INTERNATIONAL JOURNAL OF INTEGRATED ENGINEERING
ISSN: 2229-838X e-ISSN: 2600-7916

IJIE

Vol. 17 No. 2 (2025) 126-139
https://publisher.uthm.edu.my/ojs/index.php/ijie

Fitting Distribution Modeling and Traffic Policing on Real Live Metro-E Network Data

Nor Paezah Abdullah[1,4], Murizah Kassim[1,2]*, Sayang Mohd Deni[3]

[1] *School of Electrical Engineering, College of Engineering, Universiti Teknologi MARA, Shah Alam, 40450, Selangor, MALAYSIA*
[2] *Institute for Big Data Analytics and Artificial Intelligence (IBDAAI), Universiti Teknologi MARA, Shah Alam, 40450, Selangor, MALAYSIA*
[3] *College of Computing, Informatics and Media Studies, Kompleks Al-Khawarizmi, Universiti Teknologi MARA, Shah Alam, 40450, Selangor, MALAYSIA*
[4] *Institut Kemahiran Tinggi PERDA (PERDA-TECH), Nibong Tebal, 14300, Pulau Pinang, MALAYSIA*

*Corresponding Author: murizah@uitm.edu.my
DOI: https://doi.org/10.30880/ijie.2025.17.02.010

Article Info

Received: 14 August 2024
Accepted: 13 July 2025
Available online: 28 July 2025

Keywords

Internet traffic, distribution model, WAN Metro-E, policing, log-normal

Abstract

This paper presents a traffic characterization and statistical analysis of WAN Metro-E campus network internet traffic, addressing network congestion and delay issues. The increase in internet usage on campus can lead to various challenges, including traffic bursts that can impact the quality of service (QoS) experienced by users. The method involves traffic characterization and traffic policing on the Metro-E 50Mbps campus network using Python. The analysis will define the distribution model and policing the network of real-time internet traffic data where real live data at 50Mbps/6.5MB present burst traffic. The best-fitted model is the log-normal distribution model, which has the highest MLE score of -2726. Policing on inbound bytes before and after with a threshold of 50Mbps/6.5MB was done and a total of 3422404.81MB buckets were created and a total of 219273.88MB buckets after policing with a reduced percentage at 99.36%. Comparing actual traffic under three different policing scenarios compared to P1 and P2, policing on P3 has the highest traffic filtering at 3197986.21MB and the largest number of bytes filled in the bucket with a reduced percentage to 90.66%. This research is significant for Wan Metro-E Network's future QoS bandwidth management control mechanisms and optimization of network traffic performance.

1. Introduction

Performance of the network traffic must be constant, therefore evaluation on traffic models and parameters should be defined to quantify the model is in optimum approach by implementing a well-defined evaluation process and optimizing the network based on traffic models and parameters. Furthermore, it can significantly improve the consistency and reliability of internet traffic performance[1]. Internet traffic flow models are developed using traffic analysis and modeling, which analyses past network traffic data. These models might consider things like peak usage periods, the kinds of apps that drive traffic, and the communication patterns between different areas of the campus network. Although many traffic models have been put forth over the years, there aren't enough of them that can be used to adequately model traffic in networks. The development of new applications and network technology has significantly transformed the Internet traffic model throughout the years[2]. The distribution model of real-time internet traffic was established using the statistical analysis

techniques of Maximum Likelihood Estimate (MLE) and Goodness of Fit (GoF)[3]. The distribution of internet traffic is modeled using the cumulative distribution function (CDF) model equation. By changing the value of the shape parameter, which is based on the estimated parameter from the generated distribution model, the network burst can be controlled. The Anderson-Darling (AD) test and maximum likelihood estimation (MLE) are two examples of statistical models of probability distributions and estimate parameters that are used to estimate the behavior of the data population. The quality of service (QoS) of online applications must be ensured in terms of delay, bandwidth, jitter, dependability, or a combination of these criteria, given the rapid growth of internet applications[4].

Network traffic policing is a crucial aspect of managing and maintaining the quality of service in computer networks. It involves the control and regulation of incoming and outgoing data traffic to ensure that the network's resources are used efficiently and fairly. Policing mechanisms are used to enforce traffic limits, prioritize traffic, and prevent network congestion[5]. Monitoring network traffic for compliance with a traffic contract and dropping any extra traffic is the process of traffic policing. The primary goal is to prevent network congestion, ensure fair resource allocation, and maintain the quality of service for all network users. The token bucket mechanism is a widely used approach to regulate incoming network traffic by controlling the rate at which packets are allowed to be transmitted[6]. A new algorithm for traffic shaping and policing uses the token bucket technique to reduce congestion. A token bucket algorithm controls the rate at which incoming packets are allowed to be transmitted. The algorithm should grant tokens at a predetermined rate and consume tokens for each transmitted packet. Implement the token bucket mechanism to enforce traffic rate limits on incoming packets[7]. Packets that arrive without sufficient tokens should be either delayed or dropped, depending on the system's configuration.

1.1 WAN Metro-E Campus Network Architecture

Metro-Ethernet is a form of Ethernet technology that provides high-speed connectivity and scalability and is designed for usage in metropolitan areas[8]. The campus network typically refers to the local network within a specific geographical area, such as a university campus or a corporate campus[9]. A Wide Area Network Metro-Ethernet (WAN Metro-E) Campus Network refers to a network architecture that combines the features of a metropolitan Ethernet network (Metro-E) to provide seamless connectivity, high-speed, and reliable network infrastructure that facilitates communication and collaboration among geographically distributed locations within a campus area. The design should address performance, security, redundancy, and manageability to meet the organization's connectivity requirements. Fig. 1 shows the network architecture diagram for the WAN Metro-E campus network.

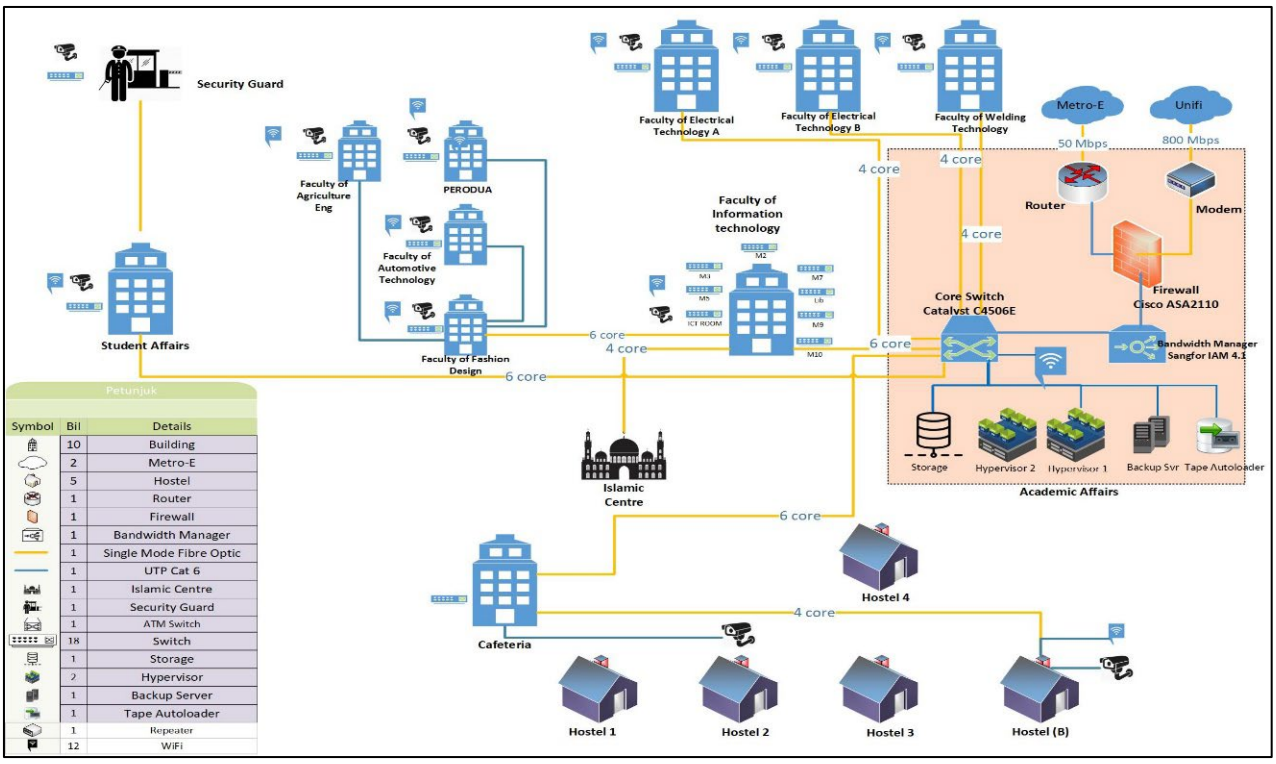

Fig. 1 *WAN Metro-E Campus network diagram*

Metro-Ethernet services, involve providing dedicated Ethernet connections between multiple locations and the providers usually have a network infrastructure with Fiber-optic cables, switches, and routers that span the metropolitan area. Metro-Ethernet networks (MEN) can be configured with Quality of Service (QoS) settings to prioritize certain types of traffic over others[10]. This ensures that critical applications receive the necessary bandwidth and low latency.

1.2 Internet Traffic Distribution Model

Mathematical representations of the patterns and behaviors of data flow within computer networks are called Internet traffic distribution models. These models provide insight into data transmission, resource allocation, and network performance enhancement. Many different distribution models are frequently employed to describe internet traffic. The Internet traffic models are developed using traffic analysis and modeling, which analyses past network traffic data[11]. These models might consider things like peak usage periods, the kinds of apps that drive traffic, and the communication patterns between different areas of the campus. The parameters of the defined models must be connected to the real performance indicators that are to be forecasted from the traffic model[12]. Several distribution models have been identified to model the internet traffic statistics, several distribution models have been identified.

The most popular and influential distribution model in statistics is the normal distribution model. As the curve resembles a bell, it is also sometimes referred to as the "Bell Curve." The "Gaussian curve" is another name for it, given to it by mathematician Karl Friedrich Gauss[13]. Internet traffic behavior is frequently described using the Pareto distribution, sometimes known as a power-law distribution. The distribution shows most of the entire amount of data is accounted for by a limited number of events (high-data traffic flows)[14]. Meanwhile, a data stream's inter-arrival periods are frequently modeled using the exponential distribution and it’s very helpful for comprehending how rapidly packets are sent through the network because it assumes that the rate of packet arrivals is constant[15]. The log-normal distribution is applied when the logarithms of the data values follow a normal distribution. The distribution can be used to model a wide range of phenomena, including internet traffic, where the underlying factors causing variation are multiplicative in nature[16]. Besides, the gamma distribution also known as Pearson Type III distribution is often used to model data that represents waiting times or durations and can be applied to internet traffic modeling when considering the time taken for specific operations to occur[17]. Other than that, the Weibull distribution is used to describe data where the rate of occurrence of an event changes over time[18]. The distribution is useful for modeling the behavior of internet traffic when the frequency of certain types of events varies. Extreme traffic loads can lead to network congestion, by using the Gumbel distribution, the distribution of extreme congestion levels will be analyzed to design more robust congestion control mechanisms[19]. Gumbel distribution is used to model extreme traffic loads or the maximum demand on network resources during peak times.

1.3 QoS Bandwidth Management

Congestion occurs when network resources are overwhelmed with traffic. QoS mechanisms detect and mitigate congestion by dropping or marking packets based on their priority, helping to maintain optimal performance[20]. A mechanism called quality of services (QoS) is used to control network traffic and guarantee the network's performance. QoS is particularly crucial in scenarios where network resources are limited or shared among various applications and services[21]. It ensures that high-priority traffic receives the necessary resources, and that lower-priority traffic doesn't hinder critical communications. It's used in various types of networks, including local area networks (LANs), wide area networks (WANs), data centers, and even in the context of cloud services. High-speed Ethernet connectivity is made possible by metro-E networks, and QoS is essential for maximizing performance, reducing latency, and guaranteeing dependable service delivery[22]. The dependable and effective transport of data across networks is a key component of network optimization, especially in situations where bandwidth is constrained or shared[23]. QoS bandwidth management addresses these issues and seeks to prioritize and distribute network resources to various types of traffic according to their unique needs and relevance[24]. As technology evolves and network demands grow, QoS continues to be a vital tool in maintaining a reliable and efficient network infrastructure especially, in supporting real-time applications, optimizing cloud services, and ensuring a consistent user experience across various network environments.

1.4 Internet Traffic Policing

Traffic policing is a QoS mechanism used to manage and control internet traffic by enforcing predefined traffic rate limits. It ensures that network resources are fairly shared among different users or applications and prevents any single user or application from overwhelming the network with excessive data[25]. Policing helps maintain network stability and provides a level playing field for all users. The network's policies keep an eye on how many tokens are in the bucket. One token often corresponds to one byte of traffic in traffic policing. Both incoming and

outgoing traffic can be managed by it and keeps the extra traffic under control. The token bucket is a widely used traffic policing mechanism. It operates by allowing packets to be transmitted only if there are sufficient tokens in the token bucket[26]. The allowed average traffic rate is represented by the fixed rate at which tokens are added to the bucket and if there are enough tokens in the bucket when a packet arrives, it is let to pass, and the necessary quantity of tokens is used. The packet is dropped or flagged if there are not enough tokens. Setting up a queue with a token pool is a necessary step in traffic policing. Assume that a token is used for some traffic unit, such as a packet that is received. The token is returned to the pool after each transmission of a packet. Short bursts in the traffic stream will be permitted if the pool is sized properly, but if the application tries to start a session utilizing more bandwidth than the policer permits, the packets will be dropped[27]. Committed Information Rate (CIR) is the guaranteed rate at which traffic is allowed to flow. Traffic exceeding the CIR can be dropped or marked. CIR is commonly used in conjunction with token bucket policing to ensure that a certain level of bandwidth is reserved for specific classes of traffic[28].

2. Research Method

The methodology and resources utilized for the analysis are described in this section. And provided an in-depth overview of the methodology employed for analysis, the resources utilized, and how the desired outcomes were represented through a flowchart and various activities.

2.1 Research Framework

The research flowchart outlines the systematic approach to analyzing and defining a distribution model for policing real-time internet traffic on a WAN Metro-E 50Mbps campus network. The aim is to ensure effective management of real-time traffic while maintaining the desired quality of service and network performance. Planning has been made for a research platform that will analyze traffic performance. The research framework is shown in Fig. 2, which also includes the stages for data collecting, data analysis and distribution modeling, internet traffic policing, and documentation.

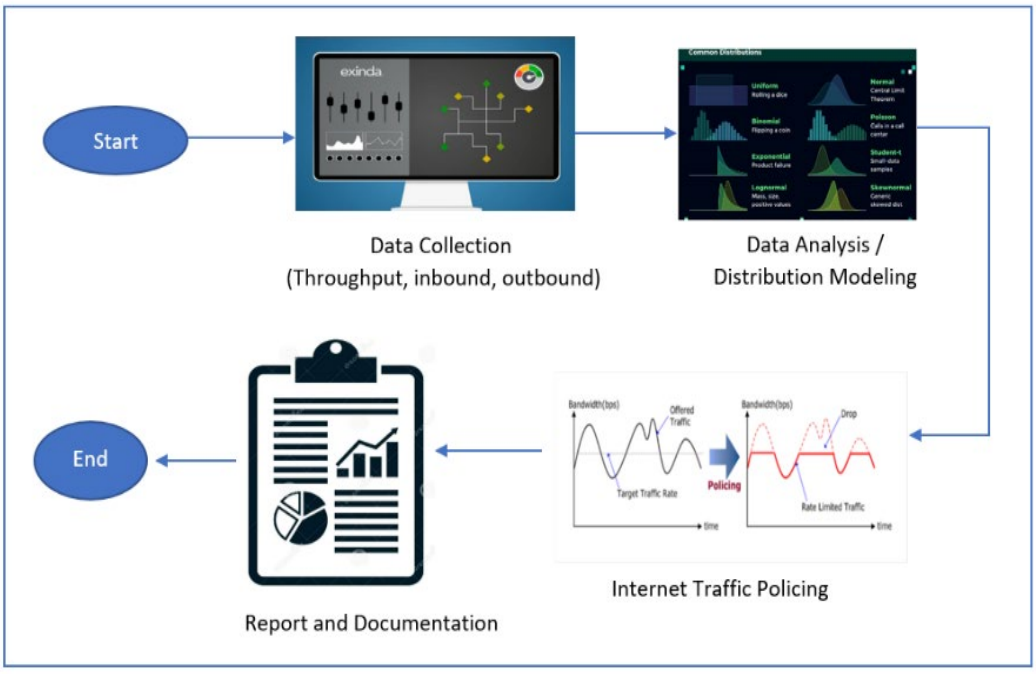

Fig. 2 *Research framework*

2.2 Activities Flow

A research flowchart has been planned that takes action to analyze and define the distribution model and policing the network of real-time internet traffic on the WAN Metro-E 50Mbps. Fig. 3 presents the flowchart of the activities of this research from the beginning until the end.

Int. Journal of Integrated Engineering Vol. 17 No. 2 (2025) p. 126-139

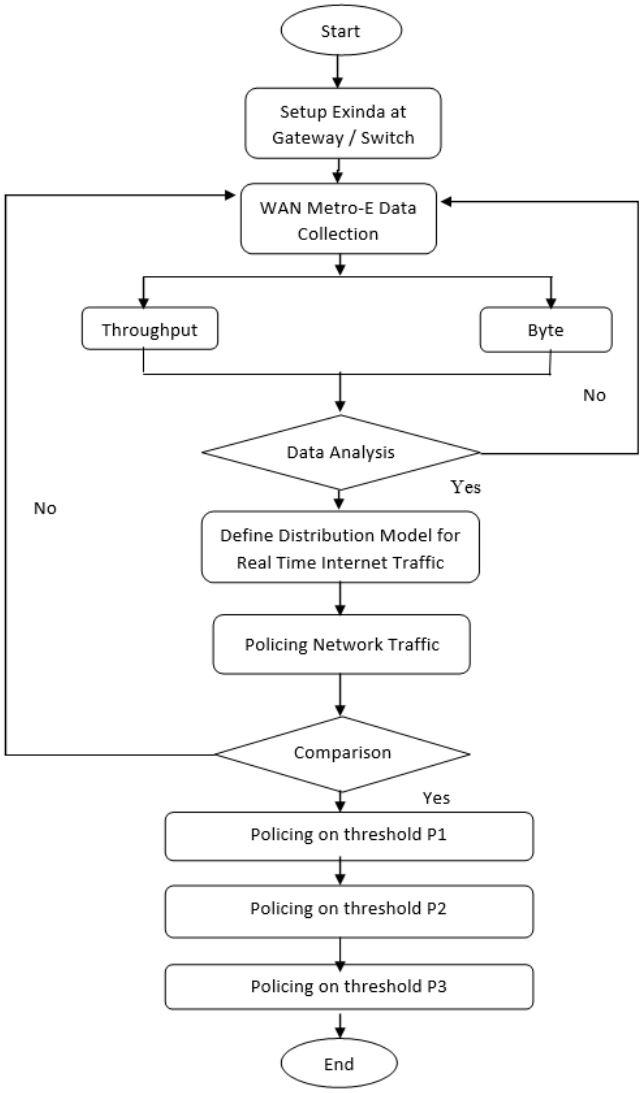

Fig. 3 *Activities flow*

The traffic modeling and internet traffic policing on the WAN Metro-E campus network will be described using a statistical analytic method based on the Python language and distribution model. A gateway switch is equipped with a network monitoring tool called Exinda Network Orchestrator to collect data. Every 10 seconds between arrival times, throughput and packet data on WAN internet traffic will be gathered at the 50Mbps Metro-E campus network and merged into 1 hour each month. Data on internet traffic was gathered for a full year, from August 1 to August 31, 2021–2022.

2.3 Exinda Monitoring Tools

Exinda is a network management and monitoring tool that focuses on optimizing network performance, ensuring Quality of Service (QoS), and enhancing the user experience. Exinda keeps track of performance indicators for applications like latency, packet loss, and response times. The data aids in identifying performance problems and enhancing application delivery. Exinda provides real-time monitoring capabilities with the ability to observe network traffic and performance data as they occur, allowing for the quick identification and correction of problems. Fig.4 shows the Exinda Networks Orchestrator for WAN monitoring and provides application throughput for both inbound and outbound traffic, as well as a list of the top applications in terms of bandwidth utilization. The network monitoring dashboard monitors and manages network traffic, optimizes bandwidth, and ensures that key applications run efficiently.

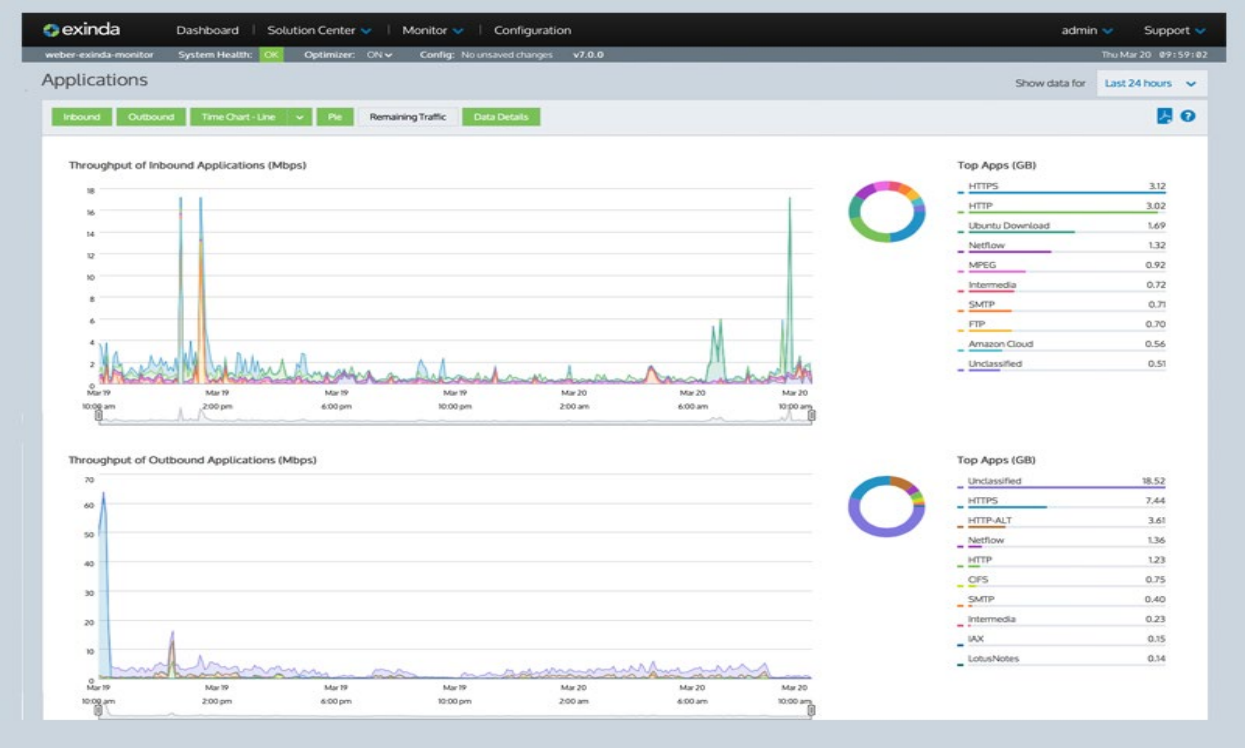

Fig. 4 *Exinda network orchestrator*

2.4 Fitted Distribution and Traffic Policing

The Metro-E Network's campus based in Penang is where the real-time internet traffic data is gathered. The internet traffic will be evaluated using a statistical analysis method. Fig. 5 shows the way analysis will be done and to choose the best analytical model, measurement data is analyzed. Before choosing which statistical distribution can be modeled, the analysis process will proceed through a few steps. The study will focus on a few fitted distribution models, including the Normal, Lognormal, Weibull, Pareto, Pearson Type III, Gumbel, and Exponential models. The distribution model of real-time internet traffic was established using the statistical analysis techniques of Maximum Likelihood Estimate (MLE) and Goodness of Fit (GoF). The distribution of internet traffic is modeled using the cumulative distribution function (CDF) model equation by changing the value of the shape parameter, which is based on the estimated parameter from the generated distribution model, network burst can be controlled. A new traffic policing system uses a token bucket technique to reduce congestion.

Int. Journal of Integrated Engineering Vol. 17 No. 2 (2025) p. 126-139

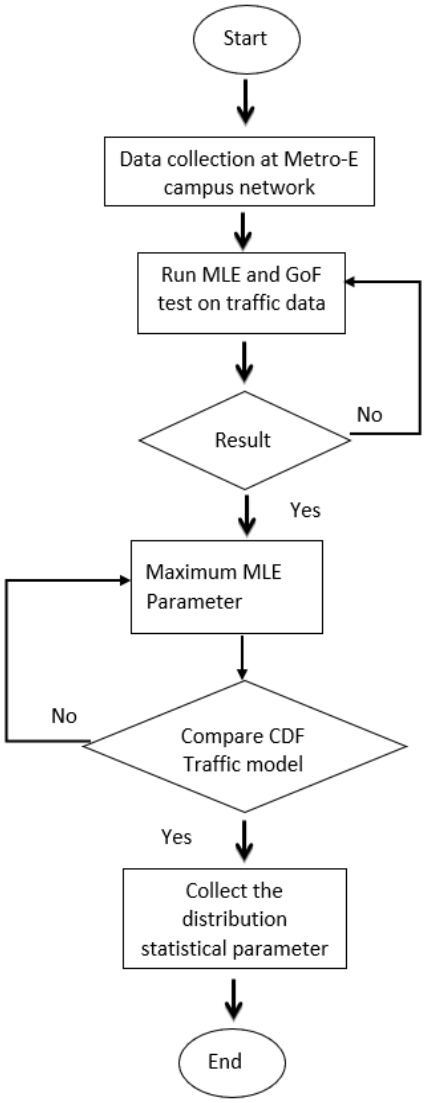

Fig. 5 *Traffic distribution modeling analysis*

The network traffic data has been analyzed, then the process of controlling the congestion must take over before the data can be transmitted to the network. Traffic policing is one strategy for network congestion traffic control. ISPs frequently employ traffic policing to lower customer traffic rates. A well-tuned traffic policer is thought to provide TCP with satisfactory performance for a very long time. The token bucket technique is used in this process for policing by moving the data, the token bucket concept helps to realize bandwidth utilization.

3. Results and Discussion

3.1 Fitted Distribution Model of Network Traffic

Fitting a distribution model to network traffic data involves selecting a probability distribution that closely matches the observed data's characteristics. It can help in understanding the underlying patterns, making predictions, and making informed decisions about network resource allocation, capacity planning, and performance optimization. The chosen distribution models such as Normal, Log Normal, Weibull, Pareto, Pearson Type III, Gumbel, and Exponential are fitted to the observed data using maximum likelihood estimation. Table 1 shows the parameter and the maximum likelihood estimator value for the selected distribution model. Log Normal distribution model has the maximum MLE value at -2726 point.

Table 1 *Parameter and Maximum Likelihood Estimator value*

Distribution Model	σ	β	μ	η	α	Xm	δ	MLE
Normal	707752748		34790621					-421219
Log-Normal	28089547912		3840393047					-2726
Weibull		1.0		99701767345				-1524572
Pareto					0.15	777		-1195681
Pearson Type III		230780703					26972523	-19228
Gumbel		513450018	339184358					-15444
Exponential	2.18		2.18					-13771

The real throughput traffic flow is examined before being characterized and to simulate the new Policing method, specific parameters are identified. The Metro-E campus network's statistical analysis of throughput flow and the optimal traffic distribution model is assessed. The best-fitted distribution throughput is examined using the Maximum Likelihood Estimator (MLE) approach. The Cumulative Distribution Function (CDF) and graph for actual traffic are shown. Fig. 6 displays the fitted distribution model for real data CDF, showcasing the accuracy of the model concerning actual traffic. Meanwhile, Fig. 7 represents the fitted distribution model specifically tailored for the Metro-E 50Mbps campus network. The comparison of several statistical models, including distributions such as Weibull, Pareto, Lognormal, Exponential, Gumbel, and others, reflects an attempt to determine the best fit for the actual internet traffic data obtained. This method is commonly used in research for internet traffic modeling, where various distributions are utilized to study traffic behavior, particularly throughput, latency, and packet loss. The log-normal distribution model is the best-fitted model based on a thorough analysis to represent the throughput traffic on the Metro-E campus network.

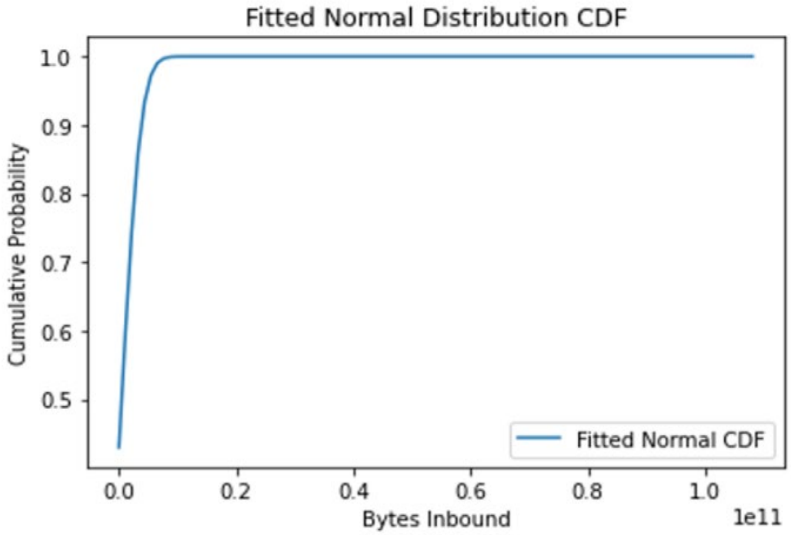

Fig. 6 *Fitted distribution model real live data CDF*

Int. Journal of Integrated Engineering Vol. 17 No. 2 (2025) p. 126-139

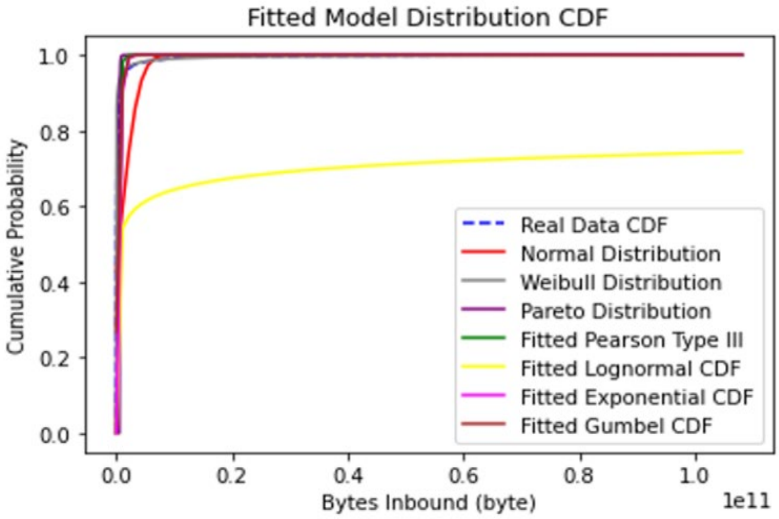

Fig. 7 *Fitted CDF distribution model*

The log-normal distribution model was shown to be the most accurate depiction of the throughput traffic flow on the Metro-E campus network through research and modeling using the Maximum Likelihood Estimator. These are essential for understanding the behavior of the network, putting in place efficient policing techniques, and guaranteeing optimal bandwidth management for the campus network.

3.2 Bucket Capacity with Traffic Policing

The token bucket algorithm, which is frequently used for traffic policing to make sure that incoming network traffic complies with established rate limitations and quality of service regulations, has bucket capacity as a core parameter. Throughput is identified as bytes flows captured and the token bucket theory mechanism for Policing the internet traffic is applied. Real live traffic data on the Metro-E Campus network with the maximum throughput allowed is the value of its threshold, which is 50Mbps/6.5MB, and maximum inbound Bytes at 108,000MB in Fig. 8. Real live data present burst traffic. The detailed router's configuration is identified in the Metro-E campus network where there is no Policing setup done at the main router configuration. This means that all inbound and outbound traffic to the internet passes out and into the internet without any Policing control.

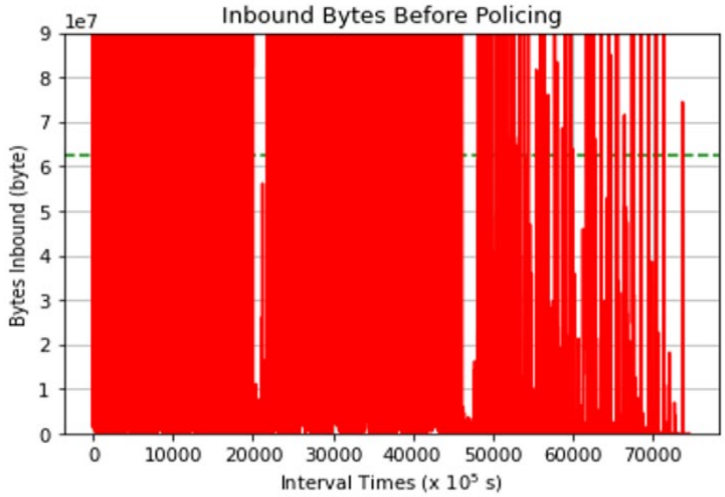

Fig. 8 *Inbound bytes before policing*

Fig. 9 shows inbound bytes before and after policing with a threshold of 50Mbps/6.5MB. The green lines in the graph present the Policing threshold. A total of 3422404.81MB buckets are created for each trace at each 10-second inter-arrival time of inbound throughput traffic collected in a year. A total of 219273.88MB buckets after policing were created with a reduced percentage of 99.36%.

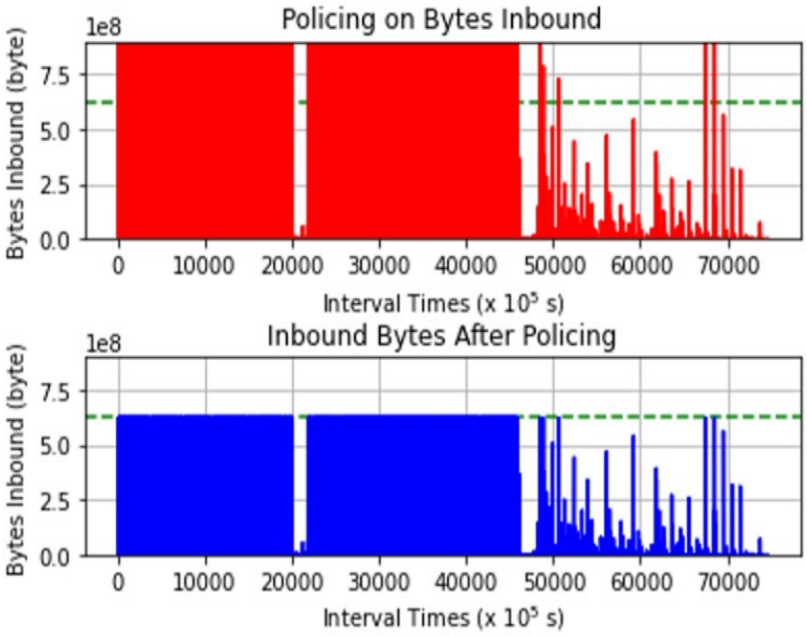

Fig. 9 *Traffic policing at threshold 50Mbps*

Meanwhile, Table 2 presents three different thresholds before Policing Filtered (PF) which threshold at P1(229250000Byte), P2(152833333.33Byte), and P3(305666666.66Byte), the bucket capacity before and after policing and the reduced percentage. The total bucket capacity (before and after) shows the total quantity of data that may be accommodated, whereas the threshold denotes the highest permitted rate of data flow and after applying the policing thresholds, the reduction % shows how much the overall bucket capacity was decreased.

Table 2 *Bucket capacity with traffic policing*

Policing	Threshold (Byte)	Total Bucket Capacity (Before) (Byte)	Total Bucket Capacity (After) (Byte)	Reduce Percentage
P1	229250000	34224048069237.0	2386251744658.0	93.03%
P2	152833333.33	34224048069237.0	1421112776385.0	95.85%
P3	305666666.66	34224048069237.0	3197986214357.0	90.66%

Fig. 9, Fig. 10, and Fig. 11 derive the Policing on three different thresholds. The graph shows the difference in throughput on the Policing condition of P1, P2, and P3 of mean value from maximum inbound bytes. The plotted graphs show the minimum and maximum values of throughput bytes after Policing. The minimum values are all equally the same as in the result before Policing. The difference between all the graphs is the bytes allowed in the bucket and the cut-off bytes after being filtered. The advantage of the algorithm is the processing performance which relates to the time of transfer and control mechanism if there is a peak time for a priority task. The total minimum and maximum bucket capacity is much larger compared to daily traffic because longer time internet collected traffic is simulated.

Int. Journal of Integrated Engineering Vol. 17 No. 2 (2025) p. 126-139

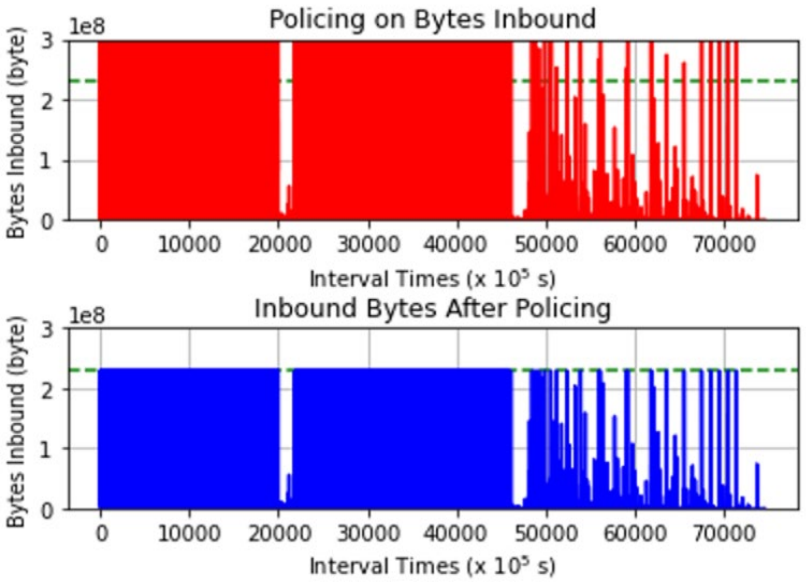

Fig. 10 *Traffic policing at P1*

The maximum permitted rate of data flow is represented by the threshold value of 229,250,000 Bytes. Fig. 10 shows before any modifications, the total bucket capacity was 34,224,048,069,237 Bytes. The entire bucket capacity was reduced to 2,386,251,744,658 Bytes after applying the policing threshold. Due to the 93.03% decrease in bucket capacity, the network's ability to handle data traffic above the set threshold has significantly decreased.

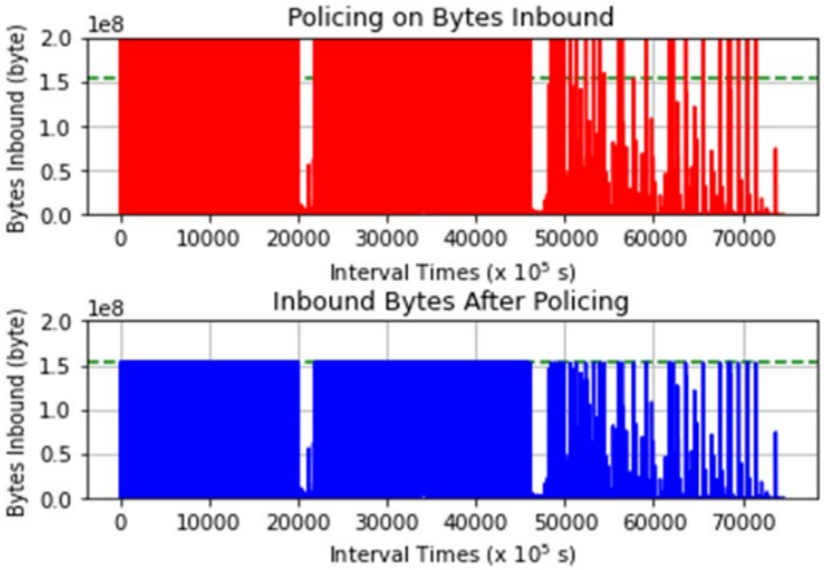

Fig. 11 *Traffic policing at P2*

A threshold of 152,833,333.33 Bytes was chosen for the data flow in Policing P2. 34,224,048,069,237 Bytes in Fig. 11 were available in the bucket's total capacity before the threshold's implementation. The overall bucket capacity reduced significantly to 1,421,112,776,385 Bytes following the implementation of the policing measures. The capacity of the network to handle data traffic over the stated threshold is significantly decreased by 95.85% as a result of this reduction. Meanwhile, Fig. 12 shows the threshold at 305,666,666.66 Bytes significantly reduced the total bucket capacity from 34,224,048,069,237 Bytes to 3,197,986,214,357 Bytes. This reduction represents a 90.66% decrease in the network's capacity to handle data traffic above the specified threshold, ensuring more controlled and efficient data flow within the network.

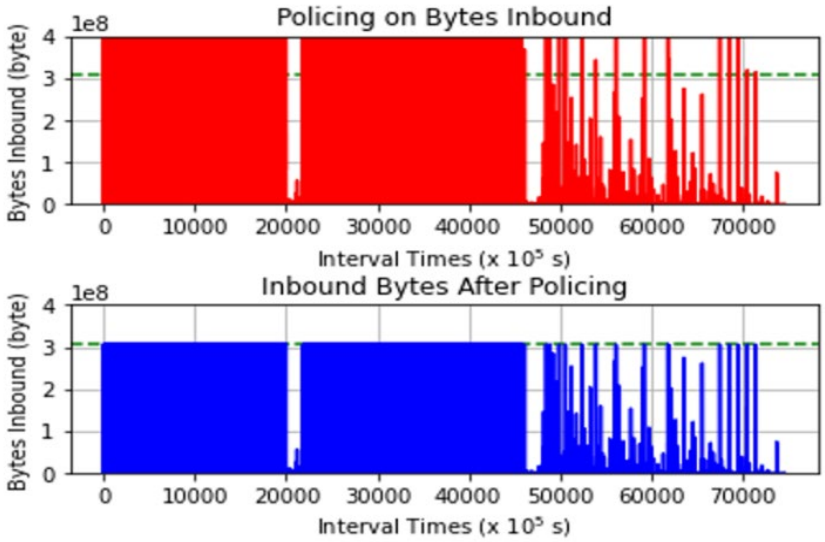

Fig. 12 *Traffic policing at P3*

Real traffic without Policing with the other three policing conditions is compared. Policing on P3 is the highest filtered traffic which presented the smallest bytes filled in the bucket compared to P1 and P2. P3 has the highest bytes filled in the bucket because it has the lowest filtered condition that presents the burst traffic controlled. The traffic management strategies can be implemented effectively. The network's overall bucket capacity was substantially reduced by establishing certain data flow thresholds, which significantly decreased the network's capacity to process data traffic above the predetermined limitations. These steps are necessary to guarantee network stability, avoid congestion, and maintain effective data flow within predetermined limits. The substantial reduction rates of 93.03% in P1, 95.85% in P2, and 90.66% in P3 emphasize the successful implementation of these policing strategies, improving the network's overall performance and dependability.

4. Conclusion

The analyzed traffic shows there are burst traffic patterns happening on inbound Internet traffic of Metro-E campus networks. Tele-traffic engineering has found that reducing the rate of traffic flow is an effective way to control traffic bursts. The bursts can lead to network congestion and reduced quality of service (QoS) and by implementing traffic policing mechanisms, the network can better manage these fluctuations and maintain the network stability. Bandwidth management is important to ensure QoS within computer networks. This research has successfully analyzed the data packet and throughput in inbound traffic on the WAN Metro-E campus network. The statistical analysis has helped with data distribution modeling and network traffic policing for the WAN Metro-E campus network's future bandwidth management control mechanisms. Implementing the bandwidth management strategies based on this analysis will be crucial for the Metro-E campus network to function efficiently and provide a seamless online experience for its users and would enhance bandwidth utilization and the quality of service, ensuring that online campus activities go without a hitch.

Acknowledgement

The authors acknowledge the College of Engineering, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia for the support research and funding of this publication.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***planning and verification of analytical methods:*** *Murizah Kassim;* ***theory development and computations:*** *Nor Paezah Abdullah;* ***analysis and interpretation of results:*** *Nor Paezah Abdulla;* ***verification of analytical methods:*** *Sayang Mohd Deni. All authors have discussed the results and contributed to the final manuscript.*

References

[1] Okonkwo, Z., Foo, E., Hou, Z., Li, Q., & Jadidi, Z. (2023). Encrypted Network Traffic Classification with Higher Order Graph Neural Network. *Information Security and Privacy*, 630–650. https://doi.org/10.1007/978-3-031-35486-1_27

[2] Varun Kumar, K. A., & Arivudainambi, D. (2019). Performance analysis of security framework for software defined network architectures. *International Journal of Advances in Applied Sciences*, 8(3), 232. https://doi.org/10.11591/ijaas.v8.i3.pp232-242

[3] Vasconcelos, J., & Lima, G. (2022). Possible risks with EVT-based timing analysis: an experimental study on a multi-core platform. *2022 XII Brazilian Symposium on Computing Systems Engineering (SBESC)*, 1–8. https://doi.org/10.1109/sbesc56799.2022.9964853

[4] Ashaari, M. N., Kassim, M., Rahman, R. A., & Mahmud, A. R. (2021, December 20). Performance Analysis on Multiple Device Connections of Small Office Home Office Network. *Baghdad Science Journal*, *18*(4(Suppl.)), 1457. https://doi.org/10.21123/bsj.2021.18.4(suppl.).1457

[5] Ltayef, N. B., Alzogni, M. Y., Abu-Gunaydah, A. A., & Alhmadi, E. A. (2022, May 23). Improving Network's Performance by Applying Different Quality of Service Mechanisms. *2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*. https://doi.org/10.1109/mi-sta54861.2022.9837711

[6] P, A., H S, V., & J, S. (2023, April 7). PQTBA: Priority Queue based Token Bucket Algorithm for congestion control in IoT network. *2023 IEEE 8th International Conference for Convergence in Technology (I2CT)*. https://doi.org/10.1109/i2ct57861.2023.10126166

[7] Shan, D., Jiang, L., Zhang, P., Jiang, W., Li, H., Tang, Y., & Ren, F. (2023). Enforcing Fairness in the Traffic Policer Among Heterogeneous Congestion Control Algorithms. *IEEE/ACM Transactions on Networking*, 1–16. https://doi.org/10.1109/tnet.2023.3276410

[8] Bahattab, A. A. (2022, March 22). RETRACTED ARTICLE: A Survey on Packet Switching Networks. *IETE Journal of Research*, 1–26. https://doi.org/10.1080/03772063.2022.2048711

[9] Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Doan, L. M. T., Hall, K., Boddu, S., & Kobusińska, A. (2022, March 13). A Survey on Intrusion Detection Systems for Fog and Cloud Computing. *Future Internet*, *14*(3), 89. https://doi.org/10.3390/fi14030089

[10] Abdullah, N. P., Kassim, M., Mohd Yusoff, Y., Mohd Deni, S., & Radman, A. J. (2023). Inbound and Outbound Internet Application Services QOS Analysis on Lan Metro-E Network. *Journal of Theoretical and Applied Information Technology*, *101*(7), 2783–2793. http://www.jatit.org/volumes/Vol101No7/27Vol101No7.pdf

[11] Mall, P. K., Narayan, V., Pramanik, S., Srivastava, S., Faiz, M., Sriramulu, S., & Kumar, M. (2023). FuzzyNet-Based Modelling smart traffic system in smart cities using deep learning models. *In Advances in data mining and database management book series* (pp. 76–95). https://doi.org/10.4018/978-1-6684-6408-3.ch005

[12] Reza, S., Ferreira, M. C., Machado, J., & Tavares, J. M. R. S. (2022). A multi-head attention-based transformer model for traffic flow forecasting with a comparative analysis to recurrent neural networks. *Expert Systems With Applications*, 202, 117275. https://doi.org/10.1016/j.eswa.2022.117275

[13] González-Estrada, E., & Cosmes, W. (2019). Shapiro–Wilk test for skew normal distributions based on data transformations. *Journal of Statistical Computation and Simulation*, 89(17), 3258–3272. https://doi.org/10.1080/00949655.2019.1658763

[14] Wang, Y., Wang, J., Zhang, W., Zhan, Y., Guo, S., Zheng, Q., & Wang, X. (2022). A survey on deploying mobile deep learning applications: A systemic and technical perspective. *Digital Communications and Networks*, 8(1), 1–17. https://doi.org/10.1016/j.dcan.2021.06.001

[15] Baltaci, A., Klügel, M., Geyer, F., Duhovnikov, S., Bajpai, V., Ott, J., & Schupke, D. (2021, May). Experimental UAV data traffic modeling and network performance analysis. *In IEEE INFOCOM 2021-IEEE Conference on Computer Communications* (pp. 1-10). https://doi.org/ 10.1109/INFOCOM42981.2021.9488878

[16] Alasmar, M., Clegg, R., Zakhleniuk, N., & Parisis, G. (2021). Internet traffic volumes are not Gaussian—They are log-normal: An 18-year longitudinal study with implications for modelling and prediction. *IEEE/ACM Transactions on Networking, 29*(3), 1266-1279. https://doi.org/10.1109/TNET.2021.3059542

[17] Cui, Z., Guan, K., Zhang, J., & Zhong, Z. (2021). SNR coverage probability analysis of RIS-aided communication systems. *IEEE Transactions on Vehicular Technology, 70*(4), 3914-3919. https://doi.org/10.1109/TVT.2021.3063408

[18] A. Shafiq, A. B. Çolak, and T. N. Sindhu, "Reliability investigation of exponentiated Weibull distribution using Shafiq, A., Çolak, A. B., & Sindhu, T. N. (2022). Reliability investigation of exponentiated Weibull distribution using IPL through numerical and artificial neural network modeling. *Quality and Reliability Engineering International*, 38(7), 3616-3631. https://doi.org/10.1002/qre.3155

[19] Huang, H., Zhu, X., Bi, J., Cao, W., & Zhang, X. (2021). Machine learning for broad-sensed internet congestion control and avoidance: A comprehensive survey. IEEE Access, 9, 31525-31545. https://doi.org/10.1109/ACCESS.2021.3060287

[20] Nandhini, C., & Gupta, G. P. (2023). Exploration and Evaluation of Congestion Control Algorithms for Data Center Networks. *SN Computer Science, 4*(5), 509. https://doi.org/10.1007/s42979-023-02016-4

[21] Koutlia, K., Bojović, B., Lagén, S., Zhang, X., Wang, P., & Liu, J. (2023). System analysis of QoS schedulers for XR traffic in 5G NR. *Simulation Modelling Practice and Theory*, *125*, 102745. https://doi.org/10.1016/j.simpat.2023.102745

[22] Abdullah, N. P., Kassim, M., & Yussoff, Y. M. (2022, July). Analysis of Internet Application Services Traffic on WAN Metro-E Network. *In 2022 IEEE 13th Control and System Graduate Research Colloquium (ICSGRC)* (pp. 209-214). IEEE. https://doi.org/10.1109/ICSGRC55096.2022.9845156

[23] Nawaz, N. A., Abid, A., Rasheed, S., Farooq, M. S., Shahzadi, A., & Mubarik, I. (2022).Impact of telecommunication network on future of telemedicine in healthcare: A systematic literature review. *International Journal of Advanced and Applied Sciences*. https://doi.org/10.21833/ijaas.2022.07.013

[24] Shallahuddin, A. A., Kadir, M. F. A., Mohamed, M. A., Amri, A. F., & Abidin, N. A. H. (2022). An enhanced adaptive duty cycle scheme for energy efficiency and QoS awareness in wireless sensor networks. *International Journal of Advanced and Applied Sciences*, *9*(5), 127-134. https://doi.org/10.21833/ijaas.2022.05.016

[25] Taleb, T., Boudi, A., Rosa, L., Cordeiro, L., Theodoropoulos, T., Tserpes, K., Dazzi, P., Protopsaltis, A. I., & Li, R. (2022). Toward Supporting XR Services: Architecture and Enablers. *IEEE Internet of Things Journal*, *10*(4), 3567-3586. https://doi.org/10.1109/JIOT.2022.3222103

[26] Om, K., Singh, R., Kaur, S. A., Kaur, D. A., McGill, T., Dixon, M., Wong, K. W., & Koutsakis, P. (2022, December 1). *Artificial intelligence – Based video traffic policing for next generation networks*. Simulation Modelling Practice and Theory. https://doi.org/10.1016/j.simpat.2022.102650

[27] Sutton, G. J., Zeng, J., Liu, R. P., Ni, W., Nguyen, D. N., Jayawickrama, B. A., ... & Lv, T. (2019). Enabling technologies for ultra-reliable and low latency communications: From PHY and MAC layer perspectives. *IEEE Communications Surveys & Tutorials*, *21*(3), 2488-2524. https://doi.org/10.1109/COMST.2019.2897800

[28] Weichlein, T., Zhang, S., Li, P., & Zhang, X. (2023). Data Flow Control for Network Load Balancing in IEEE Time Sensitive Networks for Automation. *IEEE Access*, *11*, 14044-14060. https://doi.org/10.1109/ACCESS.2023.3243286