions would be the most successful. We used the dropping method to narrow down the NOMA simulator that we built so that we could select only the data that was most pertinent to our study.

3. PROPOSED MODEL

Iterative learning from sample data is included in the vast majority of machine learning algorithms, which ultimately leads to models that are continuously growing more accurate. A single generic model cannot determine the right model parameters for all data types as a result of 5G network slicing because the data types are created by billions of diverse sets of devices. This makes it impossible for a single model to be general.

When it comes to the management of network resources, a smartphone has more requirements than an Internet of Things device such as a sensor, which has fewer resources available and is more susceptible to power loss. A smartphone, on the other hand, is more like to have access to a computer. When we examine this topic in further depth, we notice that the standards for a smartphone are significantly more severe in this particular area.

Latency is a problem that affects many different types of applications, but it is especially problematic for those that deal with augmented and virtual reality (AR/VR) as well as mission-critical services. In addition to that, the majority of UEs do not constantly operate. There is no requirement for an Internet of Things device to maintain a constant connection to the network; all it needs to do is check in with the server at regular intervals. Because of this, Internet of Things devices are able to save network resources.

It is possible that the use of a connected automobile, which is sometimes referred to as a Vehicle-to-Everything (V2X) UE, will involve a number of handoffs, just like the use of other forms of mobility. However, if we know how the car is typically used and where it goes, we can direct it to connect to locations that require the fewest number of handoffs and the most consistent and dependable links. If we know how the car is typically used and where it goes, we can direct it to connect to these locations.

There is a possibility that the KPIs will change depending on the particular kind of network service or application that is being

measured. When it comes to the generation of data, certain types of UE are significantly more effective than others is an innovative learning model for wireless communication because it creates an adaptive learning model for each of these distinct slices in order to address issues with resource management.

The ability of a single global model to be applied to a more constrained set of specific data in order to produce new predictions and estimations is what is indicated by the term adaptive. This model must have been trained on a big dataset first. Because of this, we are able to enhance performance while also cutting down on the amount of time and effort needed training the model.

The supply of traditional mobile broadband application services and the collection of traffic statistics from end devices such as smartphones are both included in the responsibilities of Slice A.

It is concerned with the data that is shared by machines and machine-like systems, such as those utilized in Industrial 4.0 and the Internet of Things. The term Slice B refers to massive machine communication, which is also referred to as mMTC or mIoT, and it is concerned with the data that is shared by machines and machine-like systems (IoT). The transfer of URLLC data is made possible by Slice C, which also supports augmented and virtual reality (AR/VR), in addition to providing support for emergency services.

Every single one of these data slices has an entirely unique workload, set of services, and assortment of data attributes in comparison to the others. To begin, we will make an estimate of the load on the network by utilizing the whole three-slice inputs (A, B, and C) as our three input vectors. This will allow us to get a better sense of how the network is being utilized. After that, in the second phase, we make use of the input vector that corresponds to that slice in order to make an educated guess regarding the load that will be applied to that slice (Slice A only, Slice B only, Slice C only).

Our research is based on the three standard slices that are defined by the 3GPP SST. However, there is no constraint on the number of slices that a network operator can deploy and there is no limit to the total number of possible slices. In this work, we made use of deep neural networks that had five different layers. Input layers (features), hidden layers 3, and output layers were the layers that were present (prediction). By making adjustments to the number of hidden layers, the learning rate, the activation function, and the number of epochs, we were able to fine-tune the MDNN model hyperparameters. Because we want to evaluate the performance of the model with both random weights and learned weights, we preserved the DNN modeling we were using for MDNN and applied it to MDNN. This is because we want to test the performance of the model using both types of weights.

Each time the training procedure is carried out, a new network with a new model is fitted. This is because the algorithm employs randomness to build an appropriate set of weights for the specific input-output mapping function of the data. This is because the process makes use of unpredictability, which is why it has this effect. The gradient estimate for each batch is one of a kind due to the fact that the training dataset is restructured in a manner that is completely random just before the beginning of each epoch.

The multi-layer MDNN model is trained by a feed-forward backpropagation network, which initially begins with random weights due to the fact that the weights are randomized (stochastic gradient descent). A forward pass through the network is considered complete whenever the required output has been reached after iterative computations have been carried out on each neuron in the subsequent layer. A cost function, designated by the letter C, and the desired output, which is found in the output layer, are utilized in order to do an analysis that determines the level of quality possessed by the output that has been produced. Evaluation loss functions are rather common, with mean squared error being one of the more widespread examples (MSE).

After the initial result has been acquired by altering the weights and biases, a backward pass is performed in order to optimize the cost function. This is done after the original result has been obtained by adjusting the weights and biases. C. Changing the weights and biases is how this is accomplished after the initial result has been generated by the model. By modifying the parameters of the complete neural network in a number of different ways, our goal is to get the highest quality output that is humanly possible. We are able to compute the overall loss, evaluate the performance of the model (determining whether it was very good or very poor), and then make any necessary revisions to the weights in order to achieve the least amount of loss that is possible. Following the completion of the step involving backpropagation, the computed weights, which are also referred to as the learnt weights, are recorded for each layer TL parameters. The term trained weights is used to refer to these particular weights.

4. EVALUATION

The goal of the study is to identify a method that is not only quick but also secure, with as little lag time as possible occurring between handoffs. It was discovered that there was a decrease in the amount of time spent waiting for authentication after the results of the simulation were analyzed for the communication overhead and the complexity of the computing. The research indicates that the recommended solution performs better than the most recent and cutting-edge approaches to the problem.

Table.1. Performance Analysis – Energy Efficiency

Small Cells	**Slice A**	**Slice B**	**Slice C**	NOMA	**Proposed 5G**
18	0.48	1.8	2.5	4.21	8.2
36	0.91	4.1	5.23	8.16	13.53
54	2.33	8.95	11.81	14.52	20.8
72	3.5	11.54	16.02	18.64	26.02

Table.2. Performance Analysis - Handoff

Small Cells	**Slice A**	**Slice B**	**Slice C**	NOMA	**Proposed 5G**
18	30.49	29.84	28.55	24.29	18.36
36	30.93	32.18	31.33	28.32	23.80
54	32.38	37.13	38.05	34.81	31.22
72	33.57	39.77	42.34	39.01	36.54

Table.3. Performance Analysis – throughput

Small Cells	**Slice A**	**Slice B**	**Slice C**	NOMA	**Proposed 5G**
18	30.96	31.60	31.00	28.42	26.40
36	31.82	36.20	36.46	36.32	37.06
54	34.66	45.90	49.62	49.04	51.60
72	37.00	51.08	58.04	57.28	62.04

Table.4. Performance Analysis - Delay

Small Cells	**Slice A**	**Slice B**	**Slice C**	NOMA	**Proposed 5G**
18	30.72	30.70	29.75	26.32	22.30
36	31.37	34.15	33.85	32.24	30.30
54	33.50	41.43	43.72	41.78	41.20
72	35.25	45.31	50.03	47.96	49.03

The answer to this question can be found by totaling up all of the packets that are entering and departing the network. When there is an increase in the volume of traffic, maintaining the same flow of traffic becomes a more challenging task. As a direct result of this, the throughput, PDR, and delay are all adversely affected. On the other hand, the throughput, PDR, and delay are all improved by the DRL approach.

This is the total number of bits or bytes that all of the autos were able to successfully receive. This could be impacted in a communication arrangement by a wide variety of factors, such as the constraints imposed by the physical medium beneath the surface, the level of processing power made available by the system, and the characteristics of the endpoint that is being received. In other words, this could be impacted in a variety of ways.

In this part of the article, the Lagrange Dual Method and the system that has been proposed will each be analyzed and compared to one another. Utilizing the universal approximation capabilities of deep neural networks (DNNs), which can be accomplished with the assistance of a computer program, can make it easier to establish a connection between the input and the optimization result. This connection can be facilitated by using the capabilities of DNNs. The trained DNN is provided with a new parameter in real time, which it may then employ in order to execute the change and provide a solution that is both efficient and prompt.

5. CONCLUSION

The strategy that has been suggested searches for the technique that results in the most advantageous distribution of resources across the several uses to which vehicles may be put. In order to successfully execute parameterization, a dataset that is available to the general public without charge was leveraged. After keeping track of data like as speed, location, and travel direction, the RSU locates the neighbors of the next forwarding node that are nearest to them and most directly connected to them. This is done so that the RSU can transfer data to those neighbors. This helps to cut down on the amount of time required for the transfer of data from one device to another. When utilizing the Q-network, the Bellman-Ford method is applied to identify the route that provides the least travel distance between the RSUs. The amount of time that is required to make a choice and authenticate a user has been greatly reduced, which has resulted in a 12% decrease in handoff latency. When compared to earlier cryptographic protocols, the DS2AN technique requires a far less amount of cryptographic key generation and a much smaller amount of message exchanges between the vehicle and the network.

REFERENCES

[1] D. Basu and R. Datta, "SoftDrone: Softwarized 5G Assisted Drone Networks for Dynamic Resource Sharing using Machine Learning Techniques", *Computers and Electrical Engineering*, Vol. 101, pp. 107962-107975, 2022.

[2] Qian Zhu, "Substrate-Integrated-Waveguide-Fed Array Antenna Covering 57-71GHz Band for 5G Applications", *IEEE Transactions on Antennas and Propagation*, Vol. 65, No. 12, pp. 6298-6306, 2017.

[3] I. Ahmad, W. Tan and H. Sun, "Latest Performance Improvement Strategies and Techniques Used in 5G Antenna Designing Technology, a Comprehensive Study", *Micromachines*, Vol. 13, pp. 717-736, 2022

[4] L. Yang, S. Shangguan and S. Li, "Location InformationAssisted Robust Beamforming Design for Ultra-Wideband Communication Systems", *Symmetry*, Vol. 14, No. 6, pp. 1171-1178, 2022.

[5] C.A. Balanis, "*Antenna Theory: Analysis and Design*", John Wiley and Sons, 2016

[6] M.S. Almutairi, "Deep Learning-Based Solutions for 5G Network and 5G-Enabled Internet of Vehicles: Advances, Meta-Data Analysis, and Future Direction", *Mathematical Problems in Engineering*, Vol. 2022, pp. 1-9, 2022.

[7] A. Adekunle, K.E. Ibe, M.E. Kpanaki, C.O. Nwafor, N. Essang and I.I. Umanah, "Evaluating the Effects of Radiation from Cell Towers and High-Tension Power Lines on Inhabitants of Buildings in Ota", *Journal for Sustainable Development*, Vol. 3, No. 1, pp. 1-21, 2015.

[8] Y. Fu and X. Wang, "Traffic Prediction-Enabled Energy-Efficient Dynamic Computing Resource Allocation in CRAN Based on Deep Learning", *IEEE Open Journal of the Communications Society*, Vol. 3, pp. 159-175, 2022.

[9] Yi. Huang and K. Boyle, "*Antennas from Theory to Practice*", John Wiley and Sons, 2008.

[10] L. Zhong and B. Ren, "Slice Allocation of 5G Network for Smart Grid with Deep Reinforcement Learning ACKTR", *Proceedings of International Conference on Intelligent Computing and Signal Processing*, pp. 242-249, 2022.

[11] M. Rajalakshmi, V. Saravanan and C. Karthik, "Machine Learning for Modeling and Control of Industrial Clarifier Process", *Intelligent Automation and Soft Computing*, Vol. 32, No. 1, pp. 339-359, 2022.

[12] H. Zhou and H.V. Poor, "Learning from Peers: Deep Transfer Reinforcement Learning for Joint Radio and Cache Resource Allocation in 5G RAN Slicing", *IEEE Transactions on Cognitive Communications and Networking*, Vol. 8, No. 4, pp. 1925-1941, 2022.