ANSPOLY Journal of Advanced Research in Science &Technology
Volume 1; Issue 1; March 2024

MONITORING OF A COMMUNICATION NETWORK USING ARTIFICIAL INTELLIGENCE-ENABLED ROUTING TECHNIQUE

Ezeobi Onyeka Stanislaus[1], Ernest_Okoye Ngozi[2], Okoli Boniface Chukwuma[3]
[1]Department of Computer Engineering Technology,
Anambra State Polytechnic, Mgbakwu, ostaneze@gmail.com
[2] Department of Computer Engineering Technology,
Anambra State Polytechnic, Mgbakwu, ernestokoyengozi@gmail.com
[3] Department of Computer Engineering Technology,
Anambra State Polytechnic, Mgbakwu, okolibonifacechukwuma@gmail.com

Abstract

A networking design known as Software-Defined Networking (SDN) separates the control plane from the data plane and consolidates network administration into a single location known as the controller. The flow tables for every switch in the data plane must be prepared by the controller. While dynamic routing may reroute in the event of congestion by regularly assessing each data flow's condition, issues with an appropriate monitoring period duration and the inability to learn from prior mistakes to prevent making similar but inefficient route choices still need to be resolved.This paper introduces an Artificial Intelligence Enabled Routing (AIER) mechanism with congestion avoidance in SDN. By introducing Artificial Intelligence (AI) technology, this mechanism can not only provide learning ability and superior route decisions, but also mitigate the impact of monitoring periods with dynamic routing. By adding three more modules to the control plane—topology discovery, monitoring period, and artificial neural network—we assess the effectiveness of the suggested AIER mechanism using the Mininet simulator. Performance measurements, such as average throughput, packet loss ratio, and packet delay vs data rate for various system monitoring periods, show the efficiency and superiority of our suggested AIER method.

Keywords: Network Monitoring; Communication; Artificial Intelligence; Routing; Software Defined Network; Artificial Neural Network

INTRODUCTION

Since the start of the Fifth Generation (5G) research phase in 2012, the designs for the network system have advanced quickly. End-to-End (E2E) network slicing, which crosses network domains such the Core Network (CN) and Radio Access Network (RAN), is considered the core foundation of the 5GS. As a result, several logical networks that correspond to various business functions or verticals can use a similar infrastructure (Lee et al., 2018).

Because of the variety and constant emergence of new communication services driven by verticals, the mobile communication sector must provide numerous telecommunications services with heterogeneous Key Performance Indicators (KPIs) in a cost-effective manner. Mobile network operators have unique chances to provide new business models to consumers, organisations, verticals, and third-party tenants and satisfy varied requirements thanks to the network, which is driven by network virtualization and network slicing (Arjoune et al., 2020; Wang et al., 2019). Thus, in order to accomplish this aim, research initiatives as well as standardisation efforts have detailed the primary components of the network architecture (Cayamcela and Lim, 2018).

The safety of vital network infrastructure and user privacy in a setting where every device is connected to the internet and vulnerable to numerous potential attacks are just two of the major security challenges that come with network technology (Salahdine, 2018; Lai et al., 2020). For instance, damage to the electrical system and disruption to other associated systems and services might result from a security compromise in a smart grid system. Sending sensitive data across the network also puts user privacy at risk. As a result, creating security solutions that can safeguard the network and guarantee fast data speeds and minimal latency is imperative. The particular network use case at hand determines how security difficulties and vulnerabilities should be categorised (Liu et al., 2017; Tran et al., 2017).

Insider, outsider, network, and virus attacks are the four primary categories of security breaches in networks. An insider attacker is a person who attempts to alter a system's behaviour by interfering with its control and execution processes. The objective of an

external attacker is to impact the communication system through the collection of data or the acquisition of sensitive information (Mijumbi et al., 2016). While virus assaults utilise software to get access to a system for nefarious reasons, network attackers try to shut down or interfere with a network's operation. These attacks fall into two groups: those that target the network and those that target users. Device trigger, node capture, and privacy leakage are a few threats that fit within the user category (Yang and Fung, 2016; Ahmad et al., 2018).

For networks today and in the future, monitoring is an essential function for controlling security and performance. New ideas in networking have, however, both simplified and complicated security and monitoring tasks. The ideas encompass distributed computing, such as massive Internet of Things (mIoT), massive Machine-Type Communications (mMTC), vehicle-to-everything (V2X), and fog computing; programmability of networks, such as Software-Defined Networks (SDN); virtualization, such as Network Function Virtualization (NFV), network slicing, cloud computing, and Mobile Edge Computing (MEC); and greater intelligence, such as cognitive and intent-based networks, Artificial Intelligence (AI), and Machine Learning (ML). These ideas provide more chances for security and monitoring, but they also bring with them new risks and difficulties that need to be resolved. (Liyanage and others, 2018).

According to Abbas et al. (2015) and Liu et al. (2016), Artificial Intelligence (AI) is a technological science that investigates and creates theories, approaches, strategies, and application systems for mimicking and expanding human intellect. It is really important from a social and economic standpoint, and AI is altering people all the time. how you work, learn, and live. According to Moosavi et al. (2016), artificial intelligence is a recognised study topic and development direction for critical information infrastructure security. It has conducted multi-level research and productization practice in certain theories, systems, technologies, and engineering both domestically and internationally.

SDN is a new networking architecture that centres network administration at the controller and separates the control plane from the data plane. The flow tables for every switch in the data plane must be prepared by the controller. While dynamic routing can

reroute in the event of congestion by regularly assessing each data flow's state, issues with an appropriate monitoring period duration and the inability to learn from past mistakes to prevent making similar but inefficient route selections still need to be resolved. (Wu et al., 2020). The aim of this paper include is to implementation of artificial intelligence approach for real-time monitoring of a computer network behaviours. This study provides an AI-Enabled Routing Scheme (AERS) particularly for SDN, focusing on the application of artificial intelligence (AI) technology to CN routing. This is because the fundamental ideas of both SDN and NFV technologies are very complimentary to each other, making them ideal candidates for integration.

Literature Review

Zhou et al., (2023) presents an AI-based model on multi-step feature engineering and deep attention network for optical network performance monitoring. The following three phases make up the primary modelling process: In Step I, features are first extracted from the original data using the Asynchronous Amplitude Histogram (AAH) approach. In Step II, the feature dimension is decreased and the optimised feature is sent to the downstream predictor using the Kernel Principal Component Analysis (KPCA) and Q-learning methods. In step III, the downstream predictor that is based on the attention mechanism and Long Short-Term Memory (LSTM) network may successfully create the feature-label mapping and achieve data prediction. As a consequence, the report concluded that component comparisons and ablation experiments show how well the suggested framework can integrate predictors and feature engineering to provide superior outcomes.

Zhou (2020) presents an AI driven wireless network remote monitoring based on Diffie–Hellman (DH) parameter method. The kinematics formula is constructed and the linkage coordinate system of wireless network remote monitoring is established using the DH parameter approach. The geometric analysis approach is used to determine the optimal motion path, precisely find the different angles of remote monitoring, and compute the motion trajectory of remote monitoring. Fuzzy control is based on the Pm angle control method of the Radial Basis Function (RBF) neural network. Fuzzy control uses the neural network's self-learning capacity and fuzzy reasoning to combine control with Pm control.

The end effector was adjusted to the target position. The performance evaluation of the system was not reported in the study.

Liu (2023) researched on the design of wireless communication base station monitoring system based on artificial intelligence and network security. To address the significant issues of "monitoring without control and low reliability" in the conventional staffed computer room for monitoring, an effective and reliable wireless communication base station monitoring system must be established in light of the advancements and challenges of wireless communication technology. A brand-new kind of surveillance system is suggested. With its triple function of monitoring, management, and automated alarm based on the widely used video surveillance technology, it offers the greatest technological solution for enhancing communication network operating capability and cutting down on operation and maintenance costs.

Zidek (2023) researched on network monitoring using AI. This study discusses the use of AI in network monitoring, including its main benefits and potential drawbacks. It goes into great depth on the network's forecasts and founding history, as well as what lies ahead for service analysis, protection, and enhancement. The study is a review work which did not report the implementation of the AI technology in network monitoring but emphasizes the need for implementing such technology in future research works.

Minea et al., (2021) presents the application of software sensing and machine learning solutions for intelligent network application monitoring and diagnosis. The adopted method's primary goal is to offer a time series prediction strategy. The foundation of this method is a multi-resolution signal decomposition using the Undecimated Wavelet Transform (UWT). The study of Long-Range Dependence (LRD), or in this example, a long-term reliance, forms the basis of the second method for evaluating traffic flow. By calculating the Hurst parameter of the time series under analysis, one may determine the extent of long-range dependency. UWT may be used to implement this relatively new statistical notion in communications traffic analysis. The selected approach is predicated on long-term reliance on traffic, and a Model Predictive Control (MPC) in conjunction with a neural network using RBF is suggested for the purpose of fault occurrence

prediction. The findings of the simulation show that the suggested approach, which makes use of the neural network-based model's predictive control, performs better than the traditional predictive control, particularly in situations when there is a lot of uncertainty.

Research Method

This research work will adopt both Simulation and design modeling approach; software like MATLAB will be used to develop models and results. The first step in the realization of the goal of this research is the modelling of a AIER mechanism for route control in data networks. To find the route between any source-to-destination pair at the beginning, the application plane's routing module is employed. The controller comprises three modules: topology discovery, period monitoring, and artificial intelligence (AI) model used to explore link states through OpenFlow switches. Following this, information exchange from the data plane is periodically received, and the AIER mechanism is implemented to select the least congested intelligent path.

The third major step carried out in the realization of the goals of the work is the creation of MATLAB/SIMULINK model as a test bed for the implementation, performance and validity assessment of the proposed link control scheme. The final step carried out is the simulation, presentation and discussion of the results. The key goal here is to validate whether the simulation results give indications that show that the proposed scheme presents the network performance metric as it related to link characteristics of spectral efficiency, link utilization, throughput.

Architecture of Network Technology

According to Arabo and Pranggono (2013), the architecture is built with extremely sophisticated network components and terminals to support a novel scenario. Furthermore, service providers may quickly integrate cutting-edge technology to deliver services with additional value. For interoperability across wireless and mobile networks, the system is built on an all-IP approach (Mantas et al., 2015). An illustration of the network system's architecture is shown in Figure 1.

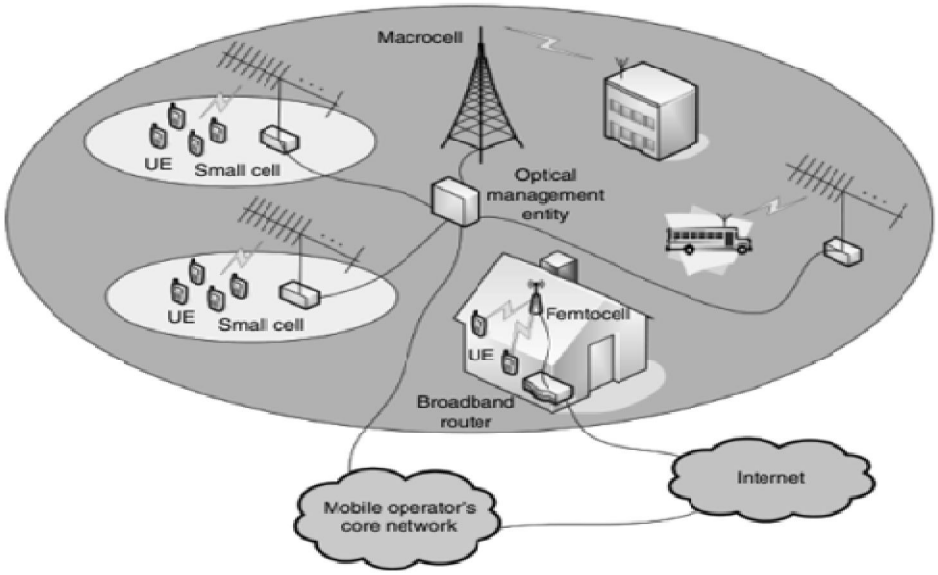

Figure 1: Communication Architecture of the Network (Mantas et al., 2015)

According to Flo and Josang (2009), IP technology is especially made to manage the information required for directing IP packets associated with a specific application connection or session between client applications and servers on the Internet. A user terminal, which is an essential component of the design, and many separate radio access technologies make up the system (Piqueras, 2013). Every radio access technology within the terminal is regarded as a separate IP connection to the web. Nevertheless, a distinct radio interface is needed for every Radio Access Technology (RAT) in the mobile terminal (Seddigh et al., 2010). For example, the mobile terminal requires four separate access-specific interfaces in order to access four different RATs. For the architecture to function, each of them has to be running at the same time (Forsberg et al., 2007).

AIER Mechanism

By adding an Artificial Neural Network (ANN) model to the SDN controller, the proposed AIER method offers protection against link fabrication attacks and migration of OpenFlow switches (Khan et al., 2020). Initially, a set of training data is gathered via the AIER method, with each record comprising feature and label data. Next, the ANN model is repeatedly trained using the training set of data. Once the model has been trained, the routing algorithm acquires learning capabilities. As a result, the AIER mechanism may

choose an appropriate routing to prevent congestion in addition to predicting the relevant output based on the incoming input. The following three steps make up the suggested AIER mechanism's pseudo code, which is shown.

Pseudocode of the AEIR mechanism (Wu et al., 2020)

Start

Input:

- Number of source nodes: n
- Number of destination nodes: m
- Number of available paths: R
- ANN model, which is obtained by training data and validated by test data
- Loads for all data flows: L= <L_1, L_2, …, L_n>// d = mn
- All available path configurations: <P_1, P_2, …, P_n> // S = R^d, |P_k| = d

Output:

Minimum congestion probability ($_{Cmin}$) among all path configurations

1. set C= [ ]
2. while has variation do
3. for each P_k do
4. ANN model input (L, P_k)
5. Ck = ANN model output
6. Append(C, C_k)
7. end for
8. C_u = congestion probability of the current path configuration
9. C_{min} = min{C}
10. if C_{min}< C_u&& (C_u − C_{min}) > Th
11. Conduct path reconfiguration to P_k with C_{min}
12. end if
13. if queuing length of any switch in the current path configuration > 80%
14. Trigger path reconfiguration
15. end if

Data Collection

An appropriate amount of training data is gathered before the ANN model is trained. Each record in the training data includes a congestion flag, the generation rates of all data flows, and every path that is allotted from a source to a destination. As an example, assume n = 3, m = 1, and R = 3 as shown in Figure 2. The training data set, comprising several data samples and all fields from each record, is displayed in Table 1. Depending on whether there is at least one OpenFlow switch with a queue length longer than 80% along the designated path, field "C" may be set to 1 or 0. C is 1 if the answer is yes; else, it is 0. The d fields immediately following from Field "C" represent the data generation rates of d data flows. The last d fields indicate the allocated path number (belonging to {0, 1, 2}) for each data flow.

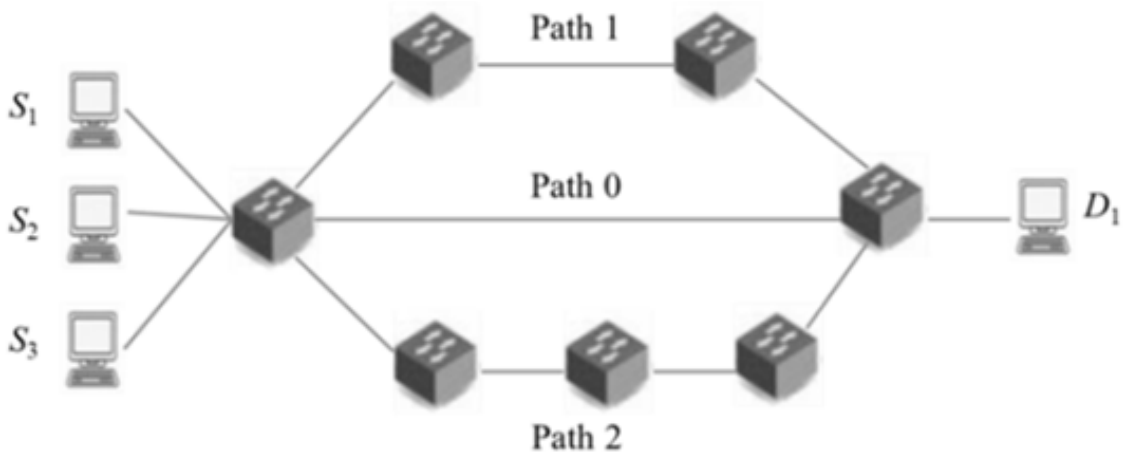

Figure 2: Data plane in the SDN (Wu et al., 2020)

Table 1: Training dataset fields

C Congestion Flag	**S_1-D_1 Data Flow**	**S_2-D_2 Data Flow**	**S_3-D_3 Data Flow**	**S_1-D_1 Allocated path number**	**S_2-D_1 Allocated path number**	**S_3-D_1Allocated path number**
0	57M	55M	70M	0	1	2
1	65M	63M	30M	0	0	1
0	65M	50M	65M	0	2	1

Training Of the Ann Model

Following the conclusion of the first phase, we train the ANN model using the Back Propagation Algorithm (BPA) (Rumelhart et al., 1986). Before training the model, the training data must be pre-processed. As indicated in Table 1, we divide the label data and feature data in the training data set. We use Field "C" as the label data and the other fields as the feature data. Each record's feature data serve as the inputs for a neuron model, while each record's label data are utilised to calculate errors with regard to the neuron model's output. Moreover, the feature data must be normalised such that their values fall between 0 and 1.Next, using the tenet that the former subset is much bigger than the latter, the training data set is split at random into two subsets: a training data subset and a test data subset. The test data subset is used to confirm that the trained ANN model is accurate, whereas the training data subset is used to train the ANN model. Accuracy typically has to be at least 0.8.

ANN Mode Application

Three source-to-destination pairings and three pathways mean that there are 33 possible ways to configure the path. For path configuration in the controller, the ANN model trained in the previous step is utilised. The congestion probability is computed for each path configuration k and is represented by Ck, as shown in Table 2. Assuming that the current path configuration is {0, 0, 0}, the controller will switch out the current path configuration for one with the least possibility of congestion if any congestion probabilities exist that are lower than the current path configuration by a predetermined threshold (denoted as Th), such as 20%. For example, in Table 2, the new route configuration will be {2, 2, 1}.The controller is in charge of sending the updated path configuration to the OpenFlow switches in the data plane via the southbound interface. The so-called ping-pong effect can be avoided by using the specified threshold Th. Furthermore, in order to prevent possibly erroneous output in the trained ANN model, the AIER mechanism can regularly check the queue duration of each OpenFlow switch for the present route configuration. Path reconfiguration occurs when an OpenFlow switch experiences any queue length longer than 80%.

Table 2: Congestion probabilities resulted from the trained model.

Configuration k	Data Rate (Mbps)			Path Configuration			Congestion Probability
	S_1-D_1	S_2-D_1	S_3-D_1	S_1-D_1	S_2-D_1	S_3-D_1	C_k
1	70	75	90	0	0	0	0.90
2	70	75	90	0	0	1	0.70
3	70	75	90	0	0	2	0.65
…	…	…	…	…	…	…	…
26	70	75	90	2	2	1	0.55
27	70	75	90	2	2	2	0.80

System Implementation

It is necessary to have the network model that serves as the proof-of-concept test bed for the suggested link control. The MATLAB LTE toolbox's code library modules offer code libraries for implementing the essential functions of LTE networks. During the simulator's development, an Embedded MATLAB function is used to calculate the Pre-coding Matrix Indicator (PMI). The Simulink library's Rectangular Quadrature Amplitude Modulation (QAM) Demodulator Base-band block powers the demodulator in the LTE test bed simulator. The Embedded MATLAB Function block is utilised in the simulator to accomplish the segmentation, zero-padding, and soft combining operations.

The AIER algorithms must be implemented on software in order for the simulation to be performed. The traffic creation code module of the simulation programme generates the characteristic network traffic by using the traffic model acquired connection characteristics model (Kozo et al., 2020).

Table 3 provides a summary of the parameters and their values utilised in the simulation. The Dijkstra algorithm is used by the application plane's routing module. OpenFlow Protocol V1.3 is used as the communication link between the data and control planes. Nine possible transmission channels, one destination node, and three source nodes make up the data plane's network structure. As a result, 729 route configuration outcomes in all

are found.We build UDP flows at data speeds ranging from 70 Mbps to 150 Mbps using the Iperf (Iperf, 2020) tool. Every link has a capacity of 250 Mbps. Every OpenFlow switch has a buffer size of 200 packets. Three, five, or ten seconds is the set monitoring time.

Table 3: Parameters and values used in the simulation.

Parameters	**Values**
Simulator	Mininet 2.3.0
SDN protocol	OpenFlow V1.3
Packet generator	Iperf
Traffic type	UDP
Link bandwidth	250 Mbps
Data rate	70 Mbps ~ 150 Mbps
Buffer size	200 packets
Routing module	Dijkstra algorithm
Monitoring period	3, 5, or 10 s
No. of source nodes 3	3
No. of destination nodes	1
No. of available paths	9

In the control plane, an ANN model called a Multilayer Perceptron (MLP) is utilised. It is composed of an input layer, an output layer, and one or more hidden layers. The two hidden layers have between 100 and 200 neutrons, which are used to gauge how accurate the ANN model is. Firstly, in order to train the ANN model, we gather 65,000 data records. Of the 65,000 data records, 80% are the training data, while the remaining 13,000 are the validation data. With 120 and 140 neutrons at the first and second hidden layers, respectively, the trained model's accuracy may be roughly estimated at 82%. Given the benefits of performance and computing complexity (Hinton and Salakhutdinov, 2006), the ANN model uses 120 and 140 neutrons at the first and second hidden layers, respectively.

Results and Discussions

By altering the data rate of every source-to-destination pair, the suggested AIER mechanism's performance is contrasted with that of static and dynamic routing techniques. The average throughput, packet loss ratio, and packet latency for various monitoring intervals (3, 5, or 10s) are examples of performance metrics. The simulation results show the efficiency and superiority of the AIER mechanism.

The average throughput of each flow is shown against the data rate for various monitoring intervals in Figure 3. Out of the three systems, static routing has the lowest average throughput and decreases with increasing data flow, irrespective of the monitoring interval. This situation arises from the fact that the shortest path selection forces all data flows to send their data over the same way.

When a predetermined congestion condition arises, dynamic routing, as opposed to static routing, has the ability to periodically switch transmission channels. Unlike the AIER method, when data rate is raised, the average throughput with dynamic routing does not rise since packet loss happens before path reconfiguration is finished.

Stated differently, the length of the monitoring period has little effect on the AIER process. Additionally, because the AIER method can execute more appropriate path construction as quickly as feasible, it has a lower path reconfiguration frequency than dynamic routing. Therefore, when it comes to average throughput, the AIER method outperforms both static and dynamic routing. Packet delay vs data rate for various monitoring intervals is seen in Figure 4.As with the previous explanation, the AIER mechanism performs better in terms of packet latency than the other two routing systems, especially during periods of high network traffic. This is due to the AIER mechanism's ability to forecast optimal routes for every flow based on historical data.

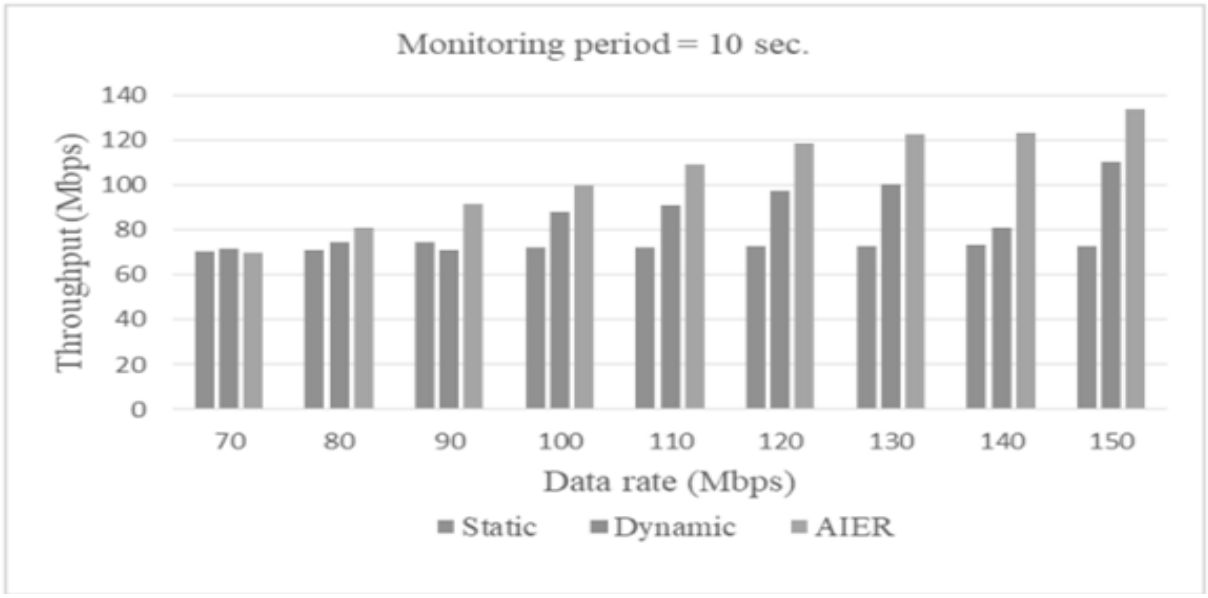

Figure 3: Average flow throughput vs. data rate for different monitoring periods. (a)

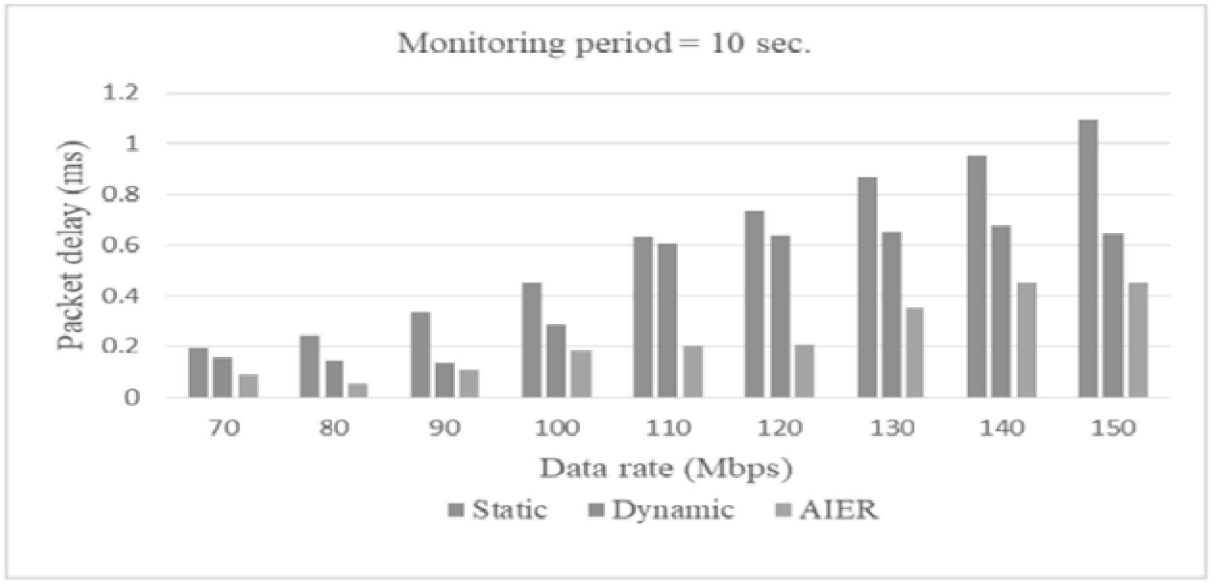

Figure 4: Packet delay vs. data rate for different monitoring periods

Figure 5 shows the packet loss ratio vs data rate for various monitoring periods in relation to packet loss performance. As the data rate rises, the packet loss ratio also rises. Since each link has a 250 Mbps capacity, when a flow's data throughput reaches about 70 Mbps, the shortest path selection leads to severe single-link stress and packet loss. On the other hand, dynamic routing has the ability to periodically modify path allocation to ease

congestion on the shortest way. Because of this, it has a lower packet loss ratio than static routing. Remarkably, Figure 5 shows that until each flow's data rate reaches 120 Mbps, almost no packet loss is seen when using the AIER technique.As a result, the AIER mechanism's intelligent path selection design with congestion avoidance shows a notable reduction in packet loss.

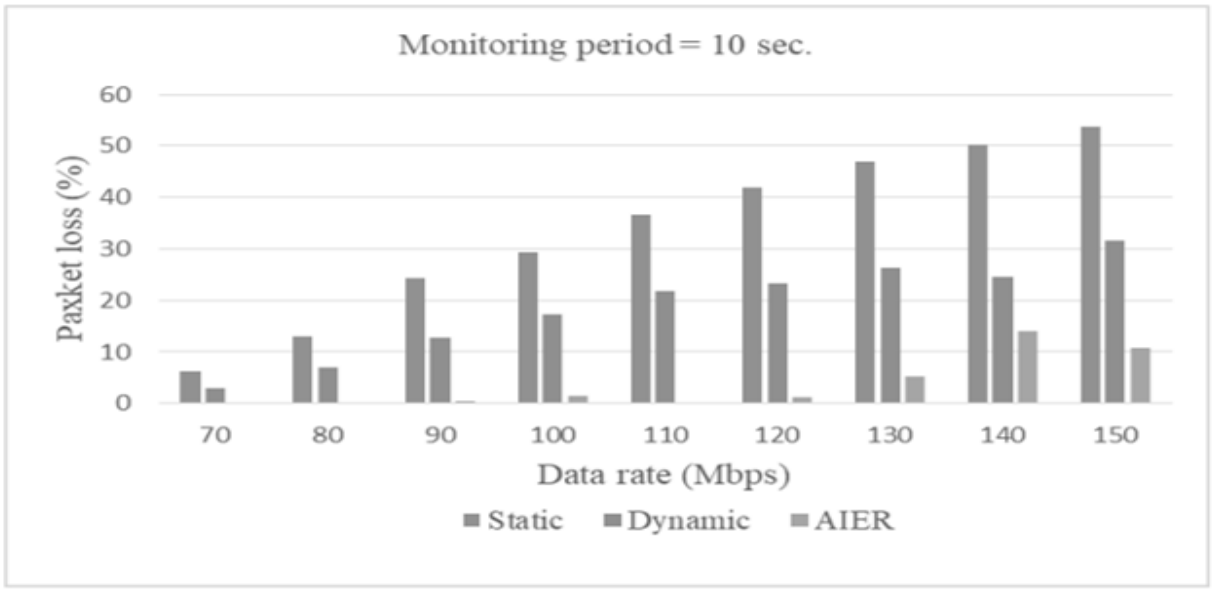

Figure 5: Packet loss ratio vs. data rate for different monitoring periods

Conclusion

This paper effectively implements an artificial neural network (ANN) for intelligent path selection with congestion avoidance in the SDN control plane. By using AI technology, the suggested AIER mechanism may not only lessen the effects of monitoring periods with dynamic routing but also offer the capacity to learn from previous experiences. Three steps make up the AIER mechanism: (1) gathering a sufficient amount of training data, (2) creating an ANN model in the control plane using the training data, and (3) using the ANN model to choose a path. The controller may execute a more appropriate path design based on the present data flow traffic and link load once the ANN model has been trained.We illustrate the superiority and efficacy of our suggested AIER mechanism through simulations using the Mininet simulator. According to the simulation findings, the average throughput, packet latency, and packet loss ratio demonstrate a significant advantage of the AIER mechanism over static and dynamic routing strategies. To

improve the comprehensiveness of the ANN model, in further works, we will propose an intelligent routing strategy that treats link breakdown between any two OpenFlow switches as feature data, apart from data flow traffic and link load.

References

Abbas N., Nasser Y., & Ahmad K., (2015) Recent advances on artificial intelligence and learning techniques in cognitive radio networks, EURASIP J. Wirel. Commun. Netw. 2015 (1) (2015) 174–182.

Ahmad I., Kumar T., Liyanage M., Okwuibe J., Ylianttila M., &Gurtov A., (2018) Overview of 5G security challenges and solutions. IEEE Commun Stand Mag. 2018;2(1):36-43.

AraboA.,&Pranggono B., (2013) Mobile malware and smart device security: trends, challenges and solutions. Control Systems and Computer Science (CSCS), 2013 19th International Conference on (pp. 526–531). IEEE.

Arjoune Y., Salahdine F., Islam S., Ghribi E., Kaabouch N., (2020) A novel jamming attacks detection approach based on machine learning for wireless communication. arXiv. 2020.

Cayamcela M., &Lim W., (2018) Artificial Intelligence in 5G Technology: A Survey. IEEE Access.,pp,1-6.

Flo A.,&Josang A., (2009) Consequences of botnets spreading to mobile devices. Short-Paper Proceedings of the 14th Nordic Conference on Secure IT Systems (NordSec 2009) (pp. 37–43).

Forsberg D., Leping H., Tsuyoshi K. &Alanara S., (2007) Enhancing security and privacy in 3GPP E- UTRAN radio interface. Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on (pp. 1–5). IEEE.

Hinton G., &Salakhutdinov R., (2006) Reducing the dimensionality of data with neural networks. Science 2006, 313, 504–507.

Iperf. (2020) Available online: https://iperf.fr/ (accessed on 8 May 2020)

Khan S., Bagiwa M., Wahab A., Gani A., & Abdelaziz A., (2020) Understanding link fabrication attack in software defined network using formal methods. In Proceedings of the IEEE International Conference on Informatics, IoT, and Enabling Technologies, Doha, Qatar, 2–5 February 2020; pp. 555–562

Kozo S., Eiji T., Takeo O., Takayuki S., Daisuke O., Kosei K., & TutomuM., (2020) Passive Method for Estimating Available Throughput forAutonomous Off-Peak Data Transfer. *Hindawi Wireless Communications and Mobile Computing*, Volume 2020, Article ID 3502394, 12 pages. https://doi.org/10.1155/2020/350239.

Lai C., Lu R., Zheng D.,& Shen X., (2020) Security and privacy challenges in 5G-enabled vehicular networks. IEEE Netw. 2020;34(2):37-45.

Lee J., Tejedor E., Ranta-Aho K., Wang H., Lee K., Semaan E., Mohyeldin E., Song J., Bergljung C.,& Jung S., (2018). Spectrum for 5G: Global Status, Challenges, and Enabling Technologies. IEEE Communications Magazine, 56(3), pp.12–18.

Liu J., Zhang S., Sun W., &Shi Y., (2017) In-vehicle network attacks and countermeasures: challenges and future directions. IEEE Netw2017;31(5):50-58.

Liu J., Zhao H., & Zhou R., (2016) Exploration of high-precision adaptive wavelet neural network artificial intelligence method, Comput. Sci. 10 (8) (2016) 1122–1132.

Liu X., (2023) Design of Wireless Communication Base Station Monitoring System Based on Artificial Intelligence and Network Security. Procedia Computer Science 228 (2023) 1254–1261 Big Data Analytics for IoT Security and Privacy 10.1016/j.procs.2023.11.097

Liyanage M., Ahmad I., &Abro A., (2018). A Comprehensive Guide to 5G Security, 231–243. Wiley https://www.researchgate.net/publication/322466640_ Software_Defined_Security_Monitoring_in_5G_Networks.

Mantas G., Komninos N., Rodriguez J., Logota E., & Marques H., (2015) Security for 5G Communications.John Wiley & Sons, Ltd. Published 2015 by John Wiley & Sons, Ltd Pp 207-220

Mijumbi R., Serrat J., Gorricho J., Latré S., Charalambides M., &Lopez D., (2016) Management and orchestration challenges in network functions virtualization. IEEE Commun Mag. 2016;54(1):98-105.

Minea M., Dumitrescu C., & Minea V., (2021) Intelligent Network Applications Monitoring and Diagnosis Employing Software Sensing and Machine Learning Solutions. Sensors 2021, 21, 5036. https://doi.org/10.3390/s21155036

Piqueras R., (2013) Security attacks against the availability of LTE mobility networks: Overview and research directions. Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on (pp. 1–9). IEEE.

Salahdine F., (2018) Compressive spectrum sensing for cognitive radio networks. arXiv Preprint arXiv:1802.03674, 2018.

Seddigh N., Nandy B., Makkar R.,& Beaumont, J., (2010) Security advances and challenges in 4G wireless networks. Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on (pp. 62– 71). IEEE.

Tran T., Hajisami A., Pandey P., &Pompili D., (2017) Collaborative mobile edge computing in 5G networks: new paradigms, scenarios, and challenges. IEEE Commun Mag. 2017;55(4):54-61.

Wang H., Zheng T., Yuan J., Towsley D., &Lee M., (2019) Physical layer security in heterogeneous cellular networks. IEEE Trans Commun. 2016;64(3):1204-1219.

Wu P., Li G., & Zhu H., (2015) Event boundary detection method based on wireless sensor network and linear neural network, Pattern Recognit. Artif. Intell. 28 (4) (2015) 377–384

Wu Y., Hwang P., Hwang W., & Cheng M., (2020) Artificial Intelligence Enabled Routing in Software Defined Networking. Appl. Sci. 2020, 10, 6564; doi:10.3390/app10186564

Yang W., & Fung C., (2016) A survey on security in network functions virtualization. Paper presented at: 2016 IEEE NetSoft Conference and Workshops (NetSoft); 2016;15-19; IEEE.

Zidek M., (2023) AI in the Network Monitoring. International Journal of Computer Science and Information Technology Research. Vol. 11, Issue 3, pp: (60-64), Month: July - September 2023

Zhou J., (2020) Artificial intelligence driven wireless network remote monitoring based on Diffie–Hellman parameter method. Computer Communications 160 (2020) 132–138 https://doi.org/10.1016/j.comcom.2020.05.047

Zhou Y., Yang Z., Sun Q., Yu C., & Yu C., (2023) An artificial intelligence model based on multi-step feature engineering and deep attention network for optical network performance monitoring. Optik - International Journal for Light and Electron Optics 273 (2023) 170443 https://doi.org/10.1016/j.ijleo.2022.170443